834. Θεωρία Ομάδων

Σημειώσεις διαλέξεων που δόθηκαν από τον Συκιώτη Μιχαήλ

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών
Αθήνα, 2013

Περιεχόμενα

Κεφάλαιο 1

Βασικές Έννοιες

1.1 Ορισμοί - παραδείγματα

Ορισμός 1.1.1. Μια **ομάδα** G είναι ένα σύνολο εφοδιασμένο με μια πράξη $G \times G \to G$, $(a, b) \mapsto a \cdot b$ έτσι ώστε:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ για κάθε $a, b, c \in G$.

(ii) Υπάρχει ένα στοιχείο 1_G τέτοιο ώστε $a \cdot 1_G = 1_G \cdot a = a$ για κάθε $a \in G$.

(iii) Για κάθε $a \in G$ υπάρχει στοιχείο $a^{-1} \in G$ (αντίστροφο) έτσι ώστε $a \cdot a^{-1} = a^{-1} \cdot a = 1_G$.

Η G λέγεται **αβελιανή** αν $a \cdot b = b \cdot a$ για κάθε $a, b \in G$.
Η **τάξη** της ομάδας G είναι η ισχύς του συνόλου G και συμβολίζεται με $|G|$ ή $o(G)$. Η G λέγεται πεπερασμένη αν $|G| < \infty$ και άπειρη διαφορετικά.

Παραδείγματα 1.1.1. (i) Το σύνολο των αντιστρέψιμων $n \times n$ πινάκων με στοιχεία από ένα σώμα $\mathbb{k}$, $GL_n(\mathbb{k})$, αποτελεί ομάδα με πράξη τον πολλαπλασιασμό πινάκων.

(ii) Το σύνολο των ακεραίων με πράξη την πρόσθεση, $(\mathbb{Z}, +)$, αποτελεί ομάδα.

(iii) Οι ακέραιοι $\bmod n$, $\mathbb{Z}_n$, αποτελούν ομάδα με πράξη την πρόσθεση.

(iv) Η συμμετρική ομάδα $S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}, f \text{ 1-1 και επί}\}$ είναι ομάδα με πράξη τη σύνθεση απεικονίσεων.

(v) Αν $F \subseteq \mathbb{R}^2$, τότε η ομάδα συμμετριών του F,

$$\mathrm{Sym}(F) = \{\phi \in \mathrm{Isom}(\mathbb{R}^2) : \phi(F) = F\}$$

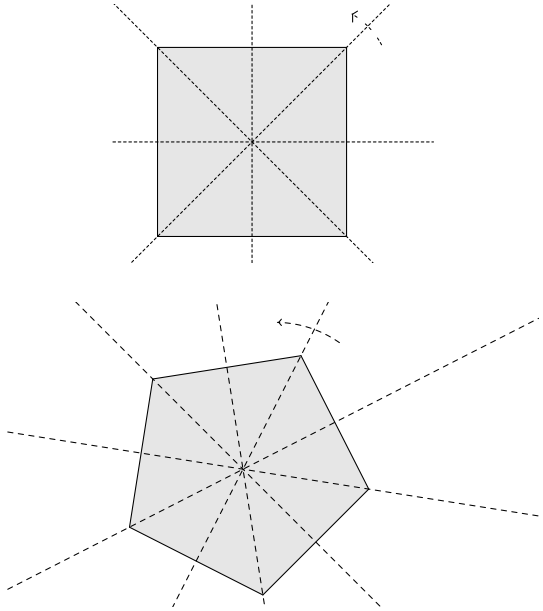
είναι ομάδα με πράξη τη σύνθεση.

(vi) Έστω Π_n ένα κανονικό πολύγωνο του $\mathbb{R}^2$ με n κορυφές. Η διεδρική ομάδα D_n είναι η ομάδα συμμετριών $\mathrm{Sym}(\Pi_n)$. Η τάξη της D_n είναι $|D_n| = 2n$.

Τα στοιχεία της D_n είναι τα εξής:

– n στροφές γωνίας $\frac{2\pi k}{n}, k = 0, 1, \ldots, n-1$, σύμφωνα με τη φορά δεικτών του ρολογιού, γύρω από το κέντρο του πολυγώνου.

– n ανακλάσεις ως προς τους άξονες που ενώνουν απέναντι κορυφές και μέσα απέναντι πλευρών αν ο n είναι άρτιος, ή κορυφές με μέσα απέναντι πλευρών αν ο n είναι περιττός.



Αν a είναι η στροφή με γωνία $\frac{2\pi}{n}$, τότε όλες οι άλλες στροφές είναι $a, a^2, \ldots, a^{n-1}, a^n = 1$. Αν b είναι μια ανάκλαση, τότε

$$D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$$

1.2 Υποομάδες και σύμπλοκα

Ορισμός 1.2.1. Ένα μη κενό υποσύνολο H της G λέγεται **υποομάδα**, και γράφουμε $H \leq G$, αν αποτελεί ομάδα με την πράξη της G, δηλαδή:

(i) Αν $a, b \in H$, τότε $ab \in H$.

(ii) Αν $a \in H$, τότε $a^{-1} \in H$.

Πρόταση 1.2.1. *Ένα μη κενό υποσύνολο H μιας ομάδος G είναι υποομάδα της G ανν $ab^{-1} \in H$, για κάθε $a, b \in H$.*

Παραδείγματα 1.2.1. (i) Έστω $g \in G$. Ορίζουμε

$$g^k = \begin{cases} g \cdot g \cdots g & , k = 1, 2, \ldots \\ 1_G & , k = 0 \\ g^{-1} \cdot g^{-1} \cdots g^{-1} & , k = -1, -2, \ldots \end{cases}$$

Θεωρούμε το υποσύνολο H της G που αποτελείται από όλες τις ακέραιες δυνάμεις του στοιχείου g, δηλαδή $H = \{g^k : k \in \mathbb{Z}\}$.

Εύκολα διαπιστώνουμε ότι η H είναι υποομάδα της G, η οποία λέγεται η **κυκλική υποομάδα της G που παράγεται από το στοιχείο g** και συμβολίζεται με $\langle g \rangle$.

(ii) Το σύνολο $SL_n(\mathbb{k})$, των $n \times n$ πινάκων με ορίζουσα 1 είναι υποομάδα της $GL_n(\mathbb{k})$.

(iii) $SL_n(\mathbb{Z}) \leq SL_n(\mathbb{R})$ (γιατί;).

(iv) Η τομή υποομάδων -και απείρου πλήθους- είναι υποομάδα.

(v) Έστω $X \subseteq G$, υποσύνολο του G. Η υποομάδα της G που παράγεται από το X ορίζεται ως η τομή όλων των υποομάδων που περιέχουν το X. Συμβολίζεται με $\langle X \rangle$ και είναι η μικρότερη υποομάδα της G που περιέχει το X.

Ορισμός 1.2.2. Η **τάξη** ενος στοιχείου $g \in G$ είναι η τάξη της υποομάδας που παράγει, δηλαδή $o(g) = |\langle g \rangle|$.

Αν $o(g) = \infty$, τότε το g είναι απείρου τάξης. Αν $o(g) = n < \infty$, τότε το g λέγεται πεπερασμένης τάξης και μάλιστα ο n είναι ο μικρότερος θετικός ακέραιος έτσι ώστε $g^n = 1$.

Επιπλέον, $g^m = 1$ αν και μόνο αν $n|m$. Πράγματι, αν όλες οι δυνάμεις του g είναι διαφορετικές μεταξύ τους, τότε προφανώς το g είναι απείρου τάξης.

Συνεπώς αν το στοιχείο g έχει πεπερασμένη τάξη n, τότε δεν μπορεί όλες οι ακέραιες δυνάμεις του g να είναι διαφορετικές μεταξύ τους. Δηλαδή, υπάρχουν ακέραιοι $k > \ell$ με $g^k = g^\ell$ και έτσι $g^{k-\ell} = 1$. Έχει νόημα λοιπόν να θεωρήσουμε τον μικρότερο θετικό ακέραιο n για τον οποίο $g^n = 1$. Τότε για $m \in \mathbb{Z}$ είναι $g^m = g^{rn+u} = (g^r)^n \cdot g^u = g^u$, $0 \leq u < n$.

Άρα $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$, δηλαδή $|\langle g \rangle| = n$.

Ορισμός 1.2.3. Μια ομάδα G λέγεται **κυκλική** αν υπάρχει $g \in G$ τέτοιο ώστε $G = \langle g \rangle$. Σε αυτή την περίπτωση το g λέγεται **γεννήτορας** της ομάδας.

Είναι άμεσο από τον ορισμό ότι κάθε κυκλική ομάδα είναι αβελιανή.

Παραδείγματα 1.2.2. (i) Το σύνολο των ακεραίων με την πρόσθεση είναι μια κυκλική ομάδα απείρου τάξης, $(\mathbb{Z}, +) = \langle 1 \rangle$.

(ii) Οι ακέραιοι $\bmod n$ με την πρόσθεση είναι μια κυκλική ομάδα τάξεως n, $(\mathbb{Z}_n, +) = \langle [1] \rangle$.

Ορισμός 1.2.4. Έστω G ομάδα και $H \leq G$. Ορίζουμε **αριστερό σύμπλοκο** ένα σύνολο της μορφής $gH = \{gh : h \in H\}$ και **δεξιό σύμπλοκο** ένα σύνολο της μορφής $Hg = \{hg : h \in H\}$.

Χρησιμοποιώντας την παρακάτω πρόταση διαπιστώνουμε ότι τα αριστερά σύμπλοκα της είναι σε αμφιμονοσήμαντη αντιστοιχία με τα δεξιά σύμπλοκα της H.

$$gH \leftrightarrow Hg^{-1}$$

Συνεπώς, το πλήθος των αριστερών συμπλόκων της H είναι ίσο με το πλήθος των δεξιών συμπλόκων της H.

Πρόταση 1.2.2. *Έστω G ομάδα, $H \leq G$ και $a, b \in G$. Τότε:*

(i) $aH = bH$ *ανν* $b^{-1}a \in H$ *ανν* $a \in bH$.

(ii) $aH = bH$ *ή* $aH \cap bH = \emptyset$.

(iii) $|H| = |aH|$.

Απόδειξη. (i) Αν $aH = bH$, τότε $a \in bH$ και άρα $a = bh$, για κάποιο $h \in H$. Τότε $b^{-1}a = h \in H$.

(iii) Ορίζουμε απεικόνιση $H \to aH, h \mapsto ah$. Η απεικόνιση αυτή είναι 1-1 και επί.

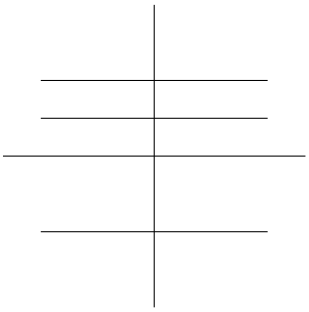
□

Μια υποομάδα H της G ορίζει σχέση ισοδυναμίας στην G ως εξής:

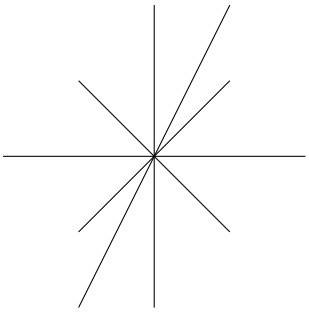
$$a \sim b \iff b^{-1}a \in H$$

Οι κλάσεις ισοδυναμίας είναι τα αριστερά σύμπλοκα.

Παραδείγματα 1.2.3. (i) Έστω $G = (\mathbb{R}^2, +) = (\mathbb{C}, +)$ και $H = \mathbb{R} \leq G$. Τα σύμπλοκα της H στην G είναι ευθείες παράλληλες προς τον άξονα x.



(ii) Έστω $G = (\mathbb{C}^*, \cdot)$ και $H = (\mathbb{R}^*, \cdot) \leq G$. Τα σύμπλοκα της H στην G είναι ευθείες που διέρχονται από την αρχή των αξόνων.



Ορισμός 1.2.5. Έστω G ομάδα. Ο **δείκτης** της H στη G, $[G : H]$, είναι το πλήθος των αριστερών συμπλόκων της H στη G.

Θεώρημα 1.2.1 (Lagrange). *Έστω G πεπερασμένη ομάδα και $H \leq G$. Τότε*

$$|G| = [G : H] \cdot |H|$$

Απόδειξη. Η G είναι ξένη ένωση $[G : H]$ το πλήθος αριστερών συμπλόκων της H, όπου κάθε σύμπλοκο gH έχει $|H|$ το πλήθος στοιχεία.

Συνεπώς, $|G| = [G : H] \cdot |H|$. □

Η μεγάλη χρησιμότητα του Θεωρήματος του Lagrange φαίνεται από τα παρακάτω άμεσα πορίσματα.

Πόρισμα 1.2.1. *Έστω G πεπερασμένη ομάδα και $H \leq G$. Τότε $|H| \Big| |G|$.*

Ένα βασικό ερώτημα είναι αν ισχύει το "αντίστροφο". Δηλαδή, αν G ομάδα, τότε για κάθε διαιρέτη m της $|G|$ υπάρχει υποομάδα $H \leq G$ τάξης m;

Κάτι τέτοιο δεν ισχύει γενικά. Ένα παράδειγμα είναι η A_4, η οποία δεν έχει υποομάδα τάξης 6.

Η απάντηση είναι καταφατική για πεπερασμένες αβελιανές ομάδες ή αν το m είναι δύναμη πρώτου.

Πόρισμα 1.2.2. *Έστω G πεπερασμένη ομάδα και $g \in G$. Τότε $o(g)\Big||G|$.*

Πόρισμα 1.2.3. *Έστω G πεπερασμένη ομάδα με $|G| = p$, όπου p ένας πρώτος. Τότε η G είναι κυκλική.*

Πόρισμα 1.2.4. *Έστω G πεπερασμένη ομάδα με $|G| = n$ και $g \in G$. Τότε $g^n = 1$.*

Απόδειξη. Αν $m = o(g)$, τότε $m|n = |G|$. Συνεπώς $n = mk$, για κάποιο $k \in \mathbb{N}$. Έχουμε, τότε, $g^n = g^{mk} = (g^m)^k = 1_G$. □

Πόρισμα 1.2.5. *Έστω G πεπερασμένη ομάδα και $K \leq H \leq G$. Τότε,*

$$[G : K] = [G : H][H : K]$$

Απόδειξη. Έχουμε

$$\begin{aligned}[G : K] &= \frac{|G|}{|K|} \\ &= \frac{[G : H] \cdot |H|}{|K|} \\ &= \frac{[G : H][H : K] \cdot |K|}{|K|} \\ &= [G : H][H : K]\end{aligned}$$

□

1.3 Κανονικές υποομάδες

Ορισμός 1.3.1. Έστω G ομάδα και $H \leq G$. Η H λέγεται **κανονική** υποομάδα της G, και γράφουμε $H \lhd G$, αν $gHg^{-1} = H$ για κάθε $g \in G$.

Πρόταση 1.3.1. *Έστω G ομάδα και $H \leq G$. Τα ακόλουθα είναι ισοδύναμα:*

(i) $H \lhd G$.

(ii) $gH = Hg$ *για κάθε* $g \in G$.

(iii) $gHg^{-1} \subseteq H$ *για κάθε* $g \in G$.

(iv) $ghg^{-1} \in H$ *για κάθε* $g \in G$ *και για κάθε* $h \in H$.

Απόδειξη. Τα (i),(ii) και (iii),(iv) είναι προφανώς ισοδύναμα.

Από το (i) έχουμε ισότητα, άρα έχουμε και τον εγκλεισμό που απαιτείται στην (iii). Αντίστροφα, αν $gHg^{-1} \subseteq H$ για κάθε $g \in G$, τότε $H \subseteq g^{-1}Hg$ για κάθε $g \in G$. Για $g = g^{-1}$ παίρνουμε $H \subseteq gHg^{-1}$.

Άρα $gHg^{-1} = H$. □

Παραδείγματα 1.3.1. (i) Έστω G ομάδα. Τότε $\{1\} \lhd G$ και $G \lhd G$.

(ii) Αν η G είναι μια αβελιανή ομάδα, τότε κάθε υποομάδα της είναι κανονική. Το αντίστροφο δεν ισχύει.

(iii) Έστω G ομάδα, $H \leq G$ και $[G : H] = 2$. Τότε $H \lhd G$.
Πράγματι, αν $g \in H$ προφανώς $gH = Hg$.

Αν $g \notin H$, τότε $G = H \sqcup gH = H \sqcup Hg$[1] και άρα $gH = G \backslash H = Hg$.

(iv) Από το προηγούμενο έπεται ότι $A_n \lhd S_n$ και $\langle a \rangle \lhd D_n$, όπου a η στροφή γωνίας $\frac{2\pi}{n}$, αφού $D_n = \{1, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\} = \langle a \rangle \sqcup \langle a \rangle b$.

(v) Η τομή κανονικών υποομάδων -και απείρου πλήθους- είναι κανονική υποομάδα.

Ορισμός 1.3.2. Έστω G μια ομάδα, $H \lhd G$ και G/H το σύνολο των αριστερών συμπλόκων της H στη G.

Το σύνολο G/H εφοδιασμένο με την πράξη πολλαπλασιασμού που ορίζεται ως $g_1H \cdot g_2H = g_1g_2H$ για κάθε $g_1, g_2 \in G$, αποκτά την δομή ομάδας και ονομάζεται **ομάδα πηλίκο**.

Παρατηρήσεις 1.3.1. (i) Η τάξη της G/H είναι $|G/H| = [G : H]$.

(ii) Η πράξη πολλαπλασιασμού με την οποία εφοδιάζουμε το σύνολο G/H είναι καλά ορισμένη.

Αν $g_1H = x_1H$ και $g_2H = x_2H$, έχουμε εξ' ορισμού $x_1^{-1}g_1 = h_1 \in H$ και $x_2^{-1}g_2 \in H$. Τότε, $(x_1x_2)^{-1}g_1g_2 = x_2^{-1}x_1^{-1}g_1g_2 = x_2^{-1}h_1g_2 = x_2^{-1}g_2h_2$ για κάποιο $h_2 \in H$.

Έτσι $x_1x_2H = g_1g_2H$.

(iii) Εύκολα διαπιστώνουμε ότι το G/H είναι ομάδα, με μονάδα το σύμπλοκο $1H = H = 1_{G/H}$ και αντίστροφο του συμπλόκου gH, $g \in G$, το σύμπλοκο $g^{-1}H$.

Ορισμός 1.3.3. Μια ομάδα G λέγεται **απλή** αν δεν έχει γνήσιες, μη τετριμμένες κανονικές υποομάδες.

Δηλαδή, αν η ομάδα G είναι απλή και $N \lhd G$, τότε $N = \{1\}$ ή $N = G$.

Πρόταση 1.3.2. *Έστω G πεπερασμένη ομάδα με τάξη πρώτο αριθμό. Τότε η G είναι απλή και κυκλική.*

Απόδειξη. Αν $1 \neq H \leq G$, τότε $1 \neq |H| \Big| |G| = p$, άρα $|H| = |G| = p$. Επίσης $H \subseteq G$, άρα $H = G$. Ιδιαιτέρως, η G είναι απλή.

Για $H = \langle g \rangle$, με $g \neq 1$, έχουμε όπως πριν $G = \langle g \rangle$. □

Παρατήρηση 1.3.1. Στο Κεφάλαιο 10, αποδεικνύεται ότι η A_n είναι απλή για κάθε $n \geq 5$.

1.4 Ομομορφισμοί ομάδων

Ορισμός 1.4.1. Έστω G, H ομάδες και $\phi : G \to H$ μια απεικόνιση. Η ϕ θα λέγεται **ομομορφισμός** αν

$$\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$$

[1] με $\sqcup$ συμβολίζουμε την ξένη ένωση

Ο ομομορφισμός ϕ θα καλείται **μονομορφισμός** αν είναι 1-1 και **επιμορφισμός** αν είναι επί.

Ένας ομομορφισμός είναι **ισομορφισμός** αν είναι 1-1 και επί. Σε αυτή τη περίπτωση λέμε ότι οι ομάδες G και H είναι ισόμορφες και γράφουμε $G \simeq H$.

Ενδομορφισμό καλούμε έναν ομομορφισμό $G \to G$ και **αυτομορφισμό** ένα ισομορφισμό $G \to G$.

Παρατηρήσεις 1.4.1. (i) Αν $\phi : G \to H$ ομομορφισμός ομάδων, τότε $\phi(1_G) = 1_H$.

Πράγματι, $\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G)\phi(1_G)$, οπότε $\phi(1_G) = 1_H$.

(ii) Αν $\phi : G \to H$ ομομορφισμός ομάδων, τότε $\phi(a^{-1}) = (\phi(a))^{-1}$ για κάθε $a \in G$.

Πράγματι, $1_H = \phi(1_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$. Έτσι $\phi(a^{-1}) = (\phi(a))^{-1}$.

(iii) Έστω $\phi : G \to H$ ένας ομομορφισμός ομάδων.

Ορίζουμε την **εικόνα** του ϕ,

$$\operatorname{im}\phi = \{\phi(a) : a \in G\} = \phi(G)$$

Η εικόνα του ϕ είναι υποομάδα της H.

Ορίζουμε τον **πυρήνα** του ϕ,

$$\ker\phi = \{a \in G : \phi(a) = 1_H\} = \phi^{-1}(1_H)$$

Ο πυρήνας του ϕ είναι κανονική υποομάδα της G: αν $a \in \ker\phi$ και $b \in G$, τότε $\phi(bab^{-1}) = \phi(b)\phi(a)\phi(b^{-1}) = 1_H$.

Λήμμα 1.4.1. *Έστω $\phi : G \to H$ ομομορφισμός ομάδων. Τότε ο ϕ είναι 1-1 αννν* $\ker\phi = \{1\}$.

Απόδειξη. Αν ο ϕ είναι 1-1, τότε $\ker\phi = \{1\}$.

Αντίστροφα, αν $\ker\phi = \{1\}$ και $\phi(a) = \phi(b)$, τότε $\phi(ab^{-1}) = 1$ και συνεπώς $ab^{-1} \in \ker\phi = \{1\}$, άρα $a = b$. □

1.4.1 Θεωρήματα ισομορφισμών

Ορισμός 1.4.2. Έστω G ομάδα, $N \lhd G$ και G/N η αντίστοιχη ομάδα πηλίκο. Η απεικόνιση

$$\pi : G \to G/N, \quad g \mapsto gN$$

είναι επιμορφισμός και ονομάζεται **φυσικός** (ή κανονικός) **επιμορφισμός**.

Θεώρημα 1.4.1 (1^o Θεώρημα Ισομορφισμών). *Έστω G ομάδα και $\phi : G \to H$ ένας ομομορφισμός ομάδων. Τότε ο ϕ επάγει ισομορφισμό ομάδων*

$$\tilde{\phi} : G/\ker\phi \to \operatorname{im}\phi$$

Σχόλιο 1.4.1. Συνεπώς κάθε επιμορφική εικόνα της G είναι (ως προς ισομορφισμό) ομάδα πηλίκο της G.

Απόδειξη. Ορίζουμε $\tilde{\phi} : G/\ker\phi \to \operatorname{im}\phi$, με $\tilde{\phi}(gK) = \phi(g)$, για κάθε $gK \in G/\ker\phi$.

Αν $gK = xK$, τότε $x^{-1}g \in \ker\phi$. Άρα $\phi(x^{-1}g) = 1$, οπότε $\phi(x) = \phi(g)$. Έτσι η $\tilde{\phi}$ είναι καλά ορισμένη.

Η $\tilde{\phi}$ είναι ομομορφισμός.
Πράγματι, $\tilde{\phi}(g_1K \cdot g_2K) = \tilde{\phi}(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \tilde{\phi}(g_1K)\tilde{\phi}(g_2K)$.

Η $\tilde{\phi}$ είναι προφανώς επί.
Τέλος, αν $\tilde{\phi}(g_1K) = 1$, τότε $\phi(g) = 1$. Συνεπώς $g \in \ker\phi$, οπότε $\ker\tilde{\phi} = \{1\}$, δηλαδή η $\tilde{\phi}$ είναι 1-1. □

Πόρισμα 1.4.1. *Έστω G πεπερασμένη ομάδα και $\phi : G \to H$ ένας ομομορφισμός ομάδων. Τότε,*

$$|G| = |\ker\phi| \cdot |\operatorname{im}\phi|$$

Παραδείγματα 1.4.1. (i) Έστω $\phi : (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*_+, \cdot)$, με $\phi(z) = |z|$ για κάθε $z \in \mathbb{C}^*$.

Τότε ο ϕ είναι επιμορφισμός και $\ker\phi = \{z \in \mathbb{C}^* : |z| = 1\} = S^1$. Άρα $\mathbb{C}^*/S^1 \simeq \mathbb{R}^*_+$.

(ii) Θεωρούμε την συνάρτηση της ορίζουσας $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$.

Τότε $\det(AB) = \det(A)\det(B)$ και άρα η det είναι επιμορφισμός. Επιπλέον $\ker\det = SL_n(\mathbb{R})$. Συνεπώς $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.

(iii) Έστω $\phi : \mathbb{Z} \to \mathbb{Z}_m$, με $\phi(n) = n \pmod m$.

Τότε η ϕ είναι επιμορφισμός και $\ker\phi = m\mathbb{Z}$. Άρα $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.

Θεώρημα 1.4.2 (2^o Θεώρημα Ισομορφισμών). *Έστω G ομάδα, $N \lhd G$ και $H \leq G$. Τότε $H \cap N \lhd H$, $HN \leq G$ και*

$$H/H \cap N \simeq HN/N$$

Απόδειξη. Έστω $h_1n_1 \in HN$, $h_2n_2 \in HN$. Για να δείξουμε ότι $HN \leq G$ αρκεί να δείξουμε ότι $(h_1n_1)(h_2n_2)^{-1} \in HN$. Έχουμε $h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}[h_2(n_1n_2^{-1})h_2^{-1}] \in HN$, αφού $n_1n_2^{-1} \in N \lhd G$, οπότε $h_2n_1n_2^{-1}h_2^{-1} \in N$.

Θεωρούμε $\phi : H \to HN/N$ με $\phi(h) = hN$ για κάθε $h \in H$.
Εύκολα, έχουμε ότι η ϕ είναι ομομορφισμός και εφόσον $hnN = hNnN = hNN = hN = \phi(h)$ για $h \in H, n \in N$ η ϕ είναι επιμορφισμός.
Έστω $h \in \ker\phi$. Τότε $\phi(h) = 1N$, δηλαδή $hN = N$, ανν $h \in N$. Συνεπώς $\ker\phi = H \cap N \lhd H$.

Από το 1^o Θεώρημα Ισομορφισμών, $H/H \cap N \simeq HN/N$. □

Θεώρημα 1.4.3 (3^o Θεώρημα Ισομορφισμών). *Έστω G ομάδα, $N \lhd H \lhd G$ και $N \lhd G$. Τότε*

$$G/H \simeq (G/N)/(H/N)$$

Απόδειξη. Θεωρούμε την σύνθεση των κανονικών επιμορφισμών

$$G \xrightarrow{\pi_1} G/N \xrightarrow{\pi_2} (G/N)/(H/N)$$

καθώς $H/N \lhd G/N$. Δηλαδή $\phi(g) = gN \cdot H/N$.
Η ϕ είναι επιμορφισμός ως σύνθεση επιμορφισμών.
Έστω $g \in \ker\phi$. Τότε $\phi(g) = 1 \Rightarrow gNH/N = 1 = H/N \Rightarrow gN \in H/N$, δηλαδή $gN = hN$, για κάποιο $h \in H \Rightarrow h^{-1}g \in N \subseteq H \Rightarrow g \in hH = H \Rightarrow \ker\phi \subseteq H$.
Για τον αντίστροφο εγκλεισμό, έστω $h \in H$.Τότε $\phi(h) = hNH/N = H/N = 1 \Rightarrow H \subseteq \ker\phi$.

Από το 1^o Θεώρημα Ισομορφισμών $G/H \simeq (G/N)/(H/N)$. □

Θεώρημα 1.4.4 (Θεώρημα της Αντιστοιχίας). *Έστω $\phi : G \to \overline{G}$ επιμορφισμός ομάδων και $K = \ker\phi$. Τότε ο ϕ επάγει μια 1-1 και επί αντιστοιχία $\tilde{\phi}$ μεταξύ της οικογένειας $\mathcal{A}$ των υποομάδων της G που περιέχουν τον πυρήνα K και της οικογένειας $\mathcal{B}$ των υποομάδων της $\overline{G}$ ως εξής: Αν $H \in \mathcal{A}$, τότε $\tilde{\phi}(H) = \phi(H)$ και αν $\overline{H} \in \mathcal{B}$, τότε $\tilde{\phi}^{-1} : \overline{H} \mapsto \phi^{-1}(\overline{H})$.*

Επιπλέον, για $H, H_1 \in \mathcal{A}$ έχουμε:

(i) $\phi(H_1) \subseteq \phi(H) \Leftrightarrow H_1 \subseteq H$, *στην οποία περίπτωση* $[H : H_1] = [\phi(H) : \phi(H_1)]$.

(ii) $\phi(H) \lhd \phi(G) \Leftrightarrow H \lhd G$ *και σε αυτή την περίπτωση* $G/H \simeq \phi(G)/\phi(H)$.

Απόδειξη. Σημειώνουμε πρώτα ότι η $\tilde{\phi}$ είναι καλά ορισμένη. Πράγματι, αν H υποομάδα της G, τότε η $\phi(H)$ είναι υποομάδα της $\overline{G}$. Επίσης, αν $\overline{H}$ υποομάδα της $\overline{G}$, τότε η $\phi^{-1}(\overline{H})$ υποομάδα της G που περιέχει τον πυρήνα $K = \phi^{-1}\{1\}$, γιατί $1 \in \overline{H}$. Δηλαδή $\phi^{-1}(H) \in \mathcal{A}$.

Για το 1-1 και επί: Έστω $H \in \mathcal{A}$. Τότε $H \mapsto \phi(H) \mapsto \phi^{-1}(\phi(H))$ και αν $\overline{H} \in \mathcal{B}$, τότε $\overline{H} \mapsto \phi^{-1}(\overline{H}) \mapsto \phi(\phi^{-1}(\overline{H}))$

Θα δείξουμε ότι $\phi^{-1}(\phi(H)) = H$ και $\phi(\phi^{-1}(\overline{H})) = \overline{H}$, από τα οποία έπεται ότι η $\tilde{\phi}$ είναι 1-1 και επί.
Έστω $g \in \phi^{-1}(\phi(H)) \Rightarrow \phi(g) \in \phi(H) \Rightarrow \exists h \in H : \phi(g) = \phi(h) \Rightarrow \phi(h^{-1}g) = 1 \Rightarrow h^{-1}g \in \ker\phi \subseteq H \Rightarrow g \in hH = H \Rightarrow \phi^{-1}(\phi(H)) \subseteq H$.
Αντίστροφα, έστω $h \in H \Rightarrow \phi(h) \in \phi(H) \Rightarrow h \in \phi^{-1}(\phi(H)) \Rightarrow H \subseteq \phi^{-1}(\phi(H))$. Έτσι $H = \phi^{-1}(\phi(H))$.

Έστω $g \in \phi(\phi^{-1}(\overline{H})) \Rightarrow g = \phi(x)$, για κάποιο $x \in \phi^{-1}(\overline{H}) \Rightarrow \phi(x) \in \overline{H} \Rightarrow g \in \overline{H}$.
Για τον αντίστροφο εγκλεισμό, έστω $g \in \overline{H}$, τότε επειδή η ϕ είναι επιμορφισμός $g = \phi(x)$, για κάποιο $x \in G$. Έτσι, $\phi(x) = g \in \overline{H} \Rightarrow x \in \phi^{-1}(\overline{H}) \Rightarrow g = \phi(x) \in \phi(\phi^{-1}(\overline{H}))$.

(i) Έστω $H, H_1 \in \mathcal{A}$ με $H_1 \subseteq H$. Τότε, $\phi(H_1) \subseteq \phi(H) \Rightarrow \phi^{-1}(\phi(H_1)) \subseteq \phi^{-1}(\phi(H)) \Rightarrow H_1 \subseteq H$.

Για τους δείκτες: ορίζουμε απεικόνιση $\psi : H/H_1 \to \phi(H)/\phi(H_1)$, μεταξύ των συνόλων των αριστερών συμπλόκων H/H_1 και $\phi(H)/\phi(H_1)$ - εδώ δεν έχουμε αναγκαστικά δομή ομάδας γιατί δεν έχουμε κανονικότητα- με $\psi(hH_1) = \phi(h)\phi(H_1)$, για κάθε $hH_1 \in H/H_1$.

Η ψ είναι καλά ορισμένη: Αν $hH_1 = xH_1 \Rightarrow x^{-1}h \in H_1 \Rightarrow \phi(x^{-1}h) \in \phi(H_1) \Rightarrow \phi(h)\phi(H_1) = \phi(x)\phi(H_1)$.
Η ψ είναι προφανώς επί.
Για το $1-1$: αν $h, x \in H$ και $\phi(h)\phi(H_1) = \phi(x)\phi(H_1)$, τότε$\phi(x^{-1}h) \in \phi(H_1)$. Αυτό σημαίνει ότι $x^{-1}h \in \phi^{-1}(\phi(H)) = H_1$ και έτσι $hH_1 = xH_1$.

Συνεπώς $[H : H_1] = [\phi(H) : \phi(H_1)]$

(ii) Έστω ότι $H \lhd G$ και $x \in \phi(H), y \in \phi(G)$. Θέλουμε να δείξουμε ότι $yxy^{-1} \in \phi(H)$. Εφόσον $x \in \phi(H)$ και $y \in \phi(G)$, $x = \phi(h)$, για κάποιο $h \in H$ και $y = \phi(g)$, για κάποιο $g \in G$. Άρα $yxy^{-1} = \phi(g)\phi(h)\phi(g)^{-1} = \phi(ghg^{-1}) \in \phi(H)$, λόγω της κανονικότητας της H στην G. Αντίστροφα, αν $\phi(H) \lhd \phi(G)$ και $g \in G, h \in H$, τότε $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} \in \phi(H)$, αφού $\phi(H) \lhd \phi(G)$. Άρα $\phi(ghg^{-1}) = \phi(h_1)$, για κάποιο $h_1 \in H \Rightarrow \phi(h_1^{-1}ghg^{-1}) = 1$, δηλαδή $h_1^{-1}ghg^{-1} \in K \subseteq H$ και συνεπώς $ghg^{-1} \in H$, δηλαδή $H \lhd G$.

Για τον ισομορφισμό, θεωρούμε τη σύνθεση $\psi : G \xrightarrow{\phi} \phi(G) \xrightarrow{\pi} \phi(G)/\phi(H)$ με $\psi(g) = \phi(g)\phi(H)$, η οποία είναι επιμορφισμός ως σύνθεση επιμορφισμών.

Αν $\psi(g) = 1 \Rightarrow \phi(g)\phi(H) = \phi(H) \Rightarrow \phi(g) \in \phi(H) \Rightarrow \phi(g) = \phi(h)$, για κάποιο $h \in H$ και $h^{-1}g \in K \subseteq H \Rightarrow g \in hH = H$, δηλαδή $\ker\psi \subseteq H$. Προφανώς $H \subseteq \ker\psi$ και έτσι $\ker\psi = H$.

Από το 1^o Θεώρημα Ισομορφισμών $G/H \simeq \phi(G)/\phi(H)$.

□

Πόρισμα 1.4.2. *Έστω $N \lhd G$. Τότε υπάρχει 1-1 και επί αντιστοιχία μεταξύ των υποομάδων της G που περιέχουν την N και των υποομάδων της ομάδας πηλίκο G/N. Η αντιστοιχία αυτή είναι*

$$N \subseteq H \longmapsto H/N$$

Επιπλέον:

(i) $H \lhd G$ ανν $H/N \lhd G/N$.

(ii) Αν $H \supseteq H_1 \supseteq N$, τότε $[H : H_1] = [H/N : H_1/N]$.

Απόδειξη. Είναι άμεση από το προηγούμενο θεώρημα για τον κανονικό επιμορφισμό $\pi : G \to G/N$. □

Θεώρημα 1.4.5 (Cayley). *Κάθε ομάδα G είναι ισόμορφη με υποομάδα ομάδας μεταθέσεων.*

Απόδειξη. Έστω $X = G$. Για κάθε $g \in G$ ορίζουμε τη μετάθεση $\phi_g : X \to X$, με $\phi_g(x) = gx$, $\forall x \in X$. Η ϕ_g είναι 1-1 και επί, δηλαδή πράγματι $\phi_g \in S(X)$.

Ορίζουμε $\phi : G \to S(X)$, $g \mapsto \phi_g$. Ο ϕ είναι ομομορφισμός.
Πράγματι, $\phi(g_1g_2)(x) = (g_1g_2)x = g_1(g_2x) = \phi(g_1)\phi(g_2)(x)$.

Αν $\phi(g) = 1$, τότε $\phi_g(x) = x$ για κάθε $x \in X$, άρα $gx = x$. Έτσι $g = 1$ και $\ker\phi = 1$, δηλαδή ο ϕ είναι ισομορφισμός $G \xrightarrow{\simeq} \phi(G)$ με $\phi(G) \leq S(X)$. □

1.5 Αυτομορφισμοί ομάδων

Ορισμός 1.5.1. Έστω G ομάδα. Με $\mathrm{Aut}(G)$ συμβολίζουμε το σύνολο των αυτομορφισμών της G. Το σύνολο $\mathrm{Aut}(G)$ γίνεται ομάδα με πράξη τη σύνθεση και ονομάζεται **ομάδα αυτομορφισμών** της G.

Παράδειγμα 1.5.1. $\mathrm{Aut}(\mathbb{Z}) = C_2$, όπου C_2 η κυκλική ομάδα τάξης 2.

Πράγματι, $\mathbb{Z} = \langle 1\rangle$. Αν $\phi \in \mathrm{Aut}(\mathbb{Z})$, τότε το $\phi(1)$ είναι γεννήτορας της $\mathbb{Z}$. Άρα $\phi(1) = 1$ ή $\phi(1) = -1$. Έχουμε ότι $|\mathrm{Aut}(\mathbb{Z})| = 2$, άρα $\mathrm{Aut}(\mathbb{Z}) \simeq C_2$.

Ορισμός 1.5.2. Έστω $g \in G$. Ο αυτομορφισμός $\tau_g : G \to G$ που ορίζεται ως $\tau_g(x) = gxg^{-1}$, ονομάζεται ο **εσωτερικός αυτομορφισμός** που επάγεται από το στοιχείο g.

Το σύνολο των εσωτερικών αυτομορφισμών της G συμβολίζεται με $\mathrm{Inn}(G)$.

Ορισμός 1.5.3. Έστω G ομάδα. Ορίζουμε το **κέντρο** της G, ως το σύνολο

$$Z(G) = \{g \in G : gx = xg \quad \forall x \in G\}$$

Πρόταση 1.5.1. *Έστω G ομάδα. Τότε $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ και*

$$\mathrm{Inn}(G) \simeq G/Z(G)$$

Απόδειξη. Έστω $\tau_{g_1}, \tau_{g_2} \in \mathrm{Inn}(G)$. Τότε $\tau_{g_1}(\tau_{g_2})^{-1} \in Inn(G)$ και άρα $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

Πράγματι, $\tau_{g_1}(\tau_{g_2})^{-1}(x) = \tau_{g_1}(g_2^{-1}xg_2) = g_1g_2^{-1}xg_2g_1^{-1} = \tau_{g_1g_2^{-1}}(x)$. Άρα $\tau_{g_1}(\tau_{g_2})^{-1} = \tau_{g_1g_2^{-1}} \in \mathrm{Inn}(G)$.

Θα δείξουμε ότι $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. Έστω $\phi \in \mathrm{Aut}(G)$ και $\tau_g \in \mathrm{Inn}(G)$. Τότε $\phi\tau_g\phi^{-1}(x) = \phi(g\phi^{-1}(x)g^{-1}) = \phi(g)x\phi(g)^{-1} = \tau_{\phi(g)}(x)$. Έτσι $\phi\tau_g\phi^{-1} = \tau_{\phi(g)} \in \mathrm{Inn}(G)$.

Τέλος, για τον ισομορφισμό, θεωρούμε $\psi : G \to \mathrm{Inn}(G)$, $g \mapsto \tau_g$. Η ψ είναι επί και ομομορφισμός γιατί $\psi(g_1)\psi(g_2) = \tau_{g_1}\tau_{g_2} = \tau_{g_1g_2} = \psi(g_1g_2)$.
Για τον υπολογισμό του πυρήνα, έχουμε $\psi(g) = 1 \Leftrightarrow \tau_g = id_G \Leftrightarrow \tau_g(x) = x \quad \forall x \in G \Leftrightarrow gxg^{-1} = x \quad \forall x \in G \Leftrightarrow gx = xg \quad \forall x \in G \Leftrightarrow g \in Z(G)$.

Άρα $\ker\psi = Z(G)$ και συνεπώς από το 1^o Θεώρημα Ισομορφισμών $\mathrm{Inn}(G) \simeq G/Z(G)$. □

1.6 Ασκήσεις

1. Αποδείξτε ότι αν $H, K \leq G$ με $[G : H] = m$ και $[G : K] = n$, τότε $[G : H \cap K] \geq$ εκπ(m, n). Επιπλέον, έχουμε ισότητα αν οι m και n είναι πρώτοι μεταξύ τους.

2. Αποδείξτε ότι αν οι $H_1, \ldots, H_n$ είναι υποομάδες της G πεπερασμένου δείκτη, τότε και η τομή τους είναι πεπερασμένου δείκτη στην G και $[G : \bigcap_{i=1}^{n} H_i] \leq \prod_{i=1}^{n} [G : H_i]$.

3. Έστω K πεπερασμένη κυκλική υποομάδα της G και $K \lhd G$. Δείξτε ότι κάθε υποομάδα της K είναι κανονική στην G.

4. Έστω $N \lhd G, g \in G$ και $|G/N| = n < \infty$. Υποθέτουμε ότι $(m, n) = 1$ και $g^m \in N$. Δείξτε ότι $g \in N$.

5. Έστω G ομάδα και $Z(G) = \{a \in G : ag = ga \quad \text{για κάθε} \quad g \in G\}$ το κέντρο της G. Αποδείξτε ότι:

   (i) Η $Z(G)$ είναι αβελιανή, κανονική υποομάδα της G.

   (ii) Κάθε υποομάδα του κέντρου είναι κανονική στην G.

   (iii) Αν η G δεν είναι αβελιανή, τότε η $G/Z(G)$ δεν είναι κυκλική.

   (iv) Αν $K \lhd G$ και $|K| = 2$, τότε $K \leq Z(G)$.

   (v) Αν $\phi : G \to G_1$ επιμορφισμός και $H \leq Z(G)$, τότε $\phi(H) \leq Z(G_1)$.

   (vi) Αν $K \lhd G$, τότε η $\frac{Z(G)}{Z(G) \cap K}$ είναι ισόμορφη με υποομάδα της $Z(G/K)$.

6. Έστω G ομάδα και $g, h \in G$. Ο **μεταθέτης** των g και h είναι το στοιχείο $[g, h] = g^{-1}h^{-1}gh$. Η **παράγωγος υποομάδα** G' ορίζεται ως η υποομάδα της G που παράγεται από όλους τους μεταθέτες των στοιχείων της. Αποδείξτε ότι:

   (i) $G' \lhd G$.

   (ii) Αν $H \leq G$ και $G' \subseteq H$, τότε $H \lhd G$.

   (iii) Αν $H \lhd G$, τότε η G/H είναι αβελιανή αν και μόνο αν $G' \leq H$. Ιδιαιτέρως, η G/G' είναι αβελιανή.

7. (i) Έστω G ομάδα και $\phi : G \to G$ απεικόνιση τέτοια ώστε $\phi(g) = g^{-1}$ για κάθε $g \in G$. Αποδείξτε ότι η ϕ είναι ομομορφισμός αν και μόνο αν η G είναι αβελιανή.

(ii) Έστω G πεπερασμένη ομάδα και $\theta : G \to G$ αυτομορφισμός τέτοιος ώστε $\theta^2(g) = g$ για κάθε $g \in G$. Υποθέτουμε επιπλέον ότι αν $g \in G$ και $\theta(g) = g$, τότε $g = 1$. Αποδείξτε ότι $\theta(g) = g^{-1}$ για κάθε $g \in G$ και συνεπώς η G είναι αβελιανή.

[Υπόδειξη:Δείξτε ότι $\{a^{-1}\theta(a) : a \in G\} = G$.]

8. Υποθέτουμε ότι η G είναι μια πεπερασμένη ομάδα με την ιδιότητα $(ab)^n = a^n b^n$ για κάθε $a, b \in G$, όπου n σταθερός ακέραιος μεγαλύτερος του 1. Έστω $G_n = \{a \in G : a^n = 1\}$ και $G^n = \{g^n : g \in G\}$. Αποδείξτε ότι οι G_n και G^n είναι κανονικές υποομάδες της G και ότι $|G^n| = [G : G_n]$.

9. Έστω G πεπερασμένη ομάδα και K κανονική υποομάδα της G με $(|K|, [G : K]) = 1$. Δείξτε ότι η K είναι η μοναδική υποομάδα της G τάξης $|K|$.

10. Έστω $\mathbb{F}$ σώμα και G πεπερασμένη ομάδα. Δείξτε ότι η G είναι ισόμορφη με υποομάδα της γενικής γραμμικής ομάδας $GL_n(\mathbb{F})$, για κάποιο $n \leq |G|$.

[Υπόδειξη: Θεωρήστε διανυσματικό χώρο επί του $\mathbb{F}$ διαστάσεως $|G|$.]

11. Έστω G πεπερασμένα παραγόμενη ομάδα και S πεπερασμένο σύνολο γεννητόρων της G. Ορίζουμε $\| \cdot \|_S : G \to [0, +\infty)$ ως εξής: $\|1_G\|_S = 0$ και για $1_G \neq g \in G$, $\|g\|_S = \min\{n \in \mathbb{N} : g = s_{i_1}^{\varepsilon_1} \cdots s_{i_n}^{\varepsilon_n}, \text{όπου} \quad s_{i_j} \in S \cup S^{-1} \quad \text{και} \quad \varepsilon_j \in \{-1, 1\}\}$.

(i) Αποδείξτε ότι η ομάδα G με την συνάρτηση $d_S(g, h) = \|g^{-1}h\|_S$ γίνεται μετρικός χώρος.

(ii) Αποδείξτε ότι κάθε πεπερασμένα παραγόμενη ομάδα εμφυτεύεται στην ομάδα ισομετριών ενός μετρικού χώρου.

12. Έστω G ομάδα, $H \leq G$ και $K \lhd G$. Αν $N \lhd H$, τότε $NK \lhd HK$.

13. Μια υποομάδα H μιας ομάδας G λέγεται **χαρακτηριστική** στην G, συμβολίζουμε με $H \trianglelefteq G$, αν $\phi(H) \leq H$ για κάθε $\phi \in \mathrm{Aut}(G)$. Αποδείξτε ότι:

(i) Αν $H \trianglelefteq G$, τότε $\phi(H) = H$ για κάθε $\phi \in \mathrm{Aut}(G)$.

(ii) Κάθε χαρακτηριστική υποομάδα είναι κανονική.

(iii) Σε αντίθεση με τις κανονικές υποομάδες, στις χαρακτηριστικές υποομάδες ισχύει η μεταβατικότητα, δηλαδή αν $H \trianglelefteq N$ και $N \trianglelefteq G$, τότε $H \trianglelefteq G$.

(iv) Αν $N \trianglelefteq K$ και $K \lhd G$, τότε $N \lhd G$.

(v) Κάθε υποομάδα μιας κυκλικής ομάδας είναι χαρακτηριστική.

(vi) $Z(G) \trianglelefteq G$ και $G' \trianglelefteq G$.

(vii) Υπάρχουν ομάδες για τις οποίες η κλάση των χαρακτηριστικών υποομάδων είναι γνησίως μικρότερη από την κλάση των κανονικών υποομάδων.

14. Έστω G πεπερασμένα παραγόμενη ομάδα και H υποομάδα της G πεπερασμένου δείκτη. Δείξτε ότι η H είναι πεπερασμένα παραγόμενη.

[Υπόδειξη: Έστω S πεπερασμένο σύνολο γεννητόρων της G και X σύνολο αντιπροσώπων δεξιών συμπλόκων της H στην G. Το σύνολο $\{x_i s_j x_k^{-1} \in H : x_i, x_k \in X, s_j \in S\}$ παράγει την H.]

Κεφάλαιο 2

Δράσεις Ομάδων

2.1 Δράσεις ομάδων επί συνόλων

Ορισμός 2.1.1. Έστω G ομάδα και $X \neq \emptyset$ σύνολο. Μια (αριστερή) **δράση** της G στο X είναι μια απεικόνιση $G \times X \to X$, $(g, x) \mapsto g * x$ με τις ακόλουθες ιδιότητες:

(i) $1_G * x = x$ για κάθε $x \in X$.

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

Το X θα λέγεται **G-σύνολο**.

Σχόλιο 2.1.1. Στο εξής θα συμβολίζουμε το $g * x$ με $g \cdot x$.

Παρατηρήσεις 2.1.1. (i) Κάθε αριστερή δράση επάγει δεξιά δράση και αντίστροφα.

$$g \cdot x \leftrightarrow x \cdot g^{-1}$$

(ii) Κάθε δράση της G στο X επάγει ομομορφισμό $\rho : G \to S_X$, ο οποίος λέγεται και αντίστοιχη (ή επαγόμενη) **αναπαράσταση**, και αντίστροφα κάθε ομομορφισμός $\rho : G \to S_X$ μας δίνει μια δράση της G στο X.
Πράγματι, αν η G δρα επί του X, τότε για κάθε $g \in G$ έχουμε την μετάθεση $p_g \in S_X$ με $p_g(x) = g \cdot x$. Η p_g είναι 1-1 και επί: αν $g \cdot x = g \cdot y$, τότε $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y)$, άρα $1 \cdot x = 1 \cdot y$. Έτσι $x = y$ και $x = g(g^{-1} \cdot x)$, άρα έχουμε ομομορφισμό $\rho : G \to S_X$ με $\rho(g) = p_g$.

Αντίστροφα, αν έχουμε ομομορφισμό $\rho : G \to S_X$ η δράση ορίζεται ως εξής, $g \cdot x = \rho(g)(x)$.

Παραδείγματα 2.1.1. (i) Έστω G ομάδα και $X = G$. Η G δρα στο X με πολλαπλασιασμό από αριστερά.

(ii) Έστω G ομάδα και X σύνολο. Η τετριμμένη δράση της G στο X είναι η δράση $g \cdot x = x$ για κάθε $g \in G$ και $x \in X$.

Δηλαδή είναι η δράση που αντιστοιχεί στον τετριμμένο ομομορφισμό $\rho : G \to S_X$ με $\rho(g) = 1$ για κάθε $g \in G$.

(iii) Έστω $H \leq G$ και $X = G/H$ το σύνολο των αριστερών συμπλόκων της H στην G. Η G δρα στο X με $g \cdot (xH) = gxH$.

(iv) Αν $X = \Pi_\nu$ ένα κανονικό ν-γωνο, τότε η $\mathbb{Z}_\nu$, η κυκλική τάξης ν, δρα στο Π_ν με στροφές. Η D_ν δρα στο X με στροφές και ανακλάσεις.

(v) Η S_X δρα στο X με τον φυσικό τρόπο.

(vi) Η $GL_n(\mathbb{R})$ δρα στο $\mathbb{R}^n$ με $A \cdot x$ το συνηθισμένο γινόμενο.

Ορισμός 2.1.2. Έστω G ομάδα η οποία δρα επί ενός συνόλου X.

Η δράση λέγεται **πιστή**, όταν η αντίστοιχη αναπαράσταση είναι 1-1, δηλαδή $\ker \rho = \{1\}$, $\rho : G \to S_X$.

Το σύνολο

$$Gx = \{g \cdot x : g \in G\} = \mathcal{O}(x)$$

λέγεται **τροχιά** (G-τροχιά) του στοιχείου $x \in X$.

Λέμε ότι η G **δρα μεταβατικά** στο X αν υπάρχει μόνο μια τροχιά για την δράση, δηλαδή για κάθε $x, y \in X$ υπάρχει $g \in G$ τέτοιο ώστε $g \cdot x = y$.

Η **σταθεροποιούσα** του $x \in X$ ορίζεται ως το σύνολο

$$G_x = \mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

Παρατήρηση 2.1.1. Η σταθεροποιούσα είναι υποομάδα της G και ισχύει $G_{gx} = gG_xg^{-1}$.

Έστω $G \rightsquigarrow X$, δηλαδή έστω ότι η G δρα στο X. Εύκολα διαπιστώνουμε ότι η σχέση που ορίζεται ως

$$x \sim y \iff x = g \cdot y$$

είναι σχέση ισοδυναμίας και οι κλάσεις ισοδυναμίας είναι οι τροχιές της δράσης.

Άρα οι τροχιές αποτελούν διαμέριση του συνόλου αυτού και έτσι μπορούμε να γράψουμε το X σαν ξένη ένωση τροχιών.

Παράδειγμα 2.1.1. Έστω G ομάδα και $H \leq G$. Η H δρα επί της G με πολλαπλασιασμό από αριστερά, δηλαδή $h \cdot g = hg$. Η τροχιά ενός x είναι $\mathcal{O}(x) = \{hx : h \in H\} = Hx$ το δεξιό σύμπλοκο του x. Άρα η G είναι ξένη ένωση τροχιών (δεξιών συμπλόκων).

Πρόταση 2.1.1. *Έστω X ένα G-σύνολο και $x \in X$. Τότε $|\mathcal{O}(x)| = [G : G_x]$.*

Απόδειξη. Ορίζουμε απεικόνιση $\phi : \mathcal{O}(x) \to G/G_x$ με $\phi(g \cdot x) = gG_x$. Η ϕ είναι καλά ορισμένη: $g_1x = g_2x \Leftrightarrow g_2^{-1}g_1x = x \Leftrightarrow g_2^{-1}g_1 \in G_x \Leftrightarrow g_1G_x = g_2G_x$. Από τα παραπάνω, έπεται και ότι η ϕ είναι 1-1. Τέλος, είναι προφανώς επί. □

Πόρισμα 2.1.1. *Αν η G είναι πεπερασμένη, τότε $|\mathcal{O}(x)| \Big| |G|$.*

Πόρισμα 2.1.2. *Έστω X πεπερασμένο σύνολο και T ένα σύνολο αντιπροσώπων των τροχιών της δράσης (δηλαδή, το T περιέχει ακριβώς ένα στοιχείο από κάθε τροχιά). Τότε*

$$|X| = \sum_{x \in T} [G : G_x]$$

Απόδειξη. Το X είναι ξένη ένωση τροχιών, δηλαδή $X = \bigsqcup_{x \in T} \mathcal{O}(x)$, άρα

$$|X| = \sum_{x \in T} |\mathcal{O}(x)| = \sum_{x \in T} [G : G_x]$$

□

Πόρισμα 2.1.3. *Θεώρημα Lagrange*

Απόδειξη. Η $H \rightsquigarrow G$ με πολλαπλασιασμό από αριστερά. Εδώ οι τροχιές είναι τα δεξιά σύμπλοκα και $|T| = [G : H]$. Επιπλέον $H_x = \text{Stab}_H(x) = 1$ για κάθε x. Συνεπώς

$$|X| = |G| = \sum_{x \in T} [H : H_x] = \sum_{x \in T} |H| = [G : H] \cdot |H|$$

□

2.2 Δράση ομάδος σε σύμπλοκα υποομάδος

Έστω G μια ομάδα και $H \leq G$. Θεωρούμε $X = G/H$ το σύνολο των αριστερών συμπλόκων της H στη G. Η G δρα επί του X ως εξής:

$$g \cdot (xH) = gxH$$

Ας συμβολίσουμε με $\rho_H : G \to S_{G/H}$ την αντίστοιχη αναπαράσταση.

Η δράση είναι μεταβατική, έχει μόνο μια τροχιά, εφόσον $g \cdot x^{-1} \cdot (xH) = gH$.

Η σταθεροποιούσα του xH είναι,

$$\text{Stab}(xH) = xHx^{-1}$$

μιας και $g \cdot xH = xH \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$.

Άρα, $|\mathcal{O}(x)| = |G/H| = [G : H] = [G : xHx^{-1}]$ για κάθε $x \in G$.

Υπολογίζουμε τώρα τον πυρήνα του ρ_H. Έχουμε ότι $\rho_H(g) = 1 \Leftrightarrow g \cdot xH = xH \quad \forall x \in G \Leftrightarrow g \in xHx^{-1} \quad \forall x \in G \Leftrightarrow g \in \bigcap_{xx \in G} xHx^{-1}$, συνεπώς

$$\ker \rho_H = \bigcap_{x \in G} xHx^{-1} \lhd G$$

Η κανονική υποομάδα της G, $\ker \rho_H = \bigcap_{x \in G} xHx^{-1}$, ονομάζεται **πυρήνας της H** και συμβολίζεται με $\text{Core}(H)$.

Η υποομάδα αυτή, $\text{Core}(H)$, είναι η μεγαλύτερη κανονική υποομάδα της G που περιέχεται στην H.

Πράγματι, αν $N \lhd G$ με $N \subseteq H$, τότε $xNx^{-1} \subseteq xHx^{-1}$ για κάθε $x \in G$. Όμως $N \lhd H \Rightarrow xNx^{-1} = N$, δηλαδή $N \subseteq xHx^{-1}$ για κάθε $x \in G$ και έτσι $N \subseteq \bigcap_{x \in G} xHx^{-1}$.

Ας υποθέσουμε επιπλέον ότι η H έχει πεπερασμένο δείκτη στη G, έστω $[G : H] = n < \infty$. Τότε $S_{G/H} \simeq S_n$ και συνεπώς έχουμε ομομορφισμό (αναπαράσταση), $\rho_H : G \to S_n$.

Πρόταση 2.2.1. *Έστω $H \leq G$ με $[G : H] = n < \infty$. Τότε υπάρχει ομομορφισμός $\rho_H : G \to S_n$ με $\ker \rho_H = \bigcap_{x \in G} xHx^{-1} \subseteq H$.*

Σχόλιο 2.2.1. Συνεπώς $\ker \rho_H \subset G$ αν $H < G$.

Πόρισμα 2.2.1. *Κάθε υποομάδα H πεπερασμένου δείκτη n σε μια ομάδα G περιέχει κανονική υποομάδα N της G πεπερασμένου δείκτη m έτσι ώστε $n|m$ και $m|n!$*

Απόδειξη. Θεωρούμε $\rho_H : G \to S_n$ όπως πριν, και έστω $N = \ker \rho_H = \bigcap_{x \in G} xHx^{-1} \lhd G$. Τότε $G/N \simeq \text{im}\, \rho_H \leq S_n$. Εφόσον η S_n είναι πεπερασμένη ομάδα, έπεται ότι η G/N είναι πεπερασμένη ομάδα, δηλαδή $[G : N] = m < \infty$.

Επιπλέον, $m = |G/N| = |\text{im}\, \rho_H| \Big| |S_n| = n!$, δηλαδή $m|n!$

Τέλος, $m = [G : N] = [G : H][H : N] = n \cdot [H : N]$ και άρα $n|m$. □

Πρόταση 2.2.2. *Το πλήθος των υποομάδων πεπερασμένου δείκτη n σε μια πεπερασμένα παραγόμενη ομάδα G είναι πεπερασμένο.*

Απόδειξη. Για κάθε υποομάδα H της G δείκτη n έχουμε ομομορφισμό $\rho_H : G \to S_n$. Εφόσον η G είναι πεπερασμένα παραγόμενη και η S_n πεπερασμένη, το πλήθος των ομομορφισμών $\phi : G \to S_n$ είναι πεπερασμένο.

Πράγματι, αν $G = \langle g_1, g_2, \ldots, g_k\rangle, X = \{g_1, g_2, \ldots, g_k\}$ και $g \in G$, τότε $g = g_{i_1}^{\varepsilon_1} \cdots g_{i_\lambda}^{\varepsilon_\lambda}$, όπου $g_{i_j} \in X$ και $\varepsilon_i \in \{\pm 1\}$. Άρα $\phi(g) = \phi(g_{i_1})^{\varepsilon_1} \cdots \phi(g_{i_\lambda})^{\varepsilon_\lambda}$. Αυτό σημαίνει ότι ο ομομορφισμός ϕ καθορίζεται πλήρως από τις εικόνες του στα στοιχεία του συνόλου γεννητόρων X, δηλαδή $\phi(g_1), \ldots, \phi(g_k)$. Εφόσον κάθε $\phi(g_i) \in S_n$ έχει το πολύ $n!$ επιλογές, υπάρχουν πεπερασμένοι το πλήθος ομομορφισμοί $\phi : G \to S_n$.

Αρκεί να δείξουμε ότι διαφορετικές υποομάδες δείκτου n επάγουν διαφορετικούς ομομορφισμούς $G \to S_n$.

Έστω, λοιπόν, $H \neq K$, $H, K \leq G$ με $[G : H] = [G : K] = n$. θα δείξουμε ότι $\rho_H \neq \rho_K : G \to S_n$. Έστω ότι $G/H = \{H, g_1H, \ldots, g_{n-1}H\}$ και $G/K = \{K, x_1K, \ldots, x_{n-1}K\}$. Τότε $\rho_H(g)(k) = \lambda \Leftrightarrow gg_kH = g_\lambda H$ και $\rho_K(g)(\mu) = \nu \Leftrightarrow gg_\mu K = g_\nu K$. Οι σχέσεις αυτές ορίζουν τους ομομορφισμούς $\rho_H : G \to S_n$, $\rho_K : G \to S_n$.

Εφόσον $H \neq K$, υπάρχει $h \in H \backslash K$ ή $k \in K \backslash H$. Έστω ότι υπάρχει $h \in H$, $h \notin K$. Παρατηρούμε ότι $\rho_H(h)(1) = 1$ ενώ $\rho_K(h)(1) \neq 1$ γιατί $h \notin K$. Έπεται ότι $\rho_H \neq \rho_K$. □

2.3 Δράση συζυγίας, Κεντροποιούσες υποομάδες, Εξίσωση κλάσεων

Έστω G ομάδα και $X = G$. Η G δρα επί του X ως εξής:

$$g \cdot x = gxg^{-1} = \tau_g(x)$$

Η απεικόνιση αυτή, που στέλνει το ζεύγος (g, x) στο g-συζυγές του x, είναι δράση, αφού $1 \cdot x = x$ και $(g_1g_2) \cdot x = g_1g_2x(g_1g_2)^{-1} = g_1(g_2xg_2)^{-1}g_1^{-1} = g_1 \cdot (g_2 \cdot x)$.

Η τροχιά $\mathcal{O}(x)$ του x λέγεται **κλάση συζυγίας** του x και συμβολίζεται με $\mathrm{Cl}_G(x)$. Δηλαδή η κλάση συζυγίας του x,

$$\mathrm{Cl}_G(x) = \{gxg^{-1} : g \in G\} = \mathcal{O}(x)$$

αποτελείται από όλα τα συζυγή του x.

Η σταθεροποιούσα του x,

$$\begin{aligned}\mathrm{Stab}(x) &= \{g \in G : g \cdot x = x\}\\ &= \{g \in G : gxg^{-1} = x\}\\ &= \{g \in G : gx = xg\}\end{aligned}$$

αποτελείται από τα στοιχεία της G που μετατίθενται με το x. Η υποομάδα $\mathrm{Stab}(x)$ λέγεται **κεντροποιούσα** του x στην G και συμβολίζεται με

$$C_G(x) = \{g \in G : gx = xg\} = \mathrm{Stab}(x)$$

Πρόταση 2.3.1. *Αν G ομάδα, τότε $|\mathrm{Cl}_G(x)| = [G : C_G(x)]$. Ιδιαιτέρως, αν η G είναι πεπερασμένη, τότε $|\mathrm{Cl}_G(x)| \Big| |G|$.*

Σχόλιο 2.3.1. Αν $\rho : G \to S_{|G|}$, η αντίστοιχη αναπαράσταση, τότε $\ker \rho = Z(G)$. Πράγματι, αν $\rho(g) = 1$, τότε $gxg^{-1} = x$ για κάθε $x \in G$, δηλαδή $gx = gx$ για κάθε $x \in G$ ανν $g \in Z(G)$.

Παρατήρηση 2.3.1. Ισχύει ότι $x \in Z(G)$ ανν το $\mathrm{Cl}_G(x)$ είναι μονοσύνολο ανν $\mathrm{Cl}_G(x) = \{x\}$. Πράγματι, αν $x \in Z(G)$, τότε $\mathrm{Cl}_G(x) = \{gxg^{-1} : g \in G\} = \{xgg^{-1} : g \in G\} = \{x\}$ και αντίστροφα, αν το $\mathrm{Cl}_G(x)$ είναι μονοσύνολο, τότε $\mathrm{Cl}_G(x) = \{1 \cdot x\} = \{x\}$ και $gxg^{-1} = x$ για κάθε $g \in G$, άρα $gx = xg$ για κάθε $g \in G$, δηλαδή $x \in Z(G)$.

Θεώρημα 2.3.1 (Εξίσωση των κλάσεων). *Έστω G πεπερασμένη ομάδα και $\mathrm{Cl}_G(x_1)$, $\mathrm{Cl}_G(x_2)$, …, $\mathrm{Cl}_G(x_k)$ οι κλάσεις της G που δεν είναι μονοσύνολα, δηλαδή έστω $\{x_1, x_2, \ldots, x_k\}$ ένα σύνολο αντιπροσώπων των τροχιών της δράσης που δεν είναι μονοσύνολα. Τότε:*

(i) $G = Z(G) \sqcup \mathrm{Cl}_G(x_1) \sqcup \mathrm{Cl}_G(x_2) \sqcup \ldots \sqcup \mathrm{Cl}_G(x_k)$ *και*

(ii) $|G| = |Z(G)| + \sum_{i=1}^{k} |\mathrm{Cl}_G(x_i)| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$

Απόδειξη. Η G δρα στο $X = G$ με συζυγία, δηλαδή $g * x = gxg^{-1}$ και συνεπώς η G είναι ξένη ένωση τροχιών. Έχουμε δει ότι οι τροχιές που είναι μονοσύνολα είναι τα στοιχεία του κέντρου $Z(G)$. □

Παρατήρηση 2.3.2. Το πλήθος των κλάσεων συζυγίας είναι $|Z(G)| + k$.

Πόρισμα 2.3.1. *Αν p πρώτος και $|G| = p^n$, τότε $Z(G) \neq 1$.*

Απόδειξη. Αν $k = 0$, τότε $G = Z(G) \neq 1$.
Αν $k > 0$, τότε $|\mathrm{Cl}_G(x_i)| \Big| |G| = p^n$ και έτσι $p \Big| |\mathrm{Cl}_G(x_i)|$ για κάθε $i = 1, 2, \ldots, k$. Έχουμε ότι $p \Big| |G|$ και $p \Big| |\mathrm{Cl}_G(x_i)|$ για κάθε $i = 1, 2, \ldots, k$. Άρα $p \Big| |G| - \sum_{i=1}^{k} |\mathrm{Cl}_G(x_i)| \Rightarrow p \Big| |Z(G)| \Rightarrow |Z(G)| \geq p$.
Ιδιαιτέρως $Z(G) \neq 1$. □

Πόρισμα 2.3.2. *(i) Αν $|G| = p^n$, όπου ο p είναι πρώτος και $n > 1$, τότε η G δεν είναι απλή.*

(ii) Αν $|G| = p^2$, όπου ο p είναι πρώτος, τότε η G είναι αβελιανή.

Απόδειξη. (i) Αφού $G = p^n$, από το προηγούμενο πόρισμα έπεται ότι $Z(G) \neq 1$. Αν $Z(G) < G$, τότε αφού η $Z(G)$ είναι κανονική, η G δεν είναι απλή.

Αν $G = Z(G)$, η G είναι αβελιανή και κάθε υποομάδα της είναι κανονική. Άρα αρκεί να δείξουμε ότι η G περιέχει γνήσια μη τετριμμένη υποομάδα. Έστω $g \neq 1$. Αν $\langle g \rangle < G$ τελειώσαμε. Αν $\langle g \rangle = G$, τότε η G είναι κυκλική και ορίζουμε $H = \langle g^p \rangle$. Έχουμε ότι $1 \neq H \trianglelefteq G$ και $H \neq G$.

- $H \neq 1$: Αν $H = 1$, τότε $g^p = 1 \Rightarrow |G| = |\langle g \rangle| = p$ -άτοπο.
- Αν $G = H$, τότε $g \in \langle g^p \rangle \Rightarrow g = g^{kp} \Rightarrow g^{kp-1} = 1 \Rightarrow o(g) | kp - 1 \Rightarrow p | kp - 1 \Rightarrow p | 1$ -άτοπο.

(ii) Έχουμε ότι $Z(G) \neq 1$ και $|Z(G)| \Big| |G| = p^2$, άρα $|Z(G)| = p$ ή p^2. Αν $|Z(G)| = p^2 = |G| \Rightarrow Z(G) = G$ και άρα η G είναι αβελιανή.

Αν $|Z(G)| = p$, τότε η ομάδα πηλίκο $G/Z(G)$ έχει $p^2/p = p$ στοιχεία. Αυτό σημαίνει ότι η $G/Z(G)$ είναι κυκλική και συνεπώς η G είναι αβελιανή.

□

2.4 Δράση συζυγίας σε υποομάδες

Έστω G ομάδα και $X = \{H : H \leq G\}$ το σύνολο που αποτελείται από όλες τις υποομάδες της G. Η G δρα στο X ως εξής:

$$g * H = gHg^{-1}$$

Η τροχιά της H, $\mathcal{O}(H) = \{gHg^{-1} : g \in G\}$, λέγεται κλάση συζυγίας της υποομάδας H, και συμβολίζεται με $\mathrm{Cl}_G(H)$.

Η σταθεροποιούσα της $H \in X$

$$\mathrm{Stab}_G(H) = \{g \in G : g * H = H\} = \{g \in G : gHg^{-1} = H\}$$

λέγεται **κανονικοποιούσα** της H στην G, συμβολίζεται με $N_G(H)$, και είναι η μεγαλύτερη υποομάδα της G, στην οποία η H είναι κανονική.

Λήμμα 2.4.1. *(i)* $H \lhd N_G(H)$.

(ii) $H \lhd G$ *ανν* $N_G(H) = G$.

(iii) $|\mathrm{Cl}_G(H)| = [G : N_G(H)]$.

2.5 Ασκήσεις

1. Αποδείξτε ότι η ομάδα αυτομορφισμών της κυκλικής ομάδας τάξης n είναι ισόμορφη με την πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$, δηλαδή $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

   [Υπόδειξη: Ένα στοιχείο $g^m \in C_n$ είναι γεννήτορας της C_n αν και μόνο αν οι m και n είναι πρώτοι μεταξύ τους.]

2. Έστω G πεπερασμένα παραγόμενη ομάδα της οποίας οι υποομάδες πεπερασμένου δείκτου έχουν τετριμμένη δομή. Δείξτε ότι κάθε επιμορφισμός $\phi : G \to G$ είναι αυτομορφισμός.

   [Υπόδειξη: Για κάθε φυσικό n θεωρήστε τις υποομάδες δείκτου n της G και χρησιμοποιήστε το θεώρημα της αντιστοιχίας για να αποδείξετε ότι ο πυρήνας του ϕ περιέχεται σε κάθε υποομάδα της G πεπερασμένου δείκτη.]

3. Έστω G μια πεπερασμένη ομάδα η οποία δρα επί ενός πεπερασμένου συνόλου X και $\mathrm{Fix}(g) = \{x \in X : gx = x\}$ το σύνολο των σταθερών σημείων του στοιχείου $g \in G$.

   (i) Δείξτε ότι το πλήθος των τροχιών της δράσης είναι ίσο με $\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$.

   [Υπόδειξη: Υπολογίστε το πλήθος των ζευγών (g, x), όπου $gx = x$ με δύο τρόπους.]

   (ii) Αν η δράση είναι μεταβατική και $|X| > 1$, τότε υπάρχει στοιχείο της G που δεν σταθεροποιεί κανένα στοιχείο του X.

4. Έστω G μια πεπερασμένη ομάδα τάξεως p^n, όπου p πρώτος, και X πεπερασμένο G-σύνολο. Αν ο πρώτος p δεν διαιρεί το $|X|$, τότε $\bigcap_{g \in G} \mathrm{Fix}(g) \neq \emptyset$.

5. Αν $|G| = n < \infty$ και p ο μικρότερος πρώτος διαιρέτης του n, τότε κάθε υποομάδα H της G δείκτου p είναι κανονική.

6. Αν G είναι μια ομάδα τάξεως p^n, όπου p πρώτος, τότε η G έχει μια κανονική υποομάδα τάξεως p^m για κάθε $m \leq n$.

   [Υπόδειξη: Χρησιμοποιήστε επαγωγή και το θεώρημα της αντιστοιχίας σε κατάλληλα γνήσια πηλίκα της G.]

7. Θεωρώντας δεδομένο ότι η A_5 είναι απλή, δείξτε ότι δεν περιέχει υποομάδες τάξεως $15, 20$ ή 30 (συνεπώς το αντίστροφο του Θεωρήματος του Lagrange δεν ισχύει).

8. Έστω G ομάδα περιττής τάξης και $N \lhd G$ με $|N| = 5$. Να αποδειχθεί ότι η N περιέχεται στο κέντρο της G, $Z(G)$.

9. Έστω G πεπερασμένη, μη-αβελιανή ομάδα και $H \leq G$ με $1 < [G : H] < 5$. Να αποδειχθεί ότι η G είναι απλή.

10. Έστω G πεπερασμένη ομάδα και H, K υποομάδες της G. Χρησιμοποιώντας κατάλληλη δράση, δείξτε ότι $|HK| \cdot |H \cap K| = |H| \cdot |K|$.

11. Έστω G ομάδα, $H \leq G$ και $C_G(H) = \{g \in G : hg = gh \text{ για κάθε } h \in H\}$ η κεντροποιούσα της H στην G. Δείξτε ότι $C_G(H) \lhd N_G(H)$ και ότι το πηλίκο $N_G(H)/C_G(H)$ είναι ισόμορφο με υποομάδα της $\mathrm{Aut}(H)$.

12. Αν G είναι μια ομάδα τάξεως p^n, όπου p πρώτος, και $1 \neq H \lhd G$, τότε $H \cap Z(G) \neq 1$.

13. Αν G μια πεπερασμένη ομάδα και $H \leq G$, τότε $|\bigcup_{g \in G} gHg^{-1}| \leq 1 + |G| - [G : H]$.

14. (i) Έστω G πεπερασμένη ομάδα και $H < G$. Δείξτε ότι υπάρχει στοιχείο της G το οποίο δεν περιέχεται στην ένωση των συζυγών της H.

    (ii) Αν η G είναι πεπερασμένη και όλες οι μεγιστικές υποομάδες της είναι συζυγείς, τότε η G είναι κυκλική.

15. Αν H γνήσια υποομάδα πεπερασμένου δείκτη σε μια ομάδα G, τότε η ένωση των συζυγών $\bigcup_{g \in G} gHg^{-1}$ της H περιέχεται στην G.

    [Υπόδειξη: Χρησιμοποιήστε κατάλληλο πεπερασμένο πηλίκο.]

16. Έστω G πεπερασμένη ομάδα και r το πλήθος των κλάσεων συζυγίας της G.

    (i) Δείξτε ότι $|C_G(a)| \geq |G/G'|$ για κάθε $a \in G$, όπου G' η παράγωγος υποομάδα της G.

    (ii) Αν p_0 είναι ο μικρότερος πρώτος που διαιρεί την τάξη της G και $rp_0 > |G|$, τότε $Z(G) \neq 1$.

    (iii) Αν η G δεν είναι αβελιανή, τότε $r > |Z(G)| + 1$.

    (iv) Αν $|G| = p^3$, όπου p πρώτος, και η G δεν είναι αβελιανή, τότε $G' = Z(G), |Z(G)| = p$ και $r = p^2 + p - 1$.

    [Υπόδειξη: Αν η $G/Z(G)$ είναι κυκλική, τότε η G είναι αβελιανή.]

17. (i) Δείξτε ότι για κάθε σταθερό r η εξίσωση $1 = \frac{1}{n_1} + \ldots + \frac{1}{n_r}$ έχει πεπερασμένες θετικές ακέραιες λύσεις $n_1, \ldots, n_r$.

    (ii) Έστω $C_1, \ldots, C_r$ οι κλάσεις συζυγίας μιας πεπερασμένης ομάδας G και $n_1, \ldots, n_r$ οι τάξεις αυτών, αντίστοιχα. Δείξτε ότι $\frac{1}{n_1} + \ldots + \frac{1}{n_r} = 1$.

(iii) Δείξτε ότι υπάρχουν πεπερασμένες το πλήθος πεπερασμένες ομάδες με ακριβώς r κλάσεις συζυγίας.

18. Έστω G πεπερασμένα παραγόμενη ομάδα. Δείξτε ότι κάθε υποομάδα της G πεπερασμένου δείκτη περιέχει μια χαρακτηριστική υποομάδα πεπερασμένου δείκτη στην G.

[Υπόδειξη: Το πλήθος των υποομάδων της G δεδομένου δείκτη ν είναι πεπερασμένο.]

19. Έστω $G = O(n) = \{A \in M_{n\times n}(\mathbb{R}) : A^tA = I_n\}$ η ομάδα των ορθογώνιων $n \times n$ πινάκων. Αποδείξτε ότι, για κάθε $m \leq n$ η φυσική δράση της G στο σύνολο των m-διάστατων υπόχωρων του $\mathbb{R}^n$ είναι μεταβατική.

[Υπόδειξη: Ένας πίνακας είναι ορθογώνιος αν και μόνο αν οι στήλες του αποτελούν ορθοκανονική βάση του $\mathbb{R}^n$.]

20. Έστω G ομάδα και X, Y δύο G-σύνολα. Μια απεικόνιση $\phi : X \to Y$ λέγεται G-**απεικόνιση** αν $\phi(gx) = g\phi(x)$ για κάθε $g \in G$ και $x \in X$ και G-**ισομορφισμός** αν είναι επιπλέον 1-1 και επί. Αποδείξτε ότι η G δρα μεταβατικά επί του X ανν το X είναι G-ισόμορφο με το G/H για κάποια υποομάδα H της G.

[Η G δρα στο σύνολο των αριστερών συμπλόκων G/H με τον φυσικό τρόπο.]

21. Έστω G πεπερασμένη ομάδα τάξεως $2 \cdot 3 \cdot 7 \cdot 11$. Δείξτε ότι κάθε υποομάδα της G τάξεως 77 είναι κανονική.

22. Έστω G μια ομάδα η οποία δρα με ομοιομορφισμούς επί ενός συνεκτικού τοπολογικού χώρου X. Υποθέτουμε ότι υπάρχει ανοικτό υποσύνολο U του X έτσι ώστε $X = \bigcup_{g\in G} gU$. Δείξτε ότι η G παράγεται από το σύνολο $S = \{g \in G : gU \cap U \neq \emptyset\}$.

[Υπόδειξη: Μελετήστε τα σύνολα HU και $(G\backslash H)U$, όπου $H = \langle S\rangle$.]

23. Έστω G ομάδα η οποία δρα μεταβατικά επί ενός συνόλου X και f αυτομορφισμός της G. Αποδείξτε ότι υπάρχει 1-1 και επί απεικόνιση $\phi : X \to X$ τέτοια ώστε $\phi(gx) = f(g)\phi(x)$ για κάθε $g \in G, x \in X$, ανν ο αυτομορφισμός f μεταθέτει τις σταθεροποιούσες των σημείων $x \in X$.

24. Αν $G = \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n}$, όπου p πρώτος, τότε η ομάδα $\mathrm{Aut}(G)$ δρα μεταβατικά (με την φυσική δράση) στο σύνολο $G\backslash\{1_G\}$. Ισχύει το αντίστροφο;

[Υπόδειξη: Δείξτε πρώτα ότι $G \simeq GL_n(\mathbb{Z}_p)$.]

Κεφάλαιο 3

Θεωρήματα Sylow

3.1 Θεωρήματα Sylow και p-ομάδες

Θεώρημα 3.1.1 ($1^ο$ Θεώρημα Sylow). *Έστω G πεπερασμένη ομάδα τάξεως $p^n m$, όπου p πρώτος και $(p,m)=1$, δηλαδή $p \nmid m$. Τότε, για κάθε $s \in \{0,1,\ldots,n\}$ η G περιέχει υποομάδα τάξεως p^s.*

Απόδειξη. Έστω $\mathcal{X} = \{S \subseteq G : |S| = p^s\} \neq \emptyset$, δηλαδή η οικογένεια των υποσυνόλων της G με p^s στοιχεία. Η G δρα στο $\mathcal{X}$ με πολλαπλασιασμό από αριστερά, $g \cdot A = gA$, για $g \in G, A \in \mathcal{X}$.

$1^ο$ Βήμα: Υπολογίζουμε

$$\begin{aligned}
|\mathcal{X}| &= \binom{p^n m}{p^s} \\
&= \frac{(p^n m)!}{p^s!(p^m - p^s)!} \\
&= \frac{p^n m(p^n m - 1)\cdots(p^n m - p^s + 1)}{1 \cdot 2 \cdots p^s} \\
&= p^{n-s} m \frac{(p^n m - 1)\cdots[p^n m - (p^s - 1)]}{1 \cdot 2 \cdots (p^s - 1)} \\
&= p^{n-s} m \prod_{i=1}^{p^s - 1} \frac{p^n m - i}{i}
\end{aligned}$$

$2^ο$ Βήμα: Θεωρούμε τους ρητούς $\frac{p^n m - i}{i}, 1 \leq i \leq p^s - 1$.

Αν $p^\lambda | i$, τότε $p^\lambda < p^s \Rightarrow \lambda < s$ και $p^\lambda | p^n m$. Άρα $p^\lambda | p^n m - i$.

Αν $p^\lambda | p^n m - i$ και $\lambda \geq s$, τότε $p^s | p^n m - i$ και $p^s | p^n m$. Άρα $p^s | i \Rightarrow p^s \leq i$ -άτοπο.

Έχουμε, λοιπόν, ότι αν $p^\lambda | p^n m - i$, τότε $\lambda < s$ και $p^\lambda | i$. Συμπεραίνουμε ότι οι φυσικοί i και $p^n m - i$ εμφανίζουν την ίδια δύναμη του πρώτου p στην ανάλυση τους σε γινόμενο πρώτων. Αυτό σημαίνει ότι $p^{n-s+1} \nmid |\mathcal{X}|$.

$3^ο$ Βήμα: Το $\mathcal{X}$ είναι ξένη ένωση τροχιών, $\mathcal{X} = \mathcal{O}_1 \sqcup \ldots \sqcup \mathcal{O}_\mu$, άρα $|\mathcal{X}| = |\mathcal{O}_1| + \ldots + |\mathcal{O}_\mu|$. Εφ' όσον $p^{n-s+1} \nmid |\mathcal{X}|$, υπάρχει τροχιά $\mathcal{O}_i$ έτσι ώστε $p^{n-s+1} \nmid |\mathcal{O}_i|$. Έστω ότι αυτή η τροχιά είναι η τροχιά $\mathcal{O}(\Lambda)$, όπου $\Lambda \in \mathcal{X}$ και έστω G_Λ η αντίστοιχη σταθεροποιούσα. Τότε

$p^n m = |G| = |\mathcal{O}(\Lambda)||G_\Lambda|$. Η μεγαλύτερη δύναμη του p που μπορεί να διαιρεί τον $|\mathcal{O}(\Lambda)|$ είναι p^{n-s}. Όμως $p^n \Big| |\mathcal{O}(\Lambda)| \cdot |G_\Lambda|$. Έπεται ότι $p^s \Big| |G_\Lambda|$.

Ιδιαιτέρως, $p^s \leq |G_\Lambda|$. Αφού $G_\Lambda \cdot \Lambda = \Lambda$, αν $x \in \Lambda$, τότε $g_\lambda \cdot x \in \Lambda$ για κάθε $g_\lambda \in G_\Lambda$. Δηλαδή $G_\Lambda \cdot x \subseteq \Lambda \Rightarrow |G_\Lambda| = |G_\Lambda \cdot x| \leq |\Lambda| = p^s$. Τελικά, $|G_\Lambda| = p^s$

□

Ορισμός 3.1.1. Έστω p πρώτος και G πεπερασμένη ομάδα. Λέμε ότι η G είναι **p-ομάδα** αν η τάξη της είναι δύναμη του πρώτου p, δηλαδή $|G| = p^\lambda, \lambda \in \mathbb{N}$.

Ορισμός 3.1.2. Έστω G πεπερασμένη ομάδα με $|G| = p^n m$, όπου p πρώτος, $n \in \mathbb{N}, p \nmid m$. Μια **Sylow p-υποομάδα** της G είναι μια p-υποομάδα της G μέγιστης τάξης, δηλαδή μια υποομάδα τάξεως p^n.

Σχόλιο 3.1.1. Η ύπαρξη των Sylow p-υποομάδων της G εξασφαλίζεται από το προηγούμενο θεώρημα.

Πόρισμα 3.1.1. *Έστω G μια πεπερασμένη ομάδα. Τότε η G είναι p-ομάδα ανν κάθε στοιχείο της G έχει τάξη μια δύναμη του πρώτου p.*

Απόδειξη. Αν η G είναι p-ομάδα και $g \in G$, τότε $o(g) \Big| |G| = p^k$ και έτσι $o(g) = p^\lambda, \lambda \leq k$.

Αντίστροφα, έστω ότι κάθε στοιχείο της G έχει τάξη μια δύναμη του πρώτου p. Έστω ότι ο q είναι πρώτος διαιρέτης της $|G|$. Από το προηγούμενο θεώρημα, η G έχει υποομάδα H τάξεως q, η οποία θα είναι κυκλική. Δηλαδή $H = \langle g \rangle, o(g) = q$. Από την υπόθεση, $o(g) = p$. Έπεται ότι $q = p$, συνεπώς κάθε πρώτος διαιρέτης της τάξεως της G είναι ίσος με τον πρώτο p, άρα $|G| = p^k$. □

Πόρισμα 3.1.2 (Cauchy). *Αν η G είναι πεπερασμένη ομάδα και p πρώτος με $p \Big| |G|$, τότε υπάρχει $g \in G$ με $o(g) = p$.*

Απόδειξη. Άμεση από την απόδειξη του προηγούμενου πορίσματος. □

Θεώρημα 3.1.2 (Sylow). *Έστω G πεπερασμένη ομάδα με $|G| = p^n m$, όπου p πρώτος με $p \nmid m$. Τότε:*

1. *Η G έχει τουλάχιστον μια Sylow p-υποομάδα.*
2. *Κάθε p-υποομάδα της G περιέχεται σε μια Sylow p-υποομάδα της G.*
3. *Όλες οι Sylow p-υποομάδες της G είναι συζυγείς στην G.*
4. *Αν n_p είναι το πλήθος των Sylow p-υποομάδων της G, τότε*

$$n_p \geq 1, n_p | m \quad \textit{και} \quad n_p \equiv 1 \pmod{p}$$

5. *Η G έχει μοναδική Sylow p-υποομάδα P ανν $P \lhd G$.*

Απόδειξη. 1. Έχει δειχθεί προηγουμένως.

2. Έστω S p-υποομάδα της G και P μια Sylow p-υποομάδα της G.

   Θεωρούμε την φυσική δράση της υποομάδας S στα αριστερά σύμπλοκα G/P της P στην G.

Αν μια τροχιά $\mathcal{O}(xP)$ δεν είναι μονοσύνολο, τότε $p\Big||\mathcal{O}(xP)|$ γιατί $|\mathcal{O}(xP)|\Big||S| = p^i$. Όμως το σύνολο G/P είναι ξένη ένωση τροχιών με $|G/P| = m$ και $p \nmid m$.

Έπεται ότι υπάρχει τροχιά που είναι μονοσύνολο, έστω $\mathcal{O}(xP) = \{xP\}$. Τότε $g \cdot xP = xP$, $\forall g \in S$. Δηλαδή $g \in xPx^{-1}$ για κάθε $g \in S$ από το οποίο έπεται ότι $S \subseteq xPx^{-1}$. Όμως xPx^{-1} Sylow p-υποομάδα της G, αφού $|xPx^{-1}| = |P| = p^n$.

3. Έστω P και P_1 Sylow p-υποομάδες της G. Όπως πριν βρίσκουμε ότι $P_1 \subseteq xPx^{-1}$ για κάποιο $x \in G$. Αφού τα σύνολα P_1 και xPx^{-1} είναι ισοπληθικά, έχουμε ότι $P_1 = xPx^{-1}$.

4. Έστω P Sylow p-υποομάδα και $C(P)$ η κλάση συζυγίας της P. Από το προηγούμενο, το $C(P)$ είναι το σύνολο όλων των Sylow p-υποομάδων της G. Άρα $n_p = |C(P)| = [G : N_G(P)]$ και $m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P] = n_p \cdot [N_G(P) : P]$, δηλαδή $n_p | m$.

   Θεωρούμε την δράση της G στο $C(P)$ με συζυγίες και τον περιορισμό αυτής στην υποομάδα P. Έτσι $P \rightsquigarrow C(P)$. Αν μια τροχιά, $\mathcal{O}(xPx^{-1})$, δεν είναι μονοσύνολο, τότε το "μήκος" της διαιρείται από τον p. θα δείξουμε ότι η μόνη τροχιά που είναι μονοσύνολο είναι η τροχιά $\mathcal{O}(P)$ της υποομάδας P.

   Έστω ότι $P_1 \in C(P)$ με $\mathcal{O}(P_1) = \{P_1\}$. Αυτό σημαίνει ότι $gP_1g^{-1} = P_1$, $\forall g \in P$ και άρα $g \in N_G(P_1)$, $\forall g \in P$, δηλαδή $P \subseteq N_G(P_1)$. Έτσι, λοιπόν, έχουμε P, $P_1 \subseteq N_G(P_1)$ και $|P| = |P_1| = p^n$. Εφόσον οι P, P_1 είναι Sylow p-υποομάδες της $N_G(P_1)$, οι P και P_1 είναι συζυγείς στην $N_G(P_1)$. Δηλαδή υπάρχει $x \in N_G(P_1)$ με $P = xP_1x^{-1} = P_1$. Τελικά, $P = P_1$. Το $C(P)$ είναι ξένη ένωση τροχιών, άρα

$$n_p = |C(P)| = 1 + \sum_{P' : \mathcal{O}(P') \supset \{P'\}} |\mathcal{O}(P')| = 1 + \sum p^{a_i}, a_i > 0$$

   Έπεται ότι $n_p \equiv 1 \pmod{p}$.

5. Η P είναι η μοναδική Sylow p-υποομάδα ανν $n_p = 1$ ανν $[G : N_G(P)] = 1$ ανν $G = N_G(P)$ ανν $P \lhd G$.

□

Πρόταση 3.1.1. *Αν P Sylow p-υποομάδα μιας πεπερασμένης ομάδας G και $N_G(P) \leq H \leq G$, τότε $H = N_G(H)$.*

Απόδειξη. Έχουμε ότι $P \subseteq N_G(P) \subseteq H \subseteq N_G(H) \subseteq G$. Έστω $g \in N_G(H)$. Τότε $gPg^{-1} \subseteq gHg^{-1} = H$. Δηλαδή, οι P και gPg^{-1} είναι Sylow p-υποομάδες της H. Άρα οι P και gPg^{-1} είναι συζυγείς στην H. Έστω $h \in H$ με $P = hgPg^{-1}h^{-1} = hgP(hg)^{-1}$. Έπεται ότι $hg \in N_G(P) \subseteq H$. Αφού $h \in H$, έχουμε ότι $g \in H$, δηλαδή $N_G(H) \subseteq H$. Τελικά, $N_G(H) = H$. □

3.2 Εφαρμογές

Πρόταση 3.2.1. *Αν $|G| = pq$, όπου p, q πρώτοι και $p \leq q$, τότε η G έχει κανονική κυκλική υποομάδα τάξεως q. Ιδιαιτέρως, η G δεν είναι απλή.*

Απόδειξη. Αν $p = q$, τότε $|G| = p^2$. Από την Άσκηση 3.1.1 η G περιέχει κανονική υποομάδα τάξεως p, η οποία είναι κυκλική.

Αν $p < q$, τότε έστω n_q το πλήθος των Sylow q-υποομάδων της G. Αν Q μια Sylow q-υποομάδα της G, τότε από το Θεώρημα Sylow $|Q| = q$ και άρα είναι κυκλική τάξεως q. Για να δείξουμε ότι $Q \lhd G$, αρκεί να δείξουμε ότι $n_q = 1$. Έστω ότι $n_q > 1$. Γνωρίζουμε ότι

$n_q|p \Rightarrow n_q = 1$ ή $p \Rightarrow n_q = p$ και
$n_q \equiv 1 \pmod{p} \Rightarrow q|n_q - 1 \Rightarrow q \leq n_q - 1 \Rightarrow q \leq p - 1 \Rightarrow q < p$ -άτοπο.
Άρα $n_q = 1 \Leftrightarrow Q \lhd G$. □

Πόρισμα 3.2.1. *Αν $|G| = 2p$, όπου p περιττός πρώτος, τότε*

$$G \simeq \mathbb{Z}_{2p} = C_{2p}$$

ή

$$G = \langle a, b | a^p = b^2 = 1, b^{-1}ab = a^{p-1} \rangle \simeq D_p$$

Απόδειξη. Από την Πρόταση 3.2.1 υπάρχει κανονική κυκλική υποομάδα της G τάξεως p, έστω $\langle a \rangle$, δηλαδή $\langle a \rangle \lhd G$ και $o(a) = p$. Από το Θεώρημα Cauchy, υπάρχει $b \in G$ με $o(b) = 2$ (άρα $b = b^{-1}$).

Εφόσον $\langle a \rangle \lhd G$, $b^{-1}ab \in \langle a \rangle$ και άρα $b^{-1}ab = a^s, 1 \leq s \leq p-1$. Επιπλέον, $a = ba^sb^{-1} = (bab^{-1})^s = (b^{-1}ab)^s = (a^s)^s = a^{s^2}$. Δηλαδή $a^{s^2} = a \Rightarrow a^{s^2-1} = 1 \Rightarrow o(a) = p|s^2 - 1 = (s-1)(s+1) \Rightarrow p|s-1$ ή $p|s+1$. Διακρίνουμε περιπτώσεις:

- Αν $p|s-1$, τότε αφού $s - 1 \leq p - 2 < p$, έχουμε $s - 1 = 0 \Rightarrow s = 1$. Σε αυτή την περίπτωση $b^{-1}ab = a \Leftrightarrow ab = ba$. Τα a και b μετατίθενται και οι τάξεις τους είναι πρώτοι μεταξύ τους. Άρα $o(ab) = o(a) \cdot o(b) = 2p = |G|$. Συνεπώς, $G = \langle ab \rangle \simeq \mathbb{Z}_{2p}$.

- Αν $p|s+1$, τότε αφού $s + 1 \leq p - 1 + 1 = p$, έχουμε $p = s + 1 \Rightarrow s = p - 1$ και $b^{-1}ab = a^{p-1}$. Έχουμε, λοιπόν, $a^p = b^2 = 1, b^{-1}ab = a^{p-1}$ και τα a, b παράγουν την G όπως αποδεικνύουμε στη συνέχεια.

  Ισχύει ότι $|G/\langle a \rangle| = 2$ και $b \notin \langle a \rangle$, αφού $o(b) = 2 \nmid p = |\langle a \rangle|$. Άρα $G/\langle a \rangle = \langle b\langle a \rangle \rangle$ και για κάθε $g \in G$, $g\langle a \rangle = (b\langle a \rangle)^k = b^k\langle a \rangle$, όπου $k = 0$ ή 1. Συνεπώς, $g \in b^k\langle a \rangle \Rightarrow g = b^k a^\lambda \Rightarrow g \in \langle b, a \rangle$.

□

Θεώρημα 3.2.1. *Έστω G πεπερασμένη ομάδα. Αν η τάξη της G έχει ακριβώς τρεις πρώτους παράγοντες, τότε η G δεν είναι απλή.*

Απόδειξη. Διακρίνουμε τρεις περιπτώσεις:

- $|G| = p^3$. Από την Άσκηση 3.1.1, η G έχει κανονική υποομάδα τάξεως p (ή και p^2) και έτσι δεν είναι απλή.

- $|G| = p^2q$, όπου p, q πρώτοι και $p \neq q$. Ας υποθέσουμε ότι $n_p > 1$ και $n_q > 1$.
  $n_p|q \Rightarrow n_p = q \geq 2$
  $n_p \equiv 1 \pmod{p} \Rightarrow p \leq n_p - 1 = q - 1 \Rightarrow p < q$
  $n_q|p^2 \Rightarrow n_q = p$ ή p^2
  $n_q \equiv 1 \pmod{q} \Rightarrow q \leq n_q - 1 \Rightarrow n_q > q > p \Rightarrow n_q = p^2$.

  Συνεπώς, η G έχει $p^2(q-1)$ στοιχεία τάξεως q (μιας και οι n_q το πλήθος Sylow q-υποομάδες της G ανά δύο έχουν τετριμμένη τομή) και τουλάχιστον $p^2 + p^2 - p$ στοιχεία τάξεως p ή p^2 ή 1.

  Άρα $|G| \geq p^2(q-1) + p^2 + p^2 - p = p^2q - p^2 + 2p^2 - p = p^2q + p^2 - p > p^2q = |G|$ -άτοπο. Άρα $n_p = 1$ ή $n_q = 1$ και η αντίστοιχη Sylow υποομάδα (p ή q) θα είναι κανονική.

- $|G| = pqr$, $p < q < r$. Ας υποθέσουμε πάλι ότι $n_p > 1, n_q > 1$ και $n_r > 1$.
  $n_r | pq \Rightarrow n_r = p$ ή q ή pq
  $n_r \equiv 1 \pmod{r} \Rightarrow r | n_r - 1 \Rightarrow r \leq n_r - 1 \Rightarrow n_r > r \Rightarrow n_r = pq$
  $n_q | pr \Rightarrow n_q = p$ ή r ή pr
  $n_q \equiv 1 \pmod{q} \Rightarrow q | n_q - 1 \Rightarrow q \leq n_q - 1 \Rightarrow n_q > q > p \Rightarrow n_q \geq r$
  $n_p | qr \Rightarrow n_p = q$ ή r ή $qr \Rightarrow n_p \geq q$.

  Οι n_r το πλήθος Sylow r-υποομάδες μας δίνουν $n_r(r-1)$ στοιχεία τάξης r.

  Οι n_q το πλήθος Sylow q-υποομάδες μας δίνουν $n_q(q-1)$ στοιχεία τάξης q.

  Οι n_p το πλήθος Sylow p-υποομάδες μας δίνουν $n_p(p-1)$ στοιχεία τάξης p.

  Συνεπώς,

$$\begin{aligned} |G| &\geq n_r(r-1) + n_q(q-1) + n_p(p-1) + 1 \\ &\geq pq(r-1) + r(q-1) + q(p-1) + 1 \\ &= pqr - pq + rq - r + qp - q + 1 \\ &= pqr + r(q-1) - (q-1) \\ &= pqr + (r-1)(q-1) \\ &> pqr = |G| \end{aligned}$$

  Τελικά, $n_r = 1$ ή $n_q = 1$ ή $n_p = 1$ και η αντίστοιχη Sylow υποομάδα θα είναι κανονική. Έτσι, η G δεν είναι απλή.

□

3.3 Ασκήσεις

1. (i) Έστω a και b δύο στοιχεία πεπερασμένης τάξης μιας ομάδας G. Αν τα a και b μετατίθενται ($ab = ba$) και οι τάξεις τους $o(a)$ και $o(b)$ είναι πρώτοι μεταξύ τους, τότε $o(ab) = o(a) \cdot o(b)$.

   (ii) Δείξτε ότι η πολλαπλασιαστική ομάδα $\mathbb{F}^*$ ενός πεπερασμένου σώματος $\mathbb{F}$ είναι κυκλική.

   [Υπόδειξη: Έστω $|\mathbb{F}^*| = p_1^{n_1} \cdots p_k^{n_k}$, όπου p_i πρώτοι διαφορετικοί μεταξύ τους και P_i η Sylow p_i-υποομάδα της $\mathbb{F}^*$ με $|P_i| = p_i^{n_i}$. Δείξτε ότι η P_i είναι κυκλική.]

2. (i) Δείξτε ότι υποομάδες και ομάδες πηλίκα p-ομάδων είναι p-ομάδες.

   (ii) Αν $N \lhd G$ και $N, G/N$ p-ομάδες, τότε και η G είναι p-ομάδα.

3. Έστω G πεπερασμένη p-ομάδα και H μεγιστική (γνήσια) υποομάδα της G. Τότε $H \lhd G$ και $[G : H] = p$.

4. (i) Έστω G ομάδα, K πεπερασμένη κανονική υποομάδα της G και P Sylow p-υποομάδα της K. Δείξτε ότι $G = N_G(P) \cdot K$.

   (ii) Αν κάθε μεγιστική υποομάδα μιας πεπερασμένης ομάδας G είναι κανονική (στην G), τότε κάθε Sylow υποομάδα της G είναι κανονική.

5. (i) Έστω $H \leq G$, P Sylow p-υποομάδα της H και Q Sylow p-υποομάδα της G τέτοια ώστε $P \leq Q$. Δείξτε ότι $P = Q \cap H$.

(ii) Έστω H p-υποομάδα της G, τέτοια ώστε $p|[G:H]$. Δείξτε ότι $H < N_G(H)$.

6. Έστω G πεπερασμένη ομάδα και P Sylow p-υποομάδα της G.

   (i) Αν $N_G(P) \leq H \leq G$, τότε $[G:H] \equiv 1 \pmod{p}$.

   (ii) Αν $K \lhd G$, τότε η $K \cap P$ είναι Sylow p-υποομάδα της K και η PK/K είναι Sylow p-υποομάδα της G/K.

   (iii) Αν $K \lhd G$, τότε $n_p(G/K) \leq n_p(G)$, όπου το n_p συμβολίζει τον αριθμό των Sylow p-υποομάδων.

7. Έστω D_n η διεδρική ομάδα τάξεως $2n$ (η ομάδα συμμετρίας ενός κανονικού πολυγώνου με n κορυφές). Δείξτε ότι αν ο n είναι περιττός, τότε όλες οι Sylow υποομάδες της D_n είναι κυκλικές. Ισχύει το συμπέρασμα αν ο n είναι άρτιος;

8. Έστω $P_1, \ldots, P_m$ οι Sylow p-υποομάδες μιας πεπερασμένης ομάδας G και S_p η ομάδα μεταθέσεων του συνόλου $\{P_1, \ldots, P_m\}$. Ορίζουμε απεικόνιση $\phi : G \to S_P$ έτσι ώστε $\phi(g)$ είναι η μετάθεση που στέλνει την P_i στην gP_ig^{-1}.

   (i) Δείξτε ότι η ϕ είναι ομομορφισμός και βρείτε τον πυρήνα της.

   (ii) Δείξτε ότι η διεδρική D_n είναι ισόμορφη με υποομάδα της S_n, αν ο n είναι περιττός.

9. Έστω G μη κυκλική πεπερασμένη ομάδα με $|G| < 60$. Δείξτε ότι η G δεν είναι απλή.

10. Δείξτε ότι δεν υπάρχουν απλές ομάδες τάξεως 90, 132, 144 ή 150.

Σκοπός των επόμενων ασκήσεων είναι να δώσουν μια διαφορετική απόδειξη του θεωρήματος του Sylow.

11. Έστω $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, p πρώτος, το σώμα με p στοιχεία, $GL_n(\mathbb{F}_p)$ η ομάδα των αντιστέψιμων $n \times n$ πινάκων επί του $\mathbb{F}_p$ και $UT_n(\mathbb{F}_p)$ η υποομάδα της που αποτελείται από εκείνους τους πίνακες των οποίων τα στοιχεία κάτω της κύριας διαγωνίου είναι μηδέν και κάθε στοιχείο της κύριας διαγωνίου είναι ίσο με 1. Δηλαδή, κάθε πίνακας στην $UT_n(\mathbb{F}_p)$ έχει την ακόλουθη μορφή

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Δείξτε ότι η $UT_n(\mathbb{F}_p)$ είναι Sylow p-υποομάδα της $GL_n(\mathbb{F}_p)$.

[Υπόδειξη: Από το γεγονός ότι ένας τετραγωνικός πίνακας είναι αντιστρέψιμος αν και μόνο αν οι στήλες του είναι γραμμικώς ανεξάρτητες, βρίσκουμε ότι $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.]

12. Έστω H μια Sylow p-υποομάδα μιας πεπερασμένης ομάδας G και K μια υποομάδα της G της οποίας η τάξη είναι πολλαπλάσιο του p. Δείξτε ότι υπάρχει στοιχείο x της G έτσι ώστε η $K \cap xHx^{-1}$ είναι Sylow p-υποομάδα της K.

13. Έστω G ομάδα τάξεως $p^k m$, όπου p πρώτος που δεν διαιρεί τον m. Τότε υπάρχει τουλάχιστον μια Sylow p-υποομάδα της G.

    [Υπόδειξη: Αρκεί να εμφυτεύσετε την G στην $GL_n(\mathbb{F}_p)$, όπου $n = |G|$.]

Κεφάλαιο 4

Γινόμενα Ομάδων

4.1 Ευθέα γινόμενα

Ορισμός 4.1.1. Έστω H και K ομάδες. Θεωρούμε το καρτεσιανό τους γινόμενο, $H \times K$,

$$H \times K = \{(h, k) : h \in H, k \in K\}$$

και το εφοδιάζουμε με την ακόλουθη πράξη

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$$

Η παραπάνω πράξη καθιστά το $H \times K$ ομάδα, την οποία ονομάζουμε **εξωτερικό ευθύ γινόμενο** των H και K.

Το ουδέτερο στοιχείο είναι το

$$(1, 1) = (1_H, 1_K)$$

και

$$(h, k)^{-1} = (h^{-1}, k^{-1})$$

Επίσης, η απεικόνιση $\phi : H \times K \to K \times H$ με $\phi((h, k)) = (k, h)$ είναι ισομορφισμός ομάδων. Δηλαδή, στον σχηματισμό του εξωτερικού ευθέως γινομένου δεν παίζει ρόλο η σειρά των παραγόντων.

Πρόταση 4.1.1. *Έστω $G = H \times K$, το εξωτερικό ευθύ γινόμενο των H και K, $\overline{H} = \{(h, 1) : h \in H\}$ και $\overline{K} = \{(1, k) : k \in K\}$. Τότε $\overline{H} \simeq H, \overline{K} \simeq K$. Επιπλέον*

(i) $\overline{H} \lhd G$ *και* $\overline{K} \lhd G$.

(ii) $G = \overline{H} \cdot \overline{K}$.

(iii) $\overline{H} \cap \overline{K} = 1$.

Απόδειξη. Είναι εύκολο να διαπιστώσουμε ότι οι $\overline{H}, \overline{K}$ είναι υποομάδες της G και ότι οι παρακάτω απεικονίσεις είναι ισομορφισμοί:

$$\overline{H} \xrightarrow{\simeq} H \quad , (h, 1) \mapsto h, \quad \overline{K} \xrightarrow{\simeq} K \quad , (1, k) \mapsto k$$

(i) Έστω $(h,1) \in \overline{H}$ και $g = (h_1, k_1) \in G$. Τότε

$$(h_1,k_1)(h,1)(h_1,k_1)^{-1} = (h_1 h h_1^{-1}, 1) \in \overline{H}$$

Άρα $\overline{H} \lhd G$. Ομοίως, $\overline{K} \lhd G$.

(ii) Έστω $g \in G$. Τότε $g = (h,k) = (h,1)(1,k) \in \overline{H} \cdot \overline{K}$.

(iii) Προφανές.

□

Η Πρόταση 4.1.1 οδηγεί στον ορισμό της έννοιας του εσωτερικού ευθέως γινομένου.

Ορισμός 4.1.2. Μια ομάδα G λέμε ότι είναι το **εσωτερικό ευθύ γινόμενο** των υποομάδων της, H και K, αν ισχύουν τα εξής:

(i) $H \lhd G$ και $K \lhd G$.

(ii) $G = H \cdot K$.

(iii) $H \cap K = 1$.

Πρόταση 4.1.2. *H G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της, H και K, ανν:*

(i) $hk = kh$, για κάθε $h \in H, k \in K$.

(ii) Κάθε $g \in G$ γράφεται κατά μοναδικό τρόπο ως $g = hk$, όπου $h \in H, k \in K$.

Απόδειξη. Υποθέτουμε ότι η G είναι το εσωτερικό ευθύ γινόμενο των H και K.

Έστω $h \in H$ και $k \in K$. Από την κανονικότητα των υποομάδων H, K έπεται ότι $h^{-1}k^{-1}hk \in H$ και $h^{-1}k^{-1}hk \in K$. Άρα, $h^{-1}k^{-1}hk \in H \cap K$, δηλαδή $hkh^{-1}k^{-1} = 1$ και έτσι $hk = kh$.

Από το (ii) του ορισμού, έχουμε ότι κάθε $g \in G$ γράφεται ως $g = hk$, με$h \in H$ και$k \in K$. Μένει να δείξουμε την μοναδικότητα.

Έστω ότι $hk = h_1k_1$, $h, h_1 \in H, k, k_1 \in K$. Τότε, $H \ni h_1^{-1}h = k_1k^{-1} \in K$. Δηλαδή $h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$. Έπεται ότι $h = h_1$ και $k_1 = k$.

Αντίστροφα, έστω ότι ισχύουν τα (i) και (ii). Από το (ii) της πρότασης, κάθε στοιχείο $g \in G$ γράφεται κατά μοναδικό τρόπο ως $g = hk, h \in H, k \in K$. Ιδιαιτέρως, $G = H \cdot K$.

Για την κανονικότητα: Έστω $h_1 \in H$ και $g = hk \in G$. Τότε,

$$gh_1g^{-1} = hkh_1k^{-1}h^{-1} = hh_1kk^{-1}h^{-1} = hh_1h^{-1} \in H$$

Άρα $H \lhd G$. Ομοίως, $K \lhd G$.

Έστω $g \in H \cap K$. Τότε,

$$H \cdot K \ni g \cdot 1 = g = 1 \cdot g \in H \cdot K$$

Από την μοναδικότητα της γραφής, έχουμε ότι $g = 1$. □

Πρόταση 4.1.3. *H G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H και K ανν η απεικόνιση $\phi : H \times K \to G$ από το εξωτερικό γινόμενο των H και K στην G, με $(h,k) \mapsto h \cdot k$ είναι ισομορφισμός.*

Απόδειξη. Αφήνεται ως άσκηση. □

Τα προηγούμενα γενικεύονται για οποιοδήποτε πεπερασμένο πλήθος ομάδων $H_1, H_2, \ldots, H_k$.

Πιο συγκεκριμένα, αν οι $H_1, H_2, \ldots, H_k$ είναι ομάδες, το εξωτερικό τους ευθύ γινόμενο είναι το καρτεσιανό τους γινόμενο

$$G = H_1 \times H_2 \cdots \times H_k$$

με πράξη τον πολλαπλασιασμό κατά "σημείο"

$$(h_1, h_2, \ldots, h_k) \cdot (h_1', h_2', \ldots, h_k') = (h_1 h_1', h_2 h_2', \ldots, h_k h_k')$$

Η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της $H_1, H_2, \ldots, H_k$ αν:

(i) $H_i \lhd G$, για κάθε $i = 1, 2, \ldots, k$.

(ii) $G = H_1 H_2 \cdots H_k$.

(iii) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) = \{1\}$, για κάθε $i = 1, 2, \ldots, k$.

Πρόταση 4.1.4. *Η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $H_1, H_2, \ldots, H_k$ ανν:*

(i) $h_i h_j = h_j h_i$, για κάθε $i \neq j$ και κάθε $h_i \in H_i, h_j \in H_j$.

(ii) Κάθε $g \in G$ γράφεται κατά μοναδικό τρόπο ως $g = h_1 h_2 \cdots h_k$ όπου $h_i \in H_i$, για κάθε $i = 1, 2, \ldots, k$.

Πρόταση 4.1.5. *Η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $H_1, H_2, \ldots, H_k$ ανν η απεικόνιση $\phi : H_1 \times H_2 \cdots \times H_k \to G$, από το εξωτερικό ευθύ γινόμενο των $H_1, H_2, \ldots, H_k$ στην G, με $(h_1, h_2, \ldots, h_k) \mapsto h_1 h_2 \cdots h_k$ είναι ισομορφισμός.*

Έτσι, λοιπόν, Διαπιστώνουμε ότι δεν υπάρχει ουσιαστική διαφορά στις έννοιες εξωτερικό ευθύ γινόμενο και εσωτερικό ευθύ γινόμενο.

Παράδειγμα 4.1.1. Αν οι m και n είναι πρώτοι μεταξύ τους, τότε

$$\mathbb{Z}_m \times \mathbb{Z}_n = \mathbb{Z}_{mn}$$

Πράγματι, έστω ότι $\mathbb{Z}_m = \langle a \rangle, o(a) = m$ και $\mathbb{Z}_n = \langle b \rangle, o(b) = n$. Θεωρούμε το στοιχείο $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

Έστω $\nu = o((a, b))$. Έχουμε ότι $(a, b)^{mn} = (a^{mn}, b^{mn}) = (1, 1) = 1$. Έπεται ότι $o((a, b)) = \nu | mn$, και έτσι $\nu \leq mn$.

Από την άλλη, $(a^\nu, b^\nu) = (a, b)^\nu = 1$, δηλαδή $a^\nu = 1$ και $b^\nu = 1$. Δηλαδή, $m | \nu, n | \nu$ και εφόσον οι m και n είναι πρώτοι μεταξύ τους ισχύει $mn | \nu$, άρα $mn \leq \nu$.

Τελικά, $\nu = mn$ και η υποομάδα που παράγεται από το (a, b) έχει mn στοιχεία, όση είναι και η τάξη της ομάδας $\mathbb{Z}_m \times \mathbb{Z}_n$. Άρα, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (a, b) \rangle = \mathbb{Z}_{mn}$.

Ομοίως, αν $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου p_i διακεκριμένοι πρώτοι, τότε

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

Λήμμα 4.1.1. *Αν $G = H_1 \times H_2 \times \cdots \times H_k$ (εσωτερικό γινόμενο), όπου $(|H_i|, |H_j|) = 1$ για κάθε $i \neq j$ και $H \leq G$, τότε*

$$H = (H_1 \cap H) \times (H_2 \cap H) \times \cdots \times (H_k \cap H)$$

Απόδειξη. Εφόσον $(|H_i|, |H_j|) = 1$, για κάθε $i \neq j$, έχουμε ότι $(|H_i \cap H|, |H_j \cap H|) = 1$ για κάθε $i \neq j$ και έτσι $(H_i \cap H) \cap (H_j \cap H) = \{1\}$.

Επίσης, $H_i \cap H \lhd H$ αφού $H_i \lhd G$. Άρα κάθε γινόμενο $(H_{i_1} \cap H) \cdots (H_{i_\nu} \cap H)$ είναι υποομάδα της G.

Με επαγωγή επί του ν δείχνουμε ότι

(1(ν)) $|(H_{i_1} \cap H) \cdots (H_{i_\nu} \cap H)| = |(H_{i_1} \cap H)| \cdots |(H_{i_\nu} \cap H)|$ για $i_\lambda \neq i_\mu$ και

(2(ν)) $[(H_{i_1} \cap H) \cdots (H_{i_\nu} \cap H)] \cap (H_{i_{\nu+1}} \cap H) = \{1\}$

Για $\nu = 1$ η 1(ν) είναι άμεση και η 2(ν) προκύπτει από τα προηγούμενα σχόλια.

Από την 2($\nu - 1$) και την Άσκηση 2.5.10(?) έπεται η 1(ν), η οποία με τη σειρά της μας δίνει την 2(ν), αφού $(|H_i \cap H|, |H_j \cap H|) = 1$ για κάθε $i \neq j$.

Συνεπώς, για κάθε i έχουμε ότι

$$(H_i \cap H) \cap ((H_1 \cap H) \cdots (H_{i-1} \cap H)(H_{i+1} \cap H) \cdots (H_k \cap H)) = 1$$

Μένει να δείξουμε ότι κάθε $h \in H$ γράφεται ως $h = h_1 h_2 \cdots h_k$, όπου $h_i \in H_i \cap H$.

Εφόσον $G = H_1 \times H_2 \times \cdots \times H_k$, αν $h \in H$, τότε $h = h_1 h_2 \cdots h_k$, για κάποια $h_i \in H_i$. Αρκεί να δείξουμε ότι $h_i \in H$ για κάθε i. Αν κάποιο $h_i = 1$, τότε $h_i \in H$. Ας υποθέσουμε, λοιπόν, ότι $h_i \neq 1$, για κάθε i.

Έστω $m_i = o(h_i)$ και $n_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k$. Τότε $(m_i, m_j) = 1$ για $i \neq j$m αφού $(|H_i|, |H_j|) = 1$, το οποίο συνεπάγεται ότι $(m_i, n_i) = 1$ για κάθε i.

Εφόσον τα h_i μετατίθενται (ως στοιχεία παραγόντων ευθέως γινομένου) και m_j διαιρέτης του n_i για κάθε $j \neq i$, έχουμε ότι

$$h^{n_i} = h_1^{n_i} h_2^{n_i} \cdots h_i^{n_i} \cdots h_k^{n_i} = h_i^{n_i}$$

Όμως, $h_i^{n_i} \neq 1$ γιατί $m_i \nmid n_i$.

Αφού $(m_i, n_i) = 1$, υπάρχουν $k_i, \lambda_i \in \mathbb{Z}$ έτσι ώστε $1 = k_i m_i + \lambda_i n_i$. Έτσι

$$h_i = (h_i^{m_i})^{k_i} (h_i^{n_i})^{\lambda_i} = (h^{n_i})^{\lambda_i} \in \langle h \rangle \subseteq H$$

□

Θεώρημα 4.1.1. *Έστω G πεπερασμένη ομάδα. Τα επόμενα είναι ισοδύναμα:*

(i) Η G είναι το ευθύ γινόμενο των Sylow υποομάδων της.

(ii) Κάθε μεγιστική υποομάδα της G είναι κανονική στην G.

(iii) Κάθε Sylow υποομάδα της G είναι κανονική στην G.

Απόδειξη. Έστω $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, όπου p_i πρώτοι διαφορετικοί μεταξύ τους και έστω P_i Sylow p_i-υποομάδα της G για κάθε i.
$(i) \Rightarrow (ii)$: Εφόσον η G είναι το ευθύ γινόμενο των Sylow υποομάδων της, δηλαδή $G = P_1 \times P_2 \times \cdots \times P_k$, όπου κάθε P_i είναι κανονική και άρα μοναδική.

Έστω H μεγιστική υποομάδα της G. Εφόσον $(|P_i|, |P_j|) = 1 = (p_i^{n_i}, p_j^{n_j})$ για κάθε $i \neq j$, από το προηγούμενο λήμμα έχουμε ότι

$$H = (P_1 \cap H) \times \cdots \times (P_j \cap H) \times \cdots \times (P_k \cap H)$$

Από την μεγιστικότητα της υποομάδας H, έπεται ότι υπάρχει ακριβώς ένας δείκτης i με $P_i \cap H \neq P_i$, διαφορετικά θα είχαμε

$$\begin{aligned} H &\subseteq P_1 \times \cdots \overbrace{(P_{i_1} \cap H)}^{<P_{i_1}} \times \cdots \times \overbrace{(P_{i_2} \cap H)}^{<P_{i_2}} \times \cdots \times (P_k \cap H) \\ &\subset P_1 \times \cdots \times P_{i_1} \times \cdots (P_{i_2} \cap H) \times \cdots \times P_k \subset G \end{aligned}$$

άτοπο, διότι η H είναι μεγιστική.

Άρα

$$H = P_1 \times \cdots \times P_{i-1} \times (P_i \cap H) \times P_{i+1} \times \cdots \times P_k$$

και $P_i \cap H < P_i$.

Για τον ίδιο λόγο, την μεγιστικότητα της H, η $P_i \cap H$ είναι μεγιστική υποομάδα της p_i-ομάδας P_i.

Από την Άσκηση 3.3 $P_i \cap H \lhd P_i$. Έχουμε, λοιπόν, ότι $P_i \cap H \lhd P_i$ και $P_1 \lhd G$. Από την Άσκηση 1.12, έπεται ότι $P_1(P_i \cap H) \lhd P_1 P_i$ αν $i \neq 1$. Αν $i = 1$ πολλαπλασιάζουμε με P_2.

Πολλαπλασιάζοντας διαδοχικά με τις Sylow υποομάδες διαφορετικές από P_i θα έχουμε

$$H = P_1 \cdots P_{i-1}(P_i \cap H)P_{i+1} \cdots P_k \lhd P_1 P_2 \cdots P_i \cdots P_k = G.$$

Δηλαδή $H \lhd G$.

$(ii) \Rightarrow (iii)$: Έστω P Sylow υποομάδα της G με $N_G(P) < G$. Τότε υπάρχει μεγιστική υποομάδα $H \leq G$ με $N_G(P) \leq H$ -ενδέχεται $N_G(P) = H$- και

$$P \leq N_G(P) \leq H < G$$

Από την υπόθεση $H \lhd G$. Έστω $g \in G$. Τότε $gPg^{-1} \subseteq gHg^{-1} = H$.

Δηλαδή, για κάθε $g \in G$ οι P, gPg^{-1} είναι Sylow p-υποομάδες της H. Συνεπώς, υπάρχει $h \in H$ με $hgPg^{-1}h^{-1} = P \Rightarrow hg \in N_G(P) \subseteq H \Rightarrow g \in H$, το οποίο είναι άτοπο γιατί $H < G$.

Άρα $N_G(P) = G$ και $P \lhd G$.

$(iii) \Rightarrow (i)$: Αφού κάθε $P_i \lhd G$, το γινόμενο $P_1 P_2 \cdots P_k$ είναι υποομάδα της G. Όπως και στο Λήμμα 4.1.1

$$|P_1 P_2 \cdots P_k| = |P_1||P_2| \cdots |P_k| = |G|$$

και

$$P_i \cap P_1 \cdots P_{i-1} P_{i+1} \cdots P_k = \{1\}$$

Άρα $G = P_1 \times P_2 \times \cdots \times P_k$. □

Πόρισμα 4.1.1. *Έστω G πεπερασμένη αβελιανή ομάδα. Τότε, η G είναι το ευθύ γινόμενο των Sylow υποομάδων της.*

4.2 Πεπερασμένα παραγόμενες αβελιανές ομάδες

Για αβελιανές ομάδες χρησιμοποιούμε $+$ αντί για $\cdot$, δηλαδή προσθετικό συμβολισμό, και 0 αντί για 1. Αν η G είναι αβελιανή και $\{x_1, x_2, \ldots, x_k\} \subseteq G$, τότε

$$\langle x_1, x_2, \ldots, x_k \rangle = \left\{ \sum_{i=1}^{k} m_i x_i : m_i \in \mathbb{Z} \right\}$$

Εδώ το ευθύ γινόμενο θα είναι ευθύ άθροισμα κ.ο.κ.

Λήμμα 4.2.1. *Υποθέτουμε ότι η G είναι αβελιανή και ότι παράγεται από το σύνολο $\{x_1, x_2, \ldots, x_k\}$. Αν $\lambda_1, \lambda_2, \ldots, \lambda_k$ ακέραιοι με $(\lambda_1, \lambda_2, \ldots, \lambda_k) = 1$, τότε υπάρχει σύνολο γεννητόρων $\{y_1, y_2, \ldots, y_k\}$ της G τέτοιο ώστε*

$$y_1 = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k$$

Απόδειξη. Αλλάζοντας τα πρόσημα των x_i και λ_i μπορούμε να υποθέσουμε ότι $\lambda_i \geq 0$.

Χρησιμοποιούμε επαγωγή επί του $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_k$.

Αν $\lambda = 1$, τότε ακριβώς ένα λ_i θα είναι μη μηδενικό και αυτό ίσο με 1. Σε αυτήν την περίπτωση $y_1 = \lambda_i x_i = x_i$ και το $\{y_1, y_2, \ldots, y_k\}$ προκύπτει από μια αναδιάταξη του $\{x_1, x_2, \ldots, x_k\}$.

Αν $\lambda > 1$, τότε υπάρχουν τουλάχιστον 2 μη-μηδενικοί όροι του αθροίσματος λ. Έστω χωρίς βλάβη της γενικότητας ότι $\lambda_1 \geq \lambda_2 > 0$.

- Το $\{x_1, x_1 + x_2, x_3, \ldots, x_k\}$ είναι ένα σύνολο γεννητόρων της G
- $(\lambda_1 - \lambda_2, \lambda_2, \lambda_3, \ldots, \lambda_k) = 1$
- $(\lambda_1 - \lambda_2) + \lambda_2 + \lambda_3 + \cdots + \lambda_k < \lambda_1 + \lambda_2 + \cdots + \lambda_k$

Από την επαγωγική υπόθεση υπάρχει σύνολο γεννητόρων $\{y_1, y_2, \ldots, y_k\}$ της G τέτοιο ώστε $y_1 = (\lambda_1 - \lambda_2)x_1 + \lambda_2(x_1 + x_2) + \cdots + \lambda_k x_k = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k$. □

Θεώρημα 4.2.1. *Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι ευθύ άθροισμα κυκλικών ομάδων.*

Απόδειξη. Με επαγωγή επί του πλήθους k των γεννητόρων ενός πεπερασμένου συνόλου γεννητόρων της G.

Αν η G παράγεται από ένα στοιχείο, τότε είναι κυκλική.

Έστω $k > 1$. Από όλα τα σύνολα γεννητόρων της G με k το πλήθος στοιχεία επιλέγουμε ένα, έστω $\{x_1, x_2, \ldots, x_k\}$, τέτοιο ώστε η τάξη $o(x_1)$ να είναι η μικρότερη δυνατή -ενδέχεται η τάξη να είναι άπειρη.

Αν $o(x_1) = 1 \Leftrightarrow x_1 = 0$, τότε το $\{x_2, \ldots, x_k\}$ παράγει την G και το συμπέρασμα έπεται από την επαγωγική υπόθεση.

Έστω ότι $o(x_1) > 1$. Θα δείξουμε ότι η G είναι το ευθύ άθροισμα των υποομάδων $\langle x_1 \rangle$ και $\langle x_2, \ldots, x_k \rangle$ το οποίο από επαγωγική υπόθεση μας δίνει το συμπέρασμα.

Έχουμε ότι $\langle x_1 \rangle \lhd G, \langle x_2, \ldots, x_k \rangle \lhd G$, γιατί η G είναι αβελιανή και προφανώς $G = \langle x_1 \rangle \cdot \langle x_2, \ldots, x_k \rangle$.

Μένει να δείξουμε ότι $\langle x_1 \rangle \cap \langle x_2, \ldots, x_k \rangle = 0$. Ας υποθέσουμε ότι $\langle x_1 \rangle \cap \langle x_2, \ldots, x_k \rangle \neq 0$. Τότε υπάρχουν $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ ώστε $m_1 x_1 + m_2 x_2 + \cdots + m_k x_k = 0$ και $m_1 x_1 \neq 0$. Αφού $m_1 x_1 \neq 0$, η τάξη του x_1 δεν διαιρεί τον ακέραιο m_1. Μπορούμε να υποθέσουμε ότι $m_1 \in \mathbb{N}$, αφού $\sum_{i=1}^{k} m_i x_i = 0 \Leftrightarrow \sum_{i=1}^{k} (-m_i x_i) = 0$. Διαιρώντας τον m_1 με $o(x_1)$ μπορούμε, επίσης, να υποθέσουμε ότι $0 < m_1 < o(x_1)$.

Έστω $d = (m_1, m_2, \ldots, m_k)$ και $\lambda_i = \frac{m_i}{d}$. Τότε $(\lambda_1, \lambda_2, \ldots, \lambda_k) = 1$. Από το Λήμμα 4.2.1 υπάρχει σύνολο γεννητόρων της G, $\{y_1, y_2, \ldots, y_k\}$, τέτοιο ώστε $y_1 = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k$. Όμως $dy = d\lambda_1 x_1 + d\lambda_2 x_2 + \cdots + d\lambda_k x_k = m_1 x_1 + m_2 x_2 + \cdots + m_k x_k = 0$.

Έπεται ότι $o(y) \leq d \leq m_1 < o(x_1)$, το οποίο αντιφάσκει στην υπόθεση ότι η τάξη $o(x_1)$ είναι η μικρότερη δυνατή. □

Έχουμε δει ότι

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} = \mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{a_k}}$$

όπου p_i διακεκριμένοι πρώτοι και $m = p_1^{a_1} \cdots p_k^{a_k}$. Συνεπώς, έχουμε το ακόλουθο:

Θεώρημα 4.2.2. *Κάθε μη τετριμμένη πεπερασμένα παραγόμενη αβελανή ομάδα G είναι ευθύ άθροισμα (ή γινόμενο) άπειρων κυκλικών και κυκλικών με τάξεις δυνάμεις πρώτων.*

Δηλαδή,

$$G = \underbrace{\mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}}_{\text{ομάδα στρέψης}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{\text{ομάδα ελευθέρας στρέψης}}$$

όπου p_i πρώτοι.

Παρατήρηση 4.2.1. Αν μια πεπερασμένα παραγόμενη αβελιανή ομάδα G είναι το ευθύ άθροισμα (ή γινόμενο) κυκλικών ομάδων τάξεων $p_1^{r_1}, \ldots, p_k^{r_k}$ και s το πλήθος άπειρων κυκλικών ομάδων, όπου $p_1, \ldots, p_k$ πρώτοι, $p_1 \leq p_2 \leq \ldots \leq p_k$ και $r_i \leq r_{i+1}$ αν $p_i = p_{i+1}$, τότε η διατεταγμένη $(k+1)$-άδα $(p_1^{r_1} p_2^{r_2}, \ldots, p_k^{r_k}, s)$ λέγεται **τύπος** της G. Μπορεί να δειχθεί ότι ο τύπος της G είναι μονοσήμαντα ορισμένος (Ασκήσεις 11,12).

Παράδειγμα 4.2.1. Να βρεθούν (ως προς ισομορφισμό) όλες οι αβελιανές ομάδες τάξεως 72.

Έχουμε ότι $72 = 2^3 \cdot 3^2$. Μια πεπερασμένη αβελιανή ομάδα είνα το ευθύ γινόμενο των Sylow υποομάδων της. Συνεπώς, αν H η Sylow 2-υποομάδα της G και K η Sylow 3-υποομάδα της G, τότε $G = H \times K$.

- $|H| = 2^3$ και $H = \mathbb{Z}_{2^{a_1}} \times \cdots \times \mathbb{Z}_{2^{a_k}}$. Άρα $|H| = 2^3 = 2^{a_1 + \cdots + a_k} \Rightarrow a_1 + \cdots + a_k = 3$. Έφόσον $3 = 1+1+1 = 1+2 = 0+3$, για την H υπάρχουν οι εξής δυνατές περιπτώσεις:

$$H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{ή} \quad \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \quad \text{ή} \quad \mathbb{Z}_{2^3}$$

- Όμοια, αφού $2 = 1 + 1 = 0 + 2$,

$$K = \mathbb{Z}_3 \times \mathbb{Z}_3 \quad \text{ή} \quad \mathbb{Z}_{3^2}$$

Τελικά, υπάρχουν 6 μη ισόμορφες αβελιανές ομάδες τάξεως 72:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2},$$

$$\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2},$$

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_3 \times \mathbb{Z}_3, \quad \mathbb{Z}_{2^3} \times \mathbb{Z}_{3^2}$$

Παράδειγμα 4.2.2. Κάθε ομάδα τάξεως 45 είναι αβελιανή.

Έστω G ομάδα με $|G| = 45 = 3^2 \cdot 5$. Έστω n_3 το πλήθος των Sylow 3-υποομάδων της G και n_5 το πλήθος των Sylow 5-υποομάδων της G.

Γνωρίζουμε ότι $n_5 | 3^2 \Rightarrow n_5 = 1$ ή 3 ή 9 και $n_5 \equiv 1 \pmod 5 \Rightarrow n_5 = 1$. Άρα, υπάρχει μόνο μια Sylow 5-υποομάδα της G, έστω P, η οποία λόγω μοναδικότητας θα είναι κανονική -$P \lhd G$.

Ομοίως, $n_3 | 5 \Rightarrow n_3 = 1$ ή 5 και $n_3 \equiv 1 \pmod 3 \Rightarrow n_3 = 1$. Συνεπώς, υπάρχει μοναδική Sylow 3-υποομάδα της G, έστω Q, η οποία λόγω μοναδικότητας θα είναι κανονική -$Q \lhd G$.

Αφού κάθε Sylow υποομάδα της G είναι κανονική, η G θα είναι το ευθύ γινόμενο των Sylow υποομάδων της, δηλαδή

$$G = P \times Q$$

όπου $|P| = 5$ και $|Q| = 3^2$.

Εφόσον $|P| = 5$, $P = \mathbb{Z}_5$. Ιδιαιτέρως, η P είναι αβελιανή. Η Q είναι επίσης αβελιανή, αφού η τάξη της είναι τετράγωνο πρώτου. Όπως στο προηγούμενο Παράδειγμα, έπεται ότι $Q = \mathbb{Z}_9$ ή $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Έπεται ότι η G είναι αβελιανή ως ευθύ γινόμενο αβελιανών ομάδων.

Μάλιστα,

$$G = \mathbb{Z}_5 \times \mathbb{Z}_{3^2} \quad \text{ή} \quad \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

Παράδειγμα 4.2.3. Περιγράψτε ως προς ισομορφισμό όλες τις ομάδες τάξεως 425.

Έχουμε $425 = 5^2 \cdot 17$. Έστω K Sylow 17-υποομάδα της G και N Sylow 5-υποομάδα της G.

Γνωρίζουμε ότι $n_{17}|5^2 \Rightarrow n_{17} = 1$ ή 5 ή 5^2 και $n_{17} \equiv 1 \pmod{17} \Rightarrow n_{17} = 1$. Άρα, υπάρχει μοναδική Sylow 17-υποομάδα της G και είναι κανονική λόγω μοναδικότητας.

Όμοια, $n_5|17 \Rightarrow n_5 = 1$ ή 17 και $n_5 \equiv 1 \pmod{5} \Rightarrow n_5 = 1$. Άρα, υπάρχει μοναδική Sylow 5-υποομάδα της G και είναι κανονική λόγω μοναδικότητας.

Αφού οι Sylow υποομάδες της G είναι κανονικές, η G είναι το ευθύ γινόμενό τους. Δηλαδή,

$$G = K \times N.$$

Αφού $|K| = 17 \Rightarrow K = \mathbb{Z}_{17}$ και αφού $|N| = 5^2$, η N είναι αβελιανή. Όπως και πριν, η G είναι αβελιανή ως γινόμενο αβελιανών ομάδων και $N = \mathbb{Z}_5 \times \mathbb{Z}_5$ ή $\mathbb{Z}_{5^2}$, άρα

$$G = \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{17} \quad \text{ή} \quad \mathbb{Z}_{5^2} \times \mathbb{Z}_{17}$$

4.3 Ημιευθέα γινόμενα

Ορισμός 4.3.1. Μια ομάδα G λέμε ότι είναι το **ημιευθύ γινόμενο** των υποομάδων της H και N αν:

(i) $N \lhd G$,

(ii) $N \cap H = 1$,

(iii) $G = NH\ (= HN)$.

Συμβολίζουμε με $G = N \rtimes H$ και λέμε επίσης ότι η G αναλύεται ως ημιευθύ γινόμενο των H και N.

Παρατήρηση 4.3.1. Όπως στην περίπτωση των ευθέων γινομένων, είναι εύκολο να δούμε ότι οι ιδιότητες (ii) και (iii) είναι ισοδύναμες με την ακόλουθη πρόταση: Κάθε στοιχείο g της G γράφεται κατά μοναδικό τρόπο ως $g = n \cdot h$, όπου $n \in N$, $h \in N$.

Παραδείγματα 4.3.1. (i) Κάθε ευθύ γινόμενο είναι ημιευθύ γινόμενο.

(ii) $S_n = A_n \rtimes \langle(12)\rangle = A_n \rtimes \mathbb{Z}_2$.

(iii) $D_n = \langle\alpha\rangle \rtimes \langle\beta\rangle = \mathbb{Z}_n \rtimes \mathbb{Z}_2$, όπου α στροφή τάξεως n και β ανάκλαση.

Αν $G = N \rtimes H$, τότε η G δεν "καθορίζεται" πλήρως από τις H και N. Πράγματι $D_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ και $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$, ενώ $D_3 \ncong \mathbb{Z}_6$ (γιατί;).

Παίζει λοιπόν ρόλο το πως πολλαπλασιάζονται τα στοιχεία της H με τα στοιχεία της N. Έστω λοιπόν ότι $G = N \rtimes H$ και $g_1, g_2 \in G$. Τότε υπάρχουν μοναδικά $n_1, n_2 \in N$ και $h_1, h_2 \in H$ έτσι ώστε $g_1 = n_1 h_1$ και $g_2 = n_2 h_2$. Συνεπώς,

$$g_1 g_2 = n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\in N} h_1 h_2$$

Αν θεωρήσουμε τον περιορισμό του εσωτερικού αυτομορφισμού τ_{h_1} στην κανονική υποομάδα N, τότε $g_1 g_2 = n_1 \tau_{h_1}(n_2) \cdot h_1 h_2$. Έτσι έχουμε τον ομομορφισμό $\phi : H \to \mathrm{Aut}(N)$ με $\phi(h) = \tau_h$ και $g_1 g_2 = n_1 \phi(h_1)(n_2) \cdot h_1 h_2$.

Αντίστροφα, έστω H και N ομάδες και $\phi : H \to \mathrm{Aut}(N)$ ομομορφισμός. Στο καρτεσιανό γινόμενο $N \times H$ ορίζουμε πολλαπλασιασμό ως εξής:

$$(n_1, h_1) \cdot (n_2, h_2) = \big(n_1 \cdot \phi(h_1)(n_2), h_1 h_2\big).$$

Είναι εύκολο να διαπιστώσουμε -αφήνεται ως άσκηση- ότι με την παραπάνω πράξη το σύνολο $G = N \times H$ γίνεται ομάδα η οποία λέγεται το (εξωτερικό) **ημιευθύ γινόμενο** των ομάδων N, H και συμβολίζεται με $G = N \rtimes_\phi H$ (για να υποδηλώσουμε την εξάρτηση από τον ομομορφισμό ϕ). Επιπλέον, αν θεωρήσουμε $\widetilde{H} = \{(h, 1) : h \in H\}$ και $\widetilde{N} = \{(n, 1) : n \in N\}$, τότε:

(i) οι $\widetilde{H}$ και $\widetilde{N}$ είναι υποομάδες της $G = N \rtimes_\phi H$ με $\widetilde{N} \lhd N \rtimes_\phi H$,

(ii) $\widetilde{H} \simeq H$, $\widetilde{N} \cong N$, και

(iii) $N \rtimes_\phi H \simeq \widetilde{N} \rtimes \widetilde{H}$.

Παρατηρήσεις 4.3.1. (i) Ο προηγούμενος ισομορφισμός μας λέει ότι επί της ουσίας δεν υπάρχει διαφορά μεταξύ εξωτερικού ημιευθέως γινομένου και (εσωτερικού;) ημιευθέως γινομένου.

(ii) Στην περίπτωση του ευθέως γινομένου ο ομομορφισμός ϕ είναι ο τετριμμένος ομομορφισμός και αντίστροφα. Έτσι το (εξωτερικό) ημιευθύ γινόμενο είναι ευθύ αν και μόνο αν ο αντίστοιχος ομομορφισμός είναι ο τετριμμένος.

Εφαρμογή 4.3.1. Υπάρχουν 5 ομάδες τάξεως $20 = 2^2 5$ (ως προς ισομορφισμό).

Πράγματι, έστω G μια ομάδα τάξεως 20. Από τα θεωρήματα του Sylow εύκολα διαπιστώνουμε ότι υπάρχει μοναδική, άρα κανονική, 5-Sylow υποομάδα $Q = \langle b \rangle \simeq \mathbb{Z}_5$. Αν P είναι μια 2-Sylow υποομάδα της G, τότε $P \cap Q = 1$ και άρα η G είναι το ημιευθύ γινόμενο των P και Q.

Ως εκ' τούτου η ταξινόμηση των ομάδων τάξεως 20, ανάγεται στην εύρεση των δυνατών ομομορφισμών ϕ της P στην $\mathrm{Aut}(Q) = U(\mathbb{Z}_5) \simeq \mathbb{Z}_4$. Υπάρχουν δύο περιπτώσεις: είτε $P \simeq \mathbb{Z}_4$, είτε $P \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Περίπτωση 1: $P \simeq \mathbb{Z}_4$. Εφόσον P κυκλική, υπάρχει στοιχείο a τάξεως 4 τέτοιο ώστε $P = \langle a \rangle$ και υπάρχουν τρεις δυνατότητες:

(i) Το στοιχείο a απεικονίζεται σε στοιχείο τάξεως 4 στην $\mathrm{Aut}(Q)$ (π.χ. $b \mapsto b^2$) και έτσι ϕ μονομορφισμός. Αυτό σημαίνει ότι η εικόνα της P είναι υποομάδα τάξεως 4 στην $\mathrm{Aut}(Q)$, η οποία ως κυκλική περιέχει μοναδική υποομάδα τάξεως 4. Από την Άσκηση 18, έπεται ότι σε αυτήν την περίπτωση τα δυνατά ημιευθέα γινόμενα είναι ισομορφικά.

(ii) Το στοιχείο a απεικονίζεται σε στοιχείο τάξεως 2 στην $\mathrm{Aut}(Q)$. Τότε ο αντίστοιχος πυρήνας είναι μη-τετριμμένος και, όπως πριν, υπάρχει μόνο μια δυνατότητα για την εικόνα του a: $b \mapsto b^{-1}$. Έτσι έχουμε πάλι μόνο ένα ημιευθύ γινόμενο το οποίο όμως δεν είναι ισόμορφο με το προηγούμενο λόγω της Άσκησης 17. Πιο αναλυτικά, στο δεύτερο ημιευθύ γινόμενο υπάρχει μη-τετριμμένο στοιχείο της P, στοιχείο του πυρήνα, που μετατίθεται με κάθε στοιχείο της Q, ενώ στο πρώτο όχι, αφού έχουμε μονομορφισμό.

(iii) Το στοιχείο a απεικονίζεται στην μονάδα. Δηλαδή έχουμε τον τετριμμένο ομομορφισμό. Το αντίστοιχο ημιευθύ γινόμενο είναι το ευθύ γινόμενο και έτσι λαμβάνουμε την $\mathbb{Z}_4 \times \mathbb{Z}_5$ η οποία είναι η κυκλική ομάδα τάξεως 20.

Περίπτωση 2: $P \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Έστω $P = \langle a, c \rangle$, όπου a και c στοιχεία τάξεως 2. Σε αυτή την περίπτωση η P απεικονίζεται στην μοναδική υποομάδα τάξεως 2 της $\mathrm{Aut}(Q)$ ή στην τετριμμένη υποομάδα.

Αν η P απεικονίζεται στην μοναδική υποομάδα τάξεως 2 (π.χ. τα a, c απεικονίζονται στο στοιχείο τάξεως 2), τότε, όπως πριν, για κάθε δυνατή επιλογή του ομομορφισμού έχουμε ένα μόνο ημιευθύ γινόμενο (ως προς ισομορφισμό). Στην περίπτωση που η P απεικονίζεται στην τετριμμένη υποομάδα, το αντίστοιχο ημιευθύ γινόμενο είναι ευθύ γινόμενο και η ομάδα που προκύπτει είναι η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.
Παρατηρούμε ότι από τις πέντε παραπάνω ομάδες μόνο οι δύο είναι αβελιανές.

4.4 Ασκήσεις

1. (i) Αν $M \lhd G$ και $N \lhd K$, τότε $M \times N \lhd G \times K$ και $(G \times K)/(M \times N) \simeq G/M \times K/N$. Γενικεύστε για πεπερασμένο πλήθος παραγόντων.
   (ii) Δείξτε ότι αν $H, K \lhd G$ και $G = HK$, τότε $G/(H \cap K) = H/(H \cap K) \times K/(H \cap K)$.
   (iii) Αν $H, K \lhd G$, τότε η $G/(H \cap K)$ είναι ισόμορφη με υποομάδα της $G/H \times G/K$.

2. Υποθέτουμε ότι $G = H \times K$.
   (i) Δείξτε ότι $H \simeq K$ αν και μόνο αν υπάρχει υποομάδα M της G τέτοια ώστε $G = HM = KM$ και $H \cap M = K \cap M = 1$.
   (ii) Αν $H \leq \Lambda \leq G$, τότε $\Lambda = H \times (K \cap \Lambda)$.

3. Έστω $G = H_1 \times H_2 \times \cdots \times H_n$. Δείξτε ότι $Z(G) = Z(H_1) \times Z(H_2) \times \cdots \times Z(H_n)$.

4. Έστω H μια ελαχιστική μη τετριμμένη κανονική υποομάδα μιας πεπερασμένης ομάδας G. Τότε $H \simeq H_1 \times H_2 \times \cdots \times H_k$, όπου H_i είναι ισόμορφες απλές ομάδες.

5. Αν η G είναι πεπερασμένη αβελιανή και $|G| = n$, τότε για κάθε διαιρέτη m του n η G περιέχει υποομάδα τάξεως m.

6. (i) Πόσες αβελιανές ομάδες υπάρχουν (ως προς ισομορφισμό) τάξεως 231 ή 432;
   (ii) Θεωρώντας δεδομένο ότι υπάρχουν 14 (ως προς ισομορφισμό) ομάδες τάξεως 81, βρείτε το πλήθος των ομάδων (ως προς ισομορφισμό) τάξεως 891.

7. Υποθέτουμε ότι η G είναι μια πεπερασμένη ομάδα της οποίας όλες οι μεγιστικές υποομάδες είναι απλές και κανονικές. Δείξτε ότι η G είναι αβελιανή και $|G| = 1, p, p^2$ ή pq, όπου p και q πρώτοι.

   [Υπόδειξη: Αν υπάρχει μοναδική μεγιστική υποομάδα της G, τότε η G είναι κυκλική.]

8. Αν οι G και H είναι πεπερασμένες ομάδες με $(|G|, |H|) = 1$, τότε $\mathrm{Aut}(G \times H) \simeq \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

9. (i) Δείξτε ότι το σύνολο των στοιχείων πεπερασμένης τάξης μιας αβελιανής ομάδας G, είναι υποομάδα της G, συμβ: $T(G)$, και κάθε στοιχείο της $G/T(G)$ είναι απείρου τάξης.

   (ii) Έστω G και H αβελιανές ομάδες. Αν $G \simeq H$, τότε $T(G) \simeq T(H)$ και $G/T(G) \simeq H/T(H)$.

10. Δύο πεπερασμένες αβελιανές ομάδες G και H είναι ισόμορφες αν και μόνο αν, για κάθε πρώτο p, οι G και H έχουν ισόμορφες Sylow p-υποομάδες.

11. Για μια αβελιανή ομάδα G και κάθε θετικό ακέραιο n ορίζουμε (χρησιμοποιώντας προσθετικό συμβολισμό)
$$nG = \{ng : g \in G\}$$
και
$$G[n] = \{g \in G : ng = 0\}$$
Δείξτε τα εξής:

   (i) Οι nG και $G[n]$ είναι υποομάδες της G.

   (ii) Αν G και H αβελιανές, τότε $n(G \times H) \simeq nG \times nH$ και $(G \times H)[n] = G[n] \times H[n]$.

   (iii) $n\mathbb{Z}_m \simeq \mathbb{Z}_k$, όπου $k = \frac{m}{(n,m)}$ και $\mathbb{Z}_m[n] \simeq \mathbb{Z}_{(n,m)}$.

   (iv) Αν η G είναι πεπερασμένη αβελιανή ομάδα και q πρώτος που δεν διαιρεί την τάξη της G, τότε $qG = G$.

   (v) Αν η G είναι πεπερασμένη αβελιανή p-ομάδα, τότε το $G[p]$ είναι διανυσματικός χώρος επί του $\mathbb{Z}_p$ πεπερασμένης διάστασης.

   (vi) Αν $G = \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \cdots \times \mathbb{Z}_{p^{m_r}}$, όπου p πρώτος, τότε $pG = \mathbb{Z}_{p^{m_1-1}} \times \mathbb{Z}_{p^{m_2-1}} \times \cdots \times \mathbb{Z}_{p^{m_r-1}}$

12. Έστω G πεπερασμένα παραγόμενη αβελιανή ομάδα και
$$G = \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_k^{m_k}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n}$$
όπου p_i πρώτοι όχι απαραιτήτως διαφορετικοί μεταξύ τους. Δείξτε ότι:

   (i) Το πλήθος n των παραγόντων που είναι άπειρες κυκλικές είναι πλήρως καθορισμένο από την G.

   (ii) Το πλήθος n_p των κυκλικών παραγόντων που έχουν τάξη μια δύναμη του πρώτου p είναι πλήρως καθορισμένο από την G.
   [Υπόδειξη: $n_p = \dim_{\mathbb{Z}_p} G_p[p]$, όπου G_p η Sylow p-υποομάδα της G.]

   (iii) Οι δυνάμεις $p_i^{m_i}$ είναι πλήρως καθορισμένες από την G.

13. Μια κυκλική ομάδα τάξεως p^2, όπου p πρώτος, δεν αναλύεται ως ημιευθύ γινόμενο.

14. Κάθε ομάδα G τάξεως pq, όπου p και q πρώτοι διαφορετικοί μεταξύ τους, είναι ημιευθύ γινόμενο κυκλικών υποομάδων τάξεως p και q, αντίστοιχα.

15. Αν $G = N \rtimes H$, τότε $G/N \simeq H$.

16. Η ομάδα $G = N \rtimes_\phi H$ δεν είναι αβελιανή, αν ο ϕ δεν είναι τετριμμένος.

17. Αν $G = N \rtimes_\phi H$, τότε ο πυρήνας $\ker\phi$ αποτελείται από τα στοιχεία της $\widetilde{H}$ που μετατίθεται με κάθε στοιχείο της υποομάδας $\widetilde{N}$, δηλαδή $\ker\phi = C_{\widetilde{H}}(\widetilde{N})$.

18. Έστω K κυκλική ομάδα, H τυχαία ομάδα και $\varphi_1, \varphi_2 : K \to \mathrm{Aut}(H)$ ομομορφισμοί έτσι ώστε οι εικόνες $\varphi_1(K)$ και $\varphi_2(K)$ είναι συζυγείς υποομάδες της $\mathrm{Aut}(H)$. Αν η K είναι άπειρη υποθέτουμε επιπλέον ότι οι ομομορφισμοί φ_1 και φ_2 είναι 1-1. Να δειχθεί ότι $H \rtimes_{\varphi_1} K \simeq H \rtimes_{\varphi_2} K$.

    [Υπόδειξη: Έστω $K = \langle x\rangle$. Εφόσον $\varphi_1(K)$ και $\varphi_2(K)$ συζυγείς, υπάρχει $\sigma \in \mathrm{Aut}(H)$ και ακέραιος a έτσι ώστε $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$, για κάθε $k \in K$. Το στοιχείο $\varphi_2(x)$ είναι γεννήτορας της $\varphi_2(K)$. Έτσι στην περίπτωση που η K είναι πεπερασμένη έχουμε ότι $(a, |\varphi_2(K)|) = 1$. Χρησιμοποιώντας την 'σκηση ?, μπορούμε να υποθέσουμε επιπλέον ότι $(a, |K|) = 1$. Άρα υπάρχει ακέραιος b τέτοιος ώστε $(x^a)^b = x$. Αν K άπειρη, τότε υπάρχει ακέραιος b τέτοιος ώστε $\sigma^{-1}\varphi_2(k)\sigma = \varphi_1(k)^b$, για κάθε $k \in K$. Το 1-1 μας δίνει πάλι ότι $(k^a)^b = k$ για κάθε $k \in K$. Η απεικόνιση $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ με $\psi(h,k) = \big((\sigma(h), k^a)\big)$ είναι ισομορφισμός με αντίστροφο $\phi : H \rtimes_{\varphi_2} K \to H \rtimes_{\varphi_1} K$, $\psi(h,k) = \big((\sigma^{-1}(h), k^b)\big)$.]

    Χρησιμοποιώντας την προηγούμενη άσκηση, έχουμε την ακόλουθη (σε συνέχεια της Άσκησης 14):

19. Έστω p και q πρώτοι με $p > q$.

    (i) Αν $p \not\equiv 1 \,(\mathrm{mod}\, q)$, τότε κάθε υποομάδα τάξεως pq είναι κυκλική.

    - (ii)] Αν $p \equiv 1 \,(\mathrm{mod}\, q)$, υπάρχουν δύο (ως προς ισομορφισμό) ομάδες τάξεως pq: η κυκλική $\mathbb{Z}_{pq}$ και μια μη αβελιανή $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$.

    [Υπόδειξη: Υπάρχει μη τετριμμένος ομομορφισμός $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p) \simeq \mathbb{Z}_{p-1}$ αν και μόνο αν ο q διαιρεί τον $p-1$.]

20. Να βρεθεί ο μικρότερος περιττός n για τον οποίο υπάρχει μη αβελιανή ομάδα τάξεως n.

    [Υπόδειξη: Είναι το 21 γιατί το 3 διαιρεί το $7-1$.]

21. Να δειχθεί ότι υπάρχουν (ως προς ισομορφισμό) ακριβώς 5 ομάδες τάξεως 12, από τις οποίες οι τρεις είναι μη αβελιανές.

22. Έστω m, n θετικοί ακέραιοι και ϕ ο φυσικός ομομορφισμός δακτυλίων $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ με $[a]_n \mapsto [a]_m$. Αν ο m διαιρεί τον n, τότε ο περιορισμός του $\phi : (\mathbb{Z}_n)^* \to (\mathbb{Z}_m)^*$ στις αντίστοιχες ομάδες μονάδων των δακτυλίων είναι επιμορφισμός.

    [Υπόδειξη: Παρατηρούμε πρώτα ότι ο περιορισμός είναι καλά ορισμένος, γιατί $m|n$. Έστω $[a]_m \in (\mathbb{Z}_m)^*$, ισοδύναμα $(a,m) = 1$. Εφόσον $(a,m) = 1$, υπάρχει πρώτος διαιρέτης του m, άρα και του n, που δεν διαιρεί τον a. Συνεπώς, το σύνολο $\mathcal{P} = \{p : \text{πρώτος } p|n,\ p \nmid a\}$ που αποτελείται από τους πρώτους διαιρέτες του n που δεν διαιρούν τον a είναι μη κενό. Θεωρούμε τον ακέραιο $a' = a + km$, όπου $k = \prod_{p\in\mathcal{P}} p$. Τότε $a' \equiv a \,(\mathrm{mod} m)$, δηλαδή $[a']_m = [a]_m$, και $(a', n) = 1$. Για να δείξουμε ότι $(a', n) = 1$, θεωρούμε πρώτο διαιρέτη p του n και διακρίνουμε δύο περιπτώσεις: $p|a$ και $p \nmid a$.]

Κεφάλαιο 5

Σειρές Ομάδων

5.1 Κανονικές σειρές

Ορισμός 5.1.1. Έστω G ομάδα. Μια πεπερασμένη αλυσίδα υποομάδων

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_i \subseteq G_{i+1} \subseteq \cdots \subseteq G_n = G$$

λέγεται **κανονική σειρά** της G αν $G_i \lhd G_{i+1}$ για κάθε i.
Δηλαδή, μια κανονική σειρά έχει τη μορφή

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

Οι ομάδες G_i λέγονται **όροι** της σειράς και τα πηλίκα G_{i+1}/G_i λέγονται **πηλίκα** (ή παράγοντες) της σειράς.
Λέμε ότι η σειρά είναι **χωρίς επαναλήψεις** αν $G_i \neq G_{i+1}$ για κάθε i.

Σε αυτή την περίπτωση το n καλείται **μήκος** της σειράς.

Παραδείγματα 5.1.1. (i) Αν G ομάδα, τότε η

$$1 \lhd G$$

είναι μια κανονική σειρά της G.

(ii) Αν $N \lhd G$, τότε η

$$1 \lhd N \lhd G$$

είναι μια κανονική σειρά της G.

(iii) Αν $G = S_n$, τότε η

$$1 \lhd A_n \lhd S_n$$

είναι μια κανονική σειρά της G.

Ορισμός 5.1.2. Έστω

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

και

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G \qquad (2)$$

δύο κανονικές σειρές της G.
Η (2) λέγεται **επιλέπτυνση** της (1), αν κάθε όρος της (1) εμφανίζεται στην (2).

Ορισμός 5.1.3. Δύο κανονικές σειρές μιας ομάδας G

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

και

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G \qquad (2)$$

λέγονται **ισοδύναμες** αν υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ των πηλίκων τους έτσι ώστε αντίστοιχα πηλίκα να είναι ισόμορφα.

Παράδειγμα 5.1.1. Έστω $G = \mathbb{Z}_{30}$. Δύο κανονικές σειρές της G είναι οι

$$1 \lhd \mathbb{Z}_5 \lhd \mathbb{Z}_{15} \lhd \mathbb{Z}_{30} = G$$

και

$$1 \lhd \mathbb{Z}_3 \lhd \mathbb{Z}_6 \lhd \mathbb{Z}_{30} = G$$

Έχουμε ότι $\mathbb{Z}_{30}/\mathbb{Z}_{15} \simeq \mathbb{Z}_2, \mathbb{Z}_{15}/\mathbb{Z}_5 \simeq \mathbb{Z}_3$ και $\mathbb{Z}_5/1 \simeq \mathbb{Z}_5$ ενώ $\mathbb{Z}_{30}/\mathbb{Z}_6 \simeq \mathbb{Z}_5, \mathbb{Z}_6/\mathbb{Z}_3 \simeq \mathbb{Z}_2$ και $\mathbb{Z}_3/1 \simeq \mathbb{Z}_3$.

Συνεπώς, αυτές οι κανονικές σειρές, της $G = \mathbb{Z}_{30}$, είναι ισοδύναμες.

Λήμμα 5.1.1 (Zassenhaus). *Έστω G ομάδα με $H, K \leq G$ και $H^* \lhd H, K^* \lhd K$. Τότε:*

(i) $H^*(H \cap K^*) \lhd H^*(H \cap K)$

(ii) $K^*(H^* \cap K) \lhd K^*(H \cap K)$ *και*

(iii) $H^*(H \cap K)/H^*(H \cap K^*) \simeq K^*(H \cap K)/K^*(H^* \cap K)$.

Απόδειξη. Εύκολα προκύπτει ότι τα παραπάνω σύνολα είναι υποομάδες. Από υπόθεση $H^* \lhd H$ και $K^* \lhd K$, οπότε $H^* \cap K$, $H \cap K^* \lhd H \cap K$. Έτσι, $N := (H^* \cap K)(H \cap K^*) \lhd H \cap K$.

Θα δείξουμε ότι κάθε πηλίκο στον ισχυρισμό (iii) είναι ισόμορφο με $H \cap K/N$. Θεωρούμε την απεικόνιση $\phi : H^*(H \cap K) \to H \cap K/N$ με $\phi(hx) = xN$, για $h \in H^*$ και $x \in H \cap K$.

Η ϕ είναι καλά ορισμένη: αν $hx = h_1x_1$, τότε $h_1^{-1}h = x_1x^{-1} \in (H \cap K) \cap H^* \subseteq K \cap H^* \subseteq N$ και έτσι $x_1N = xN$, δηλαδή $\phi(hx) = \phi(h_1x_1)$.

Η ϕ είναι ομομορφισμός: Έστω $h_1, h_2 \in H^*$ και $x_1, x_2 \in H \cap K$. Τότε, $x_1h_2x_1^{-1} \in H^*$ και

$$\phi\big((h_1x_1) \cdot (h_2x_2)\big) = \phi(h_1 \underbrace{x_1h_2x_1^{-1}}_{\in H^* \lhd H} \cdot x_1x_2) = x_1x_2N = \phi(h_1x_1) \cdot \phi(h_2x_2)$$

Προφανώς η ϕ είναι επί.

Για να προσδιορίσουμε τον πυρήνα, έστω $h \in H^*$ και $x \in H \cap K$. Τότε $\phi(hx) = 1 = N \Leftrightarrow x \in N = (H^* \cap K)(H \cap K^*) \Leftrightarrow hx \in H^*(H \cap K^*)$. Έπεται ότι $\ker \phi = H^*(H \cap K^*) \lhd H^*(H \cap K)$ και από το 1^o Θεώρημα Ισομορφισμών

$$H^*(H \cap K)/H^*(H \cap K^*) \simeq H \cap K/N$$

Ομοίως, $K^*(H \cap K)/K^*(H^* \cap K) \simeq H \cap K/N$. □

Θεώρημα 5.1.1 (Schreier). *Κάθε δύο κανονικές σειρές μιας ομάδας G έχουν ισοδύναμες επιλεπτύνσεις.*

Απόδειξη. Έστω

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G \qquad (1)$$

και

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G \qquad (2)$$

δύο κανονικές σειρές της G.
Σκοπός είναι να "εισαγάγουμε" ένα "αντίτυπο" της (2) στην (1) και της (1) στην (2) προκειμένου να κατασκευάσουμε τις υποψήφιες ισόμορφες επιλεπτύνσεις. Έχουμε

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$$

άρα

$$1 = H_{i+1} \cap K_0 \lhd H_{i+1} \cap K_1 \lhd \cdots \lhd H_{i+1} \cap K_m = H_{i+1}$$

οπότε

$$H_i = H_i(H_{i+1} \cap K_0) \lhd H_i(H_{i+1} \cap K_1) \lhd \cdots \lhd H_i(H_{i+1} \cap K_m) = H_{i+1}$$

Έστω $H_{i,j} = H_i(H_{i+1} \cap K_j)$. Τότε έχουμε την παρακάτω κανονική σειρά της G η οποία είναι επιλέπτυνση της (1):

$$\begin{aligned} 1 = H_{0,0} &\lhd H_{0,1} \lhd \cdots \lhd H_{0,m-1} \lhd H_{0,m} = H_1 = H_{1,0} \\ &\lhd H_{1,1} \lhd \cdots \lhd H_{1,m-1} \lhd H_{1,m} = H_2 = H_{2,0} \\ &\vdots \\ &\lhd H_{n-1,1} \lhd \cdots \lhd H_{n-1,m-1} \lhd H_{n-1,m} = H_n = G \end{aligned}$$

Ομοίως, για $K_{j,i} = K_j(K_{j+1} \cap H_i)$ έχουμε την παρακάτω κανονική σειρά της G η οποία είναι επιλέπτυνση της (2):

$$\begin{aligned} 1 = K_{0,0} &\lhd K_{0,1} \lhd \cdots \lhd K_{0,n-1} \lhd K_{0,n} = K_1 = K_{1,0} \\ &\lhd K_{1,1} \lhd \cdots \lhd K_{1,m-1} \lhd K_{1,n} = K_2 = K_{2,0} \\ &\vdots \\ &\lhd K_{m-1,1} \lhd \cdots \lhd K_{m-1,n-1} \lhd K_{m-1,n} = K_m = G \end{aligned}$$

Οι δύο νέες σειρές έχουν $m \cdot n + 1$ όρους η κάθε μια και είναι επιλεπτύνσεις των αρχικών.

Θεωρούμε την αντιστοιχία $H_{i,j} \leftrightarrow K_{j,i}$. Από το προηγούμενο Λήμμα τα αντίστοιχα πηλίκα είναι ισόμορφα, δηλαδή

$$H_{i,j+1}/H_{i,j} \simeq K_{j,i+1}/K_{i,j}.$$

□

5.2 Συνθετικές σειρές

Ορισμός 5.2.1. Έστω

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

μια κανονική σειρά της G. Μια επιλέπτυνση της (1) με μήκος μεγαλύτερο της (1) λέγεται **γνήσια επιλέπτυνση** της (1).

Ορισμός 5.2.2. Μια κανονική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

της ομάδας G λέγεται **συνθετική** σειρά της G αν δεν έχει γνήσιες επιλεπτύνσεις.

Πρόταση 5.2.1. *Μια κανονική σειρά*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

της G είναι συνθετική ανν κάθε πηλίκο της σειράς είναι απλή ομάδα.

Απόδειξη. Έστω

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

συνθετική σειρά της G. Θα δείξουμε ότι τα πηλίκα G_{i+1}/G_i είναι απλές ομάδες για κάθε i.

Έστω ότι κάποια G_{i+1}/G_i δεν είναι απλή, δηλαδή υπάρχει $1 < K \lhd G_{i+1}/G_i$. Από το Θεώρημα της Αντιστοιχίας, $K = \Lambda/G_i$, με $\Lambda \lhd G_{i+1}$ και $1 \neq \Lambda \neq G_{i+1}$. Τότε η κανονική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_i \lhd \Lambda \lhd G_{i+1} \lhd \cdots \lhd G_n = G$$

είναι γνήσια επιλέπτυνση της (1) -άτοπο, αφού η (1) είναι συνθετική σειρά της G. Άρα κάθε G_{i+1}/G_i είναι απλή ομάδα.

Αντίστροφα, έστω ότι κάθε πηλίκο G_{i+1}/G_i είναι απλή ομάδα. Θα δείξουμε ότι η

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

είναι συνθετική σειρά της G. Έστω ότι δεν είναι. Τότε υπάρχει γνήσια επιλέπτυνση της (1), έστω η

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_m = G$$

Αυτό σημαίνει ότι υπάρχει k τέτοιο ώστε ο όρος H_k παρεμβάλλεται γνήσια μεταξύ δύο διαδοχικών όρων της (1), έστω $G_\lambda \subsetneq H_k \subsetneq G_{\lambda+1}$.

Έτσι, $1 \neq H_k/G_\lambda \subsetneq G_{\lambda+1}/G_\lambda$ και η $G_{\lambda+1}/G_\lambda$ δεν είναι απλή, γιατί $H_k/G_\lambda \lhd G_{\lambda+1}/G_\lambda$ -άτοπο. □

Παραδείγματα 5.2.1. (i) Η

$$1 \lhd A_3 \lhd S_3$$

είναι συνθετική σειρά της S_3 με πηλίκα $A_3/1 \simeq \mathbb{Z}_3$ και $S_3/A_3 \simeq \mathbb{Z}_2$.

(ii) Έστω $G = \mathbb{Z}_{105}$. Η σειρά

$$1 \lhd \mathbb{Z}_5 \lhd \mathbb{Z}_{105} = G$$

δεν είναι συνθετική, γιατί η $\mathbb{Z}_{105}/\mathbb{Z}_5 \simeq \mathbb{Z}_{21}$ δεν είναι απλή.

Η επιλέπτυνση

$$1 \lhd \mathbb{Z}_5 \lhd \mathbb{Z}_{35} \lhd \mathbb{Z}_{105} = G$$

είναι συνθετική σειρά, με απλά πηλίκα $\mathbb{Z}_5$, $\mathbb{Z}_{35}/\mathbb{Z}_5 \simeq \mathbb{Z}_7$, $\mathbb{Z}_{105}/\mathbb{Z}_{35} \simeq \mathbb{Z}_3$.

Επίσης, η επιλέπτυνση

$$1 \lhd \mathbb{Z}_5 \lhd \mathbb{Z}_{15} \lhd \mathbb{Z}_{105} = G$$

είναι συνθετική σειρά. Τα πηλίκα που προκύπτουν είναι -με αναδιάταξη- τα απλά πηλίκα που βρήκαμε παραπάνω.

(iii) Αν $G = H_1 \times H_2 \times \cdots \times H_n$, τότε

$$1 \lhd H_1 \lhd H_1 \times H_2 \lhd \cdots \lhd H_1 \times H_2 \times \cdots \times H_n = G$$

κανονική σειρά της G. Αν, επιπλέον, οι H_i είναι απλές, τότε η σειρά είναι συνθετική.

(iv) Η άπειρη κυκλική ομάδα $\mathbb{Z}$ δεν έχει συνθετική σειρά, παρότι έχει κανονικές σειρές $(1 \lhd 8\mathbb{Z} \lhd \mathbb{Z})$.

Αν είχε, έστω την

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = \mathbb{Z}$$

τότε η G_1 θα ήταν απλή.

Όμως, $1 \neq G_1 \leq \mathbb{Z}$, άρα $G_1 = k\mathbb{Z}$ και $1 \neq 2k\mathbb{Z} < k\mathbb{Z}$ και $2k\mathbb{Z} \lhd k\mathbb{Z}$ -άτοπο.

Θεώρημα 5.2.1 (Jordan-Hölder). *Δυο συνθετικές σειρές μιας ομάδας G είναι ισοδύναμες.*

Απόδειξη. Άμεσο από το Θεώρημα Schreier, τον ορισμό συνθετικής σειράς και ισοδύναμων σειρών. □

Ορισμός 5.2.3. Λέμε ότι η ομάδα G είναι **επέκταση** της N μέσω της H αν:

(i) $N \lhd G$ και

(ii) $G/N \simeq H$.

Δηλαδή, έχουμε την εξής βραχεία ακριβή ακολουθία ομομορφισμών

$$N \overset{\psi}{\rightarrowtail} G \overset{\phi}{\twoheadrightarrow} H$$

όπου η ψ είναι 1-1, η ϕ είναι επί και $\ker \phi = \operatorname{im} \psi$.

Κάθε ημιευθύ γινόμενο είναι μια επέκταση.

Σε μια κανονική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

ο όρος G_{i+1} είναι επέκταση του G_i μέσω της G_{i+1}/G_i, δηλαδή η G λαμβάνεται από τους όρους και τα πηλίκα της σειράς, με διαδοχικές επεκτάσεις.

Αν, επιπλέον, η σειρά είναι συνθετική, τότε η G "κατασκευάζεται" με διαδοχικές επεκτάσεις απλών ομάδων.

Για να μελετηθεί, λοιπόν, μια ομάδα -τουλάχιστον πεπερασμένη- πρέπει να μελετηθούν οι απλές κανονικές υποομάδες της.

Όπως βλέπουμε στο παραπάνω Θεώρημα, αν G ομάδα και

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

συνθετική σειρά της G, τα πηλίκα (απλές υποομάδες) της σειράς δεν εξαρτώνται από την σειρά, δηλαδή καθορίζονται πλήρως από την G, αλλά δεν "καθορίζουν" την G, όπως έχουμε ήδη δει στα ημιευθέα γινόμενα.

Πρόταση 5.2.2. *Κάθε πεπερασμένη ομάδα G έχει συνθετική σειρά.*

Απόδειξη. Έστω G πεπερασμένη ομάδα. Χρησιμοποιούμε επαγωγή επί της $|G|$.

Αν η ομάδα G είναι απλή, η $1 \lhd G$ είναι συνθετική. Αν δεν είναι απλή, έστω N μεγιστική γνήσια κανονική υποομάδα της G.

Από επαγωγική υπόθεση, υπάρχει συνθετική σειρά για την N, έστω

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_m = N$$

Τότε, η σειρά

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_m = N \lhd G$$

είναι συνθετική σειρά της G. □

Συνεπώς, το πρόβλημα της ταξινόμησης των πεπερασμένων ομάδων (ή γενικότερα των ομάδων που έχουν συνθετικές σειρές) ανάγεται στα εξής δύο:

(a) Ταξινόμηση των απλών ομάδων

(b) Επίλυση του προβλήματος της επέκτασης. Δηλαδή, δοθέντος N και H, να βρεθούν όλες οι μη-ισόμορφες ομάδες G με $N \lhd G$ και $G/N \simeq H$.

Το (a) έχει επιτευχθεί για πεπερασμένες ομάδες.

Μια απάντηση στο πρόβλημα της επέκτασης έχει δοθεί από τους Holder και Schreier, αλλά έχει το ακόλουθο μειονέκτημα:

Η θεωρία τους δίνει έναν χαρακτηρισμό όλων των πιθανών λύσεων G, όμως εν' γένει δεν είναι δυνατόν να προσδιορισθεί για δύο πιθανές λύσεις αν είναι ισόμορφες ή όχι.

Πρόταση 5.2.3. *Έστω*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

και $H \leq G$. Τότε υπάρχει κανονική σειρά της H

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H$$

τέτοια ώστε η H_{i+1}/H_i να είναι ισόμορφη με υποομάδα της G_{i+1}/G_i για κάθε i.

Απόδειξη. Έστω $H_i = H \cap G_i$. Τότε, αφού $G_i \lhd G_{i+1}$, έχουμε $H \cap G_i \lhd H \cap G_{i+1}$ και

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = H$$

Τέλος,

$$\begin{aligned} H_{i+1}/H_i &= H \cap G_{i+1}/H \cap G_i \\ &= H \cap G_{i+1}/(H \cap G_{i+1}) \cap G_i \\ &\simeq (H \cap G_{i+1})G_i/G_i \\ &\leq G_{i+1}/G_i \end{aligned}$$

□

5.3 Ασκήσεις

1. Να βρεθούν δυο μη ισόμορφες ομάδες G_1, G_2 τέτοιες ώστε να υπάρχουν συνθετικές σειρές για τις G_1, G_2 με ίδια (ως προς ισομοφισμό) πηλίκα.

2. Πως είναι μια συνθετική σειρά μιας ομάδας G με

$$|G| = p^n, p^n q, p^2 q^2, pqr$$

όπου p, q, r πρώτοι;

3. Να αποδειχθεί ότι κάθε φυσικός αριθμός γράφεται κατά μοναδικό τρόπο (με αναδιάταξη) ως γινόμενο πρώτων.

4. Έστω G ομάδα. Μια κανονική σειρά της G,

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

είναι συνθετική ανν κάθε G_i είναι μεγιστική κανονική στην G_{i+1} για κάθε i.

5. Μια αβελιανή ομάδα G έχει συνθετική σειρά ανν είναι πεπερασμένη.

6. Να βρεθεί άπειρη ομάδα με συνθετική σειρά.

Κεφάλαιο 6

Επιλύσιμες Ομάδες

6.1 Επιλύσιμες ομάδες

Ορισμός 6.1.1. Μια κανονική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

μιας ομάδας G λέγεται **επιλύσιμη** αν κάθε πηλίκο της σειράς είναι αβελιανή ομάδα.

Ορισμός 6.1.2. Μια ομάδα G λέγεται **επιλύσιμη** αν έχει επιλύσιμη σειρά.

Παρατήρηση 6.1.1. Μια επιλύσιμη ομάδα προκύπτει με διαδοχικές επεκτάσεις αβελιανών ομάδων.

Σχόλιο 6.1.1. Κάθε επιλέπτυνση επιλύσιμης σειράς είναι επιλύσιμη σειρά.

Πράγματι, έστω

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

μια επιλύσιμη σειρά. Αρκεί να εξετάσουμε την περίπτωση $G_i \lhd \Lambda \lhd G_{i+1}$. Θα δείξουμε ότι οι Λ/G_i και G_{i+1}/Λ είναι αβελιανές ομάδες.

Εφόσον η G_{i+1}/G_i είναι αβελιανή, η Λ/G_i είναι αβελιανή ως υποομάδα αβελιανής ομάδας. Επιπλέον,

$$G_{i+1}/\Lambda \simeq (G_{i+1}/G_i)/(\Lambda/G_i)$$

άρα και η G_{i+1}/Λ είναι αβελιανή.

Πόρισμα 6.1.1. *Αν μια ομάδα G είναι επιλύσιμη και έχει συνθετική σειρά, τότε η συνθετική σειρά είναι επιλύσιμη σειρά.*

Απόδειξη. Άμεσο από το προηγούμενο σχόλιο, τον ορισμό της συνθετικής σειράς και το Θεώρημα Schreier. □

Παραδείγματα 6.1.1. (i) Κάθε αβελιανή ομάδα G είναι επιλύσιμη.

Πράγματι, αν η G είναι αβελιανή, τότε η

$$1 \lhd G$$

είναι επιλύσιμη σειρά της G.

(ii) Η S_3, παρότι μη αβελιανή, είναι επιλύσιμη. Η σειρά

$$1 \lhd A_3 \lhd S_3$$

είναι επιλύσιμη, γιατί $A_3/1 \simeq \mathbb{Z}_3$ και $S_3/A_3 \simeq \mathbb{Z}_2$.

(iii) Έστω D_n η διεδρική ομάδα τάξεως $2n$.

Η κανονική σειρά

$$1 \lhd \langle\alpha\rangle \lhd D_n$$

, όπου α στροφή τάξης n, είναι μια επιλύσιμη σειρά της D_n, γιατί $D_n/\langle\alpha\rangle \simeq \mathbb{Z}_2$. Άρα η D_n είναι επιλύσιμη.

(iv) Η S_n για $n \geq 5$ δεν είναι επιλύσιμη, γιατί η σειρά

$$1 \lhd A_n \lhd S_n$$

είναι συνθετική -επειδή η A_n είναι απλή για κάθε $n \geq 5$- και η A_n δεν είναι αβελιανή.

Θεώρημα 6.1.1. *Η κλάση των επιλύσιμων ομάδων είναι κλειστή ως προς υποομάδες, ομάδες πηλίκα και επεκτάσεις, δηλαδή:*

(i) Κάθε υποομάδα επιλύσιμης ομάδας είναι επιλύσιμη.

(ii) Κάθε ομάδα πηλίκο επιλύσιμης ομάδας είναι επιλύσιμη.

(iii) Αν $N \lhd G$ και οι $N, G/N$ είναι επιλύσιμες, τότε η G είναι επιλύσιμη.

Απόδειξη. Έστω G επιλύσιμη ομάδα και

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

επιλύσιμη σειρά της G.
(i) Αν $H \leq G$, τότε

$$1 = H \cap G_0 \lhd \cdots \lhd H \cap G_i \lhd \cdots \lhd H \cap G_n = H$$

επιλύσιμη σειρά της H.

Πράγματι, έχουμε ότι

$$H \cap G_{i+1} \hookrightarrow G_{i+1} \longrightarrow G_{i+1}/G_i$$
$$\phi$$

και $\ker\phi = H \cap G_i$. Έτσι, η $H \cap G_{i+1}/H \cap G_i$ εμφυτεύεται στην G_{i+1}/G_i, η οποία είναι αβελιανή.

Άρα, κάθε πηλίκο $H \cap G_{i+1}/H \cap G_i$ είναι αβελιανή ομάδα.
(ii) Έστω $N \lhd G$ και $\pi : G \to G/N$ ο φυσικός επιμορφισμός. Τότε, η

$$1 = N = \pi(G_0) \lhd \pi(G_1) \lhd \cdots \lhd \pi(G_n) = G/N$$

είναι κανονική σειρά της G/N.

Θα δείξουμε ότι είναι επιλύσιμη. Έχουμε ότι $\pi(G_i) = G_iN/N$ και

$$\begin{aligned}\pi(G_{i+1})/\pi(G_i) &= \frac{G_{i+1}N/N}{G_iN/N} \\ &\simeq \frac{G_{i+1}N}{G_iN} \\ &= \frac{G_{i+1}(G_iN)}{G_iN} \\ &\simeq \frac{G_{i+1}}{G_{i+1}\cap G_iN} \\ &\simeq \frac{G_{i+1}/G_i}{(G_{i+1}\cap G_iN)/G_i}\end{aligned}$$

η οποία είναι αβελιανή, ως πηλίκο της αβελιανής G_{i+1}/G_i.
(iii) Έστω $N \lhd G$ και $N, G/N$ επιλύσιμες. Έστω,

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_m = N$$

επιλύσιμη σειρά της N.

Από το Θεώρημα της Αντιστοιχίας, κάθε επιλύσιμη σειρά της G/N θα έχει τη μορφή

$$N = G_0/N \lhd G_1/N \lhd \cdots \lhd G_n/N = G/N$$

όπου $G_i \lhd G_{i+1}$ και $G_i \supseteq N$ για κάθε i.

Τότε, η σειρά

$$1 = N_0 \lhd \cdots \lhd N_m = N = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

είναι επιλύσιμη σειρά της G, γιατί N_{i+1}/N_i αβελιανή και $G_{i+1}/G_i \simeq \frac{G_{i+1}/N}{G_i/N}$ αβελιανή. □

Πρόταση 6.1.1. *Κάθε πεπερασμένη p-ομάδα είναι επιλύσιμη.*

Απόδειξη. Α' τρόπος: Έστω $|G| = p^n$. Χρησιμοποιούμε επαγωγή στο n.

Αν $n = 1$, τότε η G είναι κυκλική και επιλύσιμη ως αβελιανή.
Έστω $n > 1$. Γνωρίζουμε ότι $Z(G) \neq 1$. Αν $G = Z(G)$, τότε η G είναι αβελιανή και επιλύσιμη.
Αν $Z(G) \neq G$, τότε οι $G/Z(G)$ και $Z(G)$ είναι επιλύσιμες από την επαγωγική υπόθεση.

Άρα, η G είναι επιλύσιμη ως επέκταση της $Z(G)$, μέσω της $G/Z(G)$.
Β' τρόπος: Έστω $|G| = p^n$ και

$$1 = K_0 \lhd K_1 \lhd \cdots \lhd K_r = G \qquad (1)$$

μια συνθετική σειρά της G. Αφού $K_i \leq G$, κάθε K_i είναι p-ομάδα. Επίσης, $|K_{i+1}/K_i| \cdot |K_i| = |K_{i+1}|$ άρα και οι K_{i+1}/K_i είναι p-ομάδες.

Αφού η (1) είναι συνθετική σειρά κάθε K_{i+1}/K_i είναι μη τετριμμένη απλή ομάδα. Έτσι $|K_{i+1}/K_i| = p$, και $K_{i+1}/K_i \simeq \mathbb{Z}_p$. Συνεπώς, η (1) είναι επιλύσιμη. □

Παράδειγμα 6.1.1. Έστω $\Bbbk$ σώμα και

$$T_n(\Bbbk) = \left\{ \begin{pmatrix} * & * & * & * \\ & * & * & * \\ & \mathbb{0} & \ddots & * \\ & & & * \end{pmatrix} \in GL_n(\Bbbk) \right\} \leq GL_n(\Bbbk)$$

οι αντιστρέψιμοι, άνω τριγωνικοί $n \times n$ πίνακες με στοιχεία από το σώμα $\Bbbk$.

Η ομάδα $T_n(\Bbbk)$ είναι επιλύσιμη.

Θα χρησιμοποιήσουμε επαγωγή επί του n. Αν $n = 1$, τότε $T_1(\Bbbk) = \Bbbk^*$, η οποία είναι επιλύσιμη ως αβελιανή.

Για $n > 1$, παίρνουμε την απεικόνιση $\phi : T_n(\Bbbk) \to T_{n-1}(\Bbbk)$, που "διαγράφει" την τελευταία γραμμή και την τελευταία στήλη του πίνακα στον οποίο εφαρμόζεται.

Εύκολα, βλέπουμε ότι η ϕ είναι επιμορφισμός, και έτσι $T_n(\Bbbk)/\ker\phi \simeq T_{n-1}(\Bbbk)$.

Από την επαγωγική υπόθεση, η $T_{n-1}(\Bbbk)$ είναι επιλύσιμη, οπότε αρκεί να δείξουμε ότι η

$$\ker\phi = \left\{ \begin{pmatrix} I_{n-1} & \Gamma \\ 0 & a_{nn} \end{pmatrix} : \Gamma \in M_{(n-1)\times 1}(\Bbbk), a_{nn} \in \Bbbk^* \right\}$$

είναι επιλύσιμη.

Ορίζουμε

$$\pi : \ker\phi \to \Bbbk^*, \qquad \begin{pmatrix} I_{n-1} & \Gamma \\ 0 & a_{nn} \end{pmatrix} \mapsto a_{nn}$$

Η π είναι επιμορφισμός και

$$\ker\pi = \left\{ \begin{pmatrix} I_{n-1} & \Gamma \\ 0 & 1 \end{pmatrix} : \Gamma \in M_{(n-1)\times 1}(\Bbbk) \right\}$$

Εύκολα, διαπιστώνουμε ότι η $\ker\pi$ είναι αβελιανή ομάδα, και άρα η $\ker\phi$ είναι επιλύσιμη, αφού $\ker\phi/\ker\pi \simeq \Bbbk^*$.

Θεώρημα 6.1.2. *Αν G ομάδα με $|G| = p^m q$, όπου p, q πρώτοι, τότε η G είναι μη-απλή και επιλύσιμη.*

Απόδειξη. Αν $p = q$ γνωρίζουμε ήδη ότι η G δεν είναι απλή. Έστω ότι $p \neq q$. Από τα Θεωρήματα Sylow $n_p | q$ και $n_p \equiv 1 \pmod p$, άρα $n_p = 1$ ή q. Αν $n_p = 1$, τότε υπάρχει P Sylow υποομάδα της G, η οποία είναι κανονική στην G λόγω μοναδικότητας.

Έστω ότι $n_p = q$. Αν $P_i \cap P_j = 1$ για κάθε δύο διακεκριμένες Sylow p-υποομάδες της G, τότε έχουμε $q(p^m - 1) = qp^m - q$ στοιχεία τάξης μια δύναμη του p. Όλη η ομάδα έχει qp^m στοιχεία, άρα περισσεύουν q στοιχεία. Συνεπώς, έχουμε μοναδική, άρα κανονική, Sylow q-υποομάδα της G.

Εξετάζουμε, τώρα, την περίπτωση που υπάρχουν Sylow p-υποομάδες της G με μη τετριμμένη τομή. Έστω P_1, P_2 Sylow p-υποομάδες της G ώστε το $I = P_1 \cap P_2$ να έχει το μέγιστο δυνατό πλήθος στοιχείων. Ισχύει ότι αν A μια πεπερασμένη p-ομάδα και $B < A$, τότε $B < N_A(B)$. Άρα, αφού $I < P_1$, έχουμε ότι $I < N_{P_1}(I) = N_1$ και όμοια $I < N_{P_2}(I) = N_2$.

Έπεται ότι $I \lhd \langle N_1, N_2 \rangle = M$. Πράγματι, έστω $w \in M$. Τότε $w = a_1 a_2 \cdots a_k$, $a_i \in N_1 \cup N_2$. Επιπλέον $wIw^{-1} = a_1 a_2 \cdots a_k I a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1} = I$ γιατί για κάθε $x \in N_1$, $xIx^{-1} = I$ και για κάθε $y \in N_2$, $yIy^{-1} = I$.

Αν η M ήταν p-ομάδα τότε θα υπήρχε μια Sylow p-υποομάδα P_3 της G με $M \subseteq P_3$. Αν $P_1 = P_3$, τότε $I < N_1 \leq P_1 \cap P_3$ -άτοπο, από την επιλογή του I. Αν $P_2 = P_3$, βλέπουμε ότι $I < N_2 \leq P_2 \cap P_3$. Άρα η M δεν είναι p-ομάδα, δηλαδή $q \Big| |M|$.

Έστω Q μια Sylow q-υποομάδα της M. Τότε, $|P_1 Q| = \dfrac{|P_1| \cdot |Q|}{|P_1 \cap Q|} = |P_1| \cdot |Q| = p^n q$, αφού αν $K = P_1 \cap Q$, τότε $|K| \Big| |P_1| = p^n$ και $|K| \Big| |Q| = q \Rightarrow K = 1$. Έχουμε, λοιπόν, ότι $G = P_1 Q$. Δηλαδή αν $g \in G$, τότε $g = ab$, $a \in P_1, b \in Q$. Τότε για κάθε $g \in G$, $gIg^{-1} = abIb^{-1}a^{-1} =$

aIa^{-1} -αφού $b \in Q \leq M$ και $I \lhd M$- και $gIg^{-1} = aIa^{-1} \leq P_1$. Έστω $\Lambda = \langle gIg^{-1} : g \in G \rangle \leq P_1$. Όμως,

$$1 \neq I \leq \langle gIg^{-1} : g \in G \rangle \lhd G$$

και

$$\langle gIg^{-1} : g \in G \rangle \leq P_1 < G$$

Τελικά, η G δεν είναι απλή.
Ας υποθέσουμε, τώρα, ότι υπάρχουν μη επιλύσιμες ομάδες τάξεως $p^m q$. Από αυτές επιλέγουμε μια ελάχιστης τάξης, έστω G με $|G| = p^n q$.

Τότε, $p \neq q$ και η G είναι απλή -εφόσον αν $1 \neq N \lhd G$, τότε από την επιλογή της G, οι N, G/N είναι επιλύσιμες, άρα και η G είναι επιλύσιμη-, το οποίο είναι άτοπο. □

Θεώρημα 6.1.3. *Αν G ομάδα με $|G| = p^2q^2$, όπου p, q πρώτοι, τότε η G είναι μη-απλή και επιλύσιμη.*

Απόδειξη. Αν $p = q$, τότε γνωρίζουμε ότι η G δεν είναι απλή. Έστω ότι $p > q$. Τότε $n_p = 1 + kp|q^2$ και άρα $n_p = 1$ ή q^2. Αν $n_p = 1$, τελειώσαμε.

Έστω ότι $n_p = q^2$. Αν $P_i \cap P_j = 1$ για κάθε δύο διακεκριμένες Sylow p-υποομάδες της G, τότε $n_q = 1$ (γιατί;). Άρα αν Q Sylow q-υποομάδα της G, τότε $Q \lhd G$.

Μένει να εξεταστεί η περίπτωση που υπάρχουν P_1, P_2 Sylow p-υποομάδες της G με $P_1 \cap P_2 = I \neq 1$. Επειδή $|P_1| = |P_2| = p^2$ έπεται ότι οι P_1, P_2 είναι αβελιανές και $I \lhd P_1, I \lhd P_2 \Rightarrow 1 \neq I \lhd \langle P_1, P_2 \rangle = M$. Επειδή, $|M| > |P_1| = p^2$, έχουμε ότι $|M| = p^2q$ ή p^2q^2. Αν $|M| = p^2q^2$, τότε $M = G$ και τελειώσαμε.

Αν $|M| = p^2q$, τότε η G έχει υποομάδα δείκτη q και άρα υπάρχει ομομορφισμός $\rho : G \to S_q$. Αν $\ker\rho = 1$, τότε $G \hookrightarrow S_q$ και $p^2q^2 = |G| \Big| q!$ -άτοπο. Άρα $1 \neq \ker\rho \leq M < G$ και $\ker\rho \lhd G$.

Έτσι, η G δεν είναι απλή.
Δείχνουμε, τώρα ότι είναι και επιλύσιμη. Έστω $p \neq q$. Αν $1 \neq N \trianglelefteq G$, τότε οι τάξεις των N και G/N θα έχουν την μορφή της υποθέσεως του Θεωρήματος 6.1.2, δηλαδή οι N και G/N είναι επιλύσιμες. Τελικά, η G είναι επιλύσιμη ως επέκταση επιλυσίμων. □

Θεώρημα 6.1.4. *Μια ομάδα G με $|G| = pqr$, όπου p, q, r πρώτοι είναι μη-απλή και επιλύσιμη.*

Απόδειξη. Γνωρίζουμε ότι η G δεν είναι απλή. Άρα, υπάρχει $N \lhd G$ με $1 \neq N$ και οι ομάδες N, G/N έχουν τάξη της μορφής $\kappa \cdot \lambda$, όπου οι κ, λ είναι πρώτοι ή $\kappa = 1$.

Από τα δυο προηγούμενα θεωρήματα, οι N, G/N είναι επιλύσιμες, άρα και η G είναι επιλύσιμη ως επέκταση επιλύσιμων ομάδων. □

Τα παραπάνω συνοψίζονται στο εξής:

Θεώρημα 6.1.5. *Μια ομάδα G με $|G| = p^n$ ή p^nq ή p^2q^2 ή pqr, όπου p, q, r πρώτοι, είναι επιλύσιμη.*

Πρόταση 6.1.2. *Αν η G είναι μια πεπερασμένη p-ομάδα και $K < G$, τότε $K < N_G(K)$.*

Απόδειξη. Η G δεν είναι αβελιανή. Επίσης $1 \neq Z(G) \neq G$ και η $1 \neq G/Z(G)$ είναι p-ομάδα, άρα $Z(G/Z(G)) \neq 1$. Συμπεραίνουμε ότι $Z(G/Z(G)) = J_2(G)/Z(G)$ και $J_2(G) \lhd G$.

Έχουμε ότι $J_2(G) = G$ ή $J_2(G) < G$. Αν $J_2(G) < G$, τότε η $1 \neq G/J_2(G)$ είναι μια p-ομάδα, άρα $Z(G/J_2(G)) \neq 1$. Επιπλέον, $Z(G/J_2(G)) = J_3(G)/J_2(G)$ και $J_3(G) \lhd G$, οπότε $J_3(G) = G$ ή $J_3(G) \neq G$.

Η ομάδα είναι πεπερασμένη, άρα μετά από κάποια βήματα έχουμε

$$1 = J_0(G) < Z(G) = J_1(G) < J_2(G) < \cdots < J_n(G) = G$$

με $J_i(G) \lhd G$ και $J_{i+1}/J_i(G) = Z(G/J_i(G))$ για κάθε i.

Έστω $K \lhd G$. Τότε $KJ_i(G) \lhd KJ_{i+1}(G)$. Πράγματι, έστω $b = k_1 z_{i+1} \in KJ_{i+1}(G)$ και $a = k_2 z_i \in KJ_i(G)$. Θα δείξουμε ότι $bab^{-1} \in KJ_i(G)$.

$$k_1 z_{i+1} \underbrace{k_2 z_i}_{g} z_{i+1}^{-1} k_1^{-1} = k_1 z_{i+1} z_{i+1}^{-1} k_2 z_i z_i' k_1^{-1} = k_1 k_2 z_i z_i' k_1^{-1} \in KJ_i(G)K = KJ_i(G)$$

Αφού η G είναι πεπερασμένη p-ομάδα και

$$1 = J_0(G) < Z(G) = J_1(G) < J_2(G) < \cdots < J_n(G) = G$$

αν $K_i = KJ_i(G)$, τότε

$$1 \lhd K = K_0 \lhd K_1 \lhd \cdots \lhd K_n = G$$

για κάθε $K \leq G$.

Αν $K < G$, τότε υπάρχει i ώστε $K_i = K$ και $K_{i+1} \neq K$, αλλά $K = K_i \lhd K_{i+1}$ και $K_{i+1} \leq N_G(K) = \{g : gKg^{-1} = K\}$, άρα $K < N_G(K)$. □

Παράδειγμα 6.1.2. Αν G ομάδα με $|G| = 72$, τότε η G είναι επιλύσιμη.

Έχουμε $|G| = 72 = 2^3 \cdot 3^2$. Γνωρίζουμε ότι $n_3 = 3k + 1 | 8$, άρα $n_3 = 1$ ή 4. Αν $n_3 = 1$, τότε υπάρχει μοναδική Sylow 3-υποομάδα $P \lhd G$. Οι P και G/P είναι επιλύσιμες ως p-ομάδες, και έτσι η G είναι επιλύσιμη.

Έστω, τώρα, ότι $n_3 = 4$. Τότε, αν P είναι μια από τις 4 Sylow 3-υποομάδες της G, έχουμε $[G : N_G(P)] = 4$. θέτουμε $N_G(P) = K$. Γνωρίζουμε ότι υπάρχει ομομορφισμός

$$\rho : G \to S_4$$

με $\ker \rho \leq K$. Τότε $G/\ker \rho \simeq \operatorname{im} \rho$. Αφού $[G : K] = 4$, $|K| = 3^2 \cdot 2$. Αφού η $|K|$ είναι της μορφής $p^n q$, η K είναι επιλύσιμη και άρα και ο $\ker \rho$ ως υποομάδα επιλύσιμης ομάδας είναι επιλύσιμη. Επίσης, η S_4 είναι επιλύσιμη, άρα η $\operatorname{im} \rho \leq S_4$ είναι επιλύσιμη.

Τελικά, η G είναι επιλύσιμη.

Παράδειγμα 6.1.3. Αν G ομάδα με $|G| = 90$, τότε η G είναι επιλύσιμη.

Έστω G ομάδα με $|G| = 90 = 2 \cdot 45$.

Υπενθύμιση: Αν $|G| = 2n$, με n περιττό, τότε υπάρχει $N \lhd G$ με $[G : N] = 2$.

Έχουμε τους ομομορφισμούς

$$\rho : G \to \operatorname{Sym}(G)$$

$$g \mapsto \rho_g : G \to G, \rho_g(x) = gx$$

Επειδή $2 \Big| |G|$, υπάρχει $a \in G$ με $a^2 = 1$. Έστω

$$\rho_a : G \to G, \quad x_1 \mapsto ax_1 \to aax_1 = a^2 x_1 = x_1$$

Η $(x_1, ax_1)(x_2, ax_2) \dots (x_n, ax_n)$ είναι περιττή μετάθεση.

Έχουμε $S_{|G|} = A_{|G|} \cup \rho_a A_{|G|}$ και $\rho(G) \leq S_{|G|}$ άρα

$$\begin{aligned}
\rho(G) &= \big(\rho(G) \cap A_{|G|}\big) \cup \big(\rho(G) \cap \rho_a A_{|G|}\big) \\
&= {}^{1}K \cup \rho_a \rho(G) \cap \rho_a A_{|G|} \\
&= K \cup \rho_a \big(\rho(G) \cap A_{|G|}\big) \\
&= K \cup \rho_a K
\end{aligned}$$

οπότε $K = \rho(G) \cap A_{|G|}$ και $[\rho(G) : K] = 2$.

Έτσι υπάρχει $N \lhd G$ με $[G : N] = 2$ και $|N| = 45 = 5 \cdot 3^2$. Συνεπώς η N είναι επιλύσιμη. Επιπλέον $|G/N| = 2$, άρα και η G/N είναι επιλύσιμη.

Τελικά, η G είναι επιλύσιμη ως επέκταση επιλύσιμων.

Θεώρημα 6.1.6 (Hall). *Αν η G είναι επιλύσιμη και $|G| = mn$, όπου $(m, n) = 1$, τότε υπάρχει $A \leq G$ με $|A| = m$ και κάθε δύο τέτοιες υποομάδες είναι συζυγείς.*

Σχόλιο 6.1.2. Η επιλυσιμότητα της G είναι αναγκαία συνθήκη. Πράγματι, $|A_5| = 60 = 3 \cdot 20$, αλλά δεν υπάρχει υποομάδα της A_5 τάξης 20.

Ισχύει και το αντίστροφο:

Θεώρημα 6.1.7 (Hall). *Έστω G ομάδα με $|G| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, όπου p_i διακεκριμένοι πρώτοι. Αν η G περιέχει υποομάδα τάξεως $|G|/p_i^{r_i}$ για κάθε i, τότε η G είναι επιλύσιμη.*

Θεώρημα 6.1.8 (Burnside). *Κάθε ομάδα τάξης $p^m q^n$, όπου p, q πρώτοι, είναι επιλύσιμη.*

Θεώρημα 6.1.9 (Feit-Thompson). *Κάθε ομάδα περιττής τάξης είναι επιλύσιμη.*

6.2 Παράγωγος σειρά

Έστω G ομάδα και $\alpha, \beta \in G$. Τότε, ορίζουμε τον μεταθέτη των α, β ως $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$. Η **παράγωγος υποομάδα** της G είναι η $G' = \langle [\alpha, \beta] : \alpha, \beta \in G \rangle$.

Παρατηρούμε ότι $G' \lhd G$ και ότι G/G' είναι αβελιανή. Η ομάδα-πηλίκο G/G' καλείται **αβελιανοποίηση** της G και συμβολίζεται με $G_{\alpha\beta}$.

Υπενθυμίζουμε ότι αν $H \lhd G$, τότε η G/H είναι αβελιανή ανν $G' \leq H$. Ιδαιτέρως, G αβελιανή ανν $G' = 1$.

Ορισμός 6.2.1. Η **n-οστή παράγωγος υποομάδα** $G^{(n)}$ της G ορίζεται επαγωγικά ως εξής $G^{(n)} = (G^{(n-1)})'$, όπου $G^{(0)} = G$.

Προφανώς $G^{(n+1)} \lhd G^{(n)}$.

Ορισμός 6.2.2. Η **παράγωγος σειρά** της G είναι η "σειρά"

$$\cdots \lhd G^{(n)} \lhd G^{(n-1)} \lhd \cdots \lhd G^{(1)} \lhd G^{(0)} = G$$

Παρατηρήσεις 6.2.1. (i) Κάθε πηλίκο της παραγώγου σειράς, $G^{(n+1)}/G^{(n)}$, είναι αβελιανή ομάδα.

Συνεπώς, αν $G^{(n)} = 1$ για κάποιο n, τότε η G είναι επιλύσιμη.

(ii) Αν $\phi : G \to G$ ομομορφισμός, τότε $\phi(G^{(n)}) \leq G^{(n)}$, δηλαδή η $G^{(n)}$ είναι **πλήρως αναλλοίωτη** υποομάδα της G, $G^{(n)} \underset{\text{π.α.}}{\leq} G$.

Παραδείγματα 6.2.1. (i) Αν $n \geq 5$ παρατηρούμε ότι η $S_n/A_n \simeq \mathbb{Z}_2$ είναι αβελιανή. Έπεται ότι $S_n' \leq A_n$. Αλλά $S_n' \lhd S_n$ και η A_n είναι απλή, άρα αφού $S_n' \lhd A_n$, έχουμε ότι $S_n' = 1$ ή $S_n' = A_n$.

Αν $S_n' = 1$, τότε η S_n είναι αβελιανή -άτοπο.

Άρα $S_n' = A_n$. Αφού η A_n είναι απλή και μη αβελιανή, έχουμε ότι $S_n'' = (S_n')' = A_n' = A_n$ και έτσι $S_n^{(k)} = A_n$.

Η παράγωγος σειρά της S_n, λοιπόν, είναι η

$$\cdots = S_n^{(3)} = S_n^{(2)} = S_n' = A_n \lhd S_n$$

(ii) Έστω $n \geq 3$, D_n η διεδρική ομάδα και α η στροφή τάξης n.

Γνωρίζουμε ότι $\langle\alpha\rangle \lhd D_n$ και $D_n/\langle\alpha\rangle \simeq \mathbb{Z}_2$, άρα $D_n' \leq \langle\alpha\rangle$. Αφού η D_n δεν είναι αβελιανή, $D_n' \neq 1$.

Η D_n', όμως, είναι αβελιανή ως υποομάδα κυκλικής ομάδας, και έτσι $D_n^{(2)} = 1$.

Άρα η

$$1 = D_n^{(2)} \lhd D_n^{(1)} \lhd D_n$$

είναι η παράγωγος σειρά της D_n.

Πρόταση 6.2.1. *Έστω G ομάδα. Τότε, $G^{(n)} \lhd G$ για κάθε n.*

Απόδειξη. Χρησιμοποιούμε επαγωγή επί του n. Προφανώς $G^{(0)}$, $G^{(1)} \lhd G$.
Έστω ότι $G^{(n)} \lhd G$. Θα δείξουμε ότι $G^{(n+1)} \lhd G$.
Έστω $g \in G$ και $\alpha, \beta \in G^{(n)}$. Τότε, $\tau_g[\alpha, \beta] = [\tau_g(\alpha), \tau_g(\beta)] \in G^{(n+1)}$.
Άρα, $\tau_g(G^{(n+1)}) \subseteq G^{(n+1)}$ και έτσι $G^{(n+1)} \lhd G$. □

Πρόταση 6.2.2. *Έστω G επιλύσιμη ομάδα και*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G \qquad (1)$$

μια επιλύσιμη σειρά. Τότε, $G^{(i)} \leq G_{n-i}$ για κάθε i.

Απόδειξη. Με επαγωγή επί του i.

Για $i = 1$ θα δείξουμε ότι $G^{(1)} = G' \leq G_{n-1}$. Επειδή η (1) είναι επιλύσιμη σειρά κάθε πηλίκο της σειράς είναι αβελιανή ομάδα, ιδιαίτερα η $G_n/G_{n-1} = G/G_{n-1}$ είναι αβελιανή. Συνεπώς $G' \leq G_{n-1}$.

Έστω ότι $G^{(i)} \leq G_{n-i}$. Θα δείξουμε ότι $G^{(i+1)} \leq G_{n-i-1}$. Έχουμε $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_{n-i}, G_{n-i}]$, αλλά η G_{n-i}/G_{n-i-1} είναι αβελιανή, άρα $G_{n-i}' \leq G_{n-i-1}$.

Συνεπώς, $G^{(i+1)} \leq G_{n-i-1}$. □

Παρατηρήσεις 6.2.2. (i) Αν η G είναι επιλύσιμη, τότε η G περιέχει πλήρως αναλλοίωτη αβελιανή υποομάδα.

(ii) Αν η G είναι επιλύσιμη και $G \neq 1$, τότε $G \neq G'$.

Θεώρημα 6.2.1. *Η G είναι επιλύσιμη ανν $G^{(n)} = 1$ για κάποιο n.*

Απόδειξη. Αν $G^{(n)} = 1$ για κάποιο n, τότε είναι προφανές ότι η G είναι επιλύσιμη.

Αντίστροφα, έστω ότι η G είναι επιλύσιμη και έστω

$$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

μια επιλύσιμη σειρά της G.

Από τη προηγούμενη Πρόταση, έχουμε ότι $G^{(n)} \subseteq H_0 = 1$. □

6.3 Επιλυσιμότητα με ριζικά

6.3.1 Πολυώνυμα βαθμού ≤ 4

Ξεκινάμε με μια ιστορική αναδρομή στη μελέτη των ριζών των πολυωνύμων. Οι μαθηματικοί του Μεσαίωνα, και πιθανώς και αυτοί στη Βαβυλωνία, γνώριζαν τον τύπο που δίνει

τις ρίζες του τριωνύμου $f(X) = X^2 + aX + b$. Θέτοντας $X = x - \frac{1}{2}b$ το $f(X)$ μετατρέπεται σε ένα πολυώνυμο

$$g(x) = x^2 + c - 1/4b^2$$

Παρατηρήστε ότι ο α είναι ρίζα του $g(x)$ ανν ο $\alpha - \frac{1}{2}b$ είναι ρίζα του $f(X)$. Οι ρίζες του $g(x)$ είναι οι $\pm\frac{1}{2}\sqrt{b^2 - 4c}$, και έτσι οι ρίζες του $f(X)$ είναι οι

$$\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$$

Οι Scipione del Ferro, Tartaglia (Niccolo Fontana) και Cardano βρήκαν τύπο για τις ρίζες ενός πολυωνύμου 3ου βαθμού. Ένα πολυώνυμο $f(X) = X^3 + aX^2 + bX + c$ μπορεί να μετασχηματιστεί, θέτοντας $X = x - \frac{1}{3}a$, σε ένα πολυώνυμο

$$g(x) = x^3 + qx + r$$

και ο α είναι ρίζα του $g(x)$ ανν ο $\alpha - \frac{1}{3}a$ είναι ρίζα του $f(X)$. Αν α ρίζα του $g(x)$, γράφοντας $\alpha = \beta + \gamma$ -όπου τα β και γ θα βρεθούν αργότερα- έχουμε

$$\begin{aligned}\alpha^3 &= (\beta + \gamma)^3 \\ &= \beta^3 + \gamma^3 + 3(\beta^2\gamma + \beta\gamma^2) \\ &= \beta^3 + \gamma^3 + 3\alpha\beta\gamma\end{aligned}$$

και υπολογίζοντας το $g(\alpha)$ παίρνουμε

$$\beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r = 0$$

Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $\beta\gamma = -q/3$. Έτσι,

$$\beta^3 + \gamma^3 = -r$$

Γνωρίζουμε, επιπλέον, ότι

$$\beta^3\gamma^3 = -q^3/27$$

και βρίσκουμε τα β^3 και γ^3. Αντικαθιστώντας,

$$\beta^3 - \frac{q^3}{27}\beta^3 = -r$$

έχουμε

$$\beta^3 = \frac{1}{2}[-r \pm (r^2 + 4q^3/27)^{1/2}]$$

Όμοια,

$$\gamma^3 = \frac{1}{2}[-r \mp (r^2 + 4q^3/27)^{1/2}]$$

Αν $\omega = e^{2\pi i/3}$ πρωταρχική κυβική ρίζα της μονάδας, υπάρχουν έξι πιθανές κυβικές ρίζες: οι β, $\omega\beta$, $\omega^2\beta$, γ, $\omega\gamma$ και $\omega^2\gamma$. Ζευγαρώνοντας ώστε να δώσουν γινόμενο $-q/3$, βρίσκουμε

$$-q/3 = \beta\gamma = (\omega\beta)(\omega^2\gamma) = (\omega^2\beta)(\omega\gamma)$$

Έπεται ότι οι ρίζες του $g(x)$ είναι οι $\beta + \gamma$, $\omega\beta + \omega^2\gamma$ και $\omega^2\beta + \omega\gamma$.

Ο τύπος για τις ρίζες ενός πολυωνύμου 4ου βαθμού βρέθηκε από τον Lodovici Ferrari, το 1545. Παρουσιάζουμε μια εξαγωγή του τύπου αυτού που οφείλεται στον Descartes.

Ένα πολυώνυμο $f(X) = X^4 + aX^3 + bX^2 + cX + d$ μπορεί να μετασχηματιστεί, θέτοντας $X = x - \frac{1}{4}a$, στο πολυώνυμο

$$g(x) = x^4 + qx^2 + rx + s$$

Επιπλέον, ο α είναι ρίζα του $g(x)$ ανν ο $\alpha - \frac{1}{4}a$ είναι ρίζα του $f(X)$.

Παραγοντοποιούμε το $g(x)$ σε τριώνυμα:

$$x^4 + qx^2 + rx + s = (x^2 + kx + \ell)(x^2 - kx + m)$$

Αν τα k, ℓ, m μπορούν να βρεθούν, τότε και οι ρίζες του $g(x)$ μπορούν να βρεθούν. Αναπτύσσοντας το δεξί μέλος, και εξισώνοντας συντελεστές βρίσκουμε

$$q = \ell + m - k^2,$$

$$r = km - k\ell$$

και

$$s = \ell m$$

Ξαναγράφουμε τις δυο πρώτες εξισώσεις ως

$$m + \ell = q + k^2$$

και

$$m - \ell = r/k$$

Προσθέτοντας και αφαιρώντας παίρνουμε

$$2\ell = k^2 + q - r/k$$

και

$$2m = k^2 + q + r/k$$

Αυτές οι εξισώσεις δείχνουν ότι τελειώσαμε αν μπορούμε να βρούμε το k. Αλλά, η

$$(k^2 + q - r/k)(k^2 + q + r/k) = 4\ell m = 4s$$

δίνει

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0$$

από όπου βρίσκουμε το k^2.

6.3.2 Θεωρία Galois

Υποθέτουμε ότι κάθε σώμα F είναι υπόσωμα ενός αλγεβρικά κλειστού σώματος C. Αυτό σημαίνει ότι αν $f(x) \in F[x]$, τον δακτύλιο των πολυωνύμων με συντελεστές από το F, και το $f(x)$ έχει βαθμό $n \geq 1$, τότε υπάρχουν στοιχεία $\alpha_1, \alpha_2, \ldots, \alpha_n \in C$ -οι **ρίζες** του $f(x)$- και $\alpha \in F$ μη μηδενικό τέτοιο ώστε

$$f(x) = \alpha(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in C[x]$$

Η τομή μιας οικογένειας υποσωμάτων ενός σώματος είναι υπόσωμα.

Ορίζουμε το **μικρότερο υπόσωμα** του C που περιέχει ένα σύνολο X ως την τομή όλων των υποσωμάτων του C που περιέχουν το X. Αν, παραδείγματος χάριν, $\alpha \in C$, τότε το μικρότερο υπόσωμα του C που περιέχει το $F \cup \{\alpha\}$ είναι το

$$F(a) = \{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x],\ g(\alpha) \neq 0\}$$

Το $F(a)$ καλείται και το υπόσωμα που προκύπτει από το F **επισυνάπτοντας** το α. Όμοια, κανείς μπορεί να ορίσει το $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, το υπόσωμα που προκύπτει από το F επισυνάπτοντας τα $\alpha_1, \alpha_2, \ldots, \alpha_n$. Πιο συγκεκριμένα, αν $f(x) \in F[x]$ και

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \in C[x]$$

τότε το σώμα $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, το υπόσωμα που προκύπτει από το F επισυνάπτοντας τις ρίζες του $f(x)$, καλείται το **σώμα ριζών** του $f(x)$ επί του F.

Παρατηρήστε ότι το σώμα ριζών του $f(x)$ εξαρτάται από το F. Αν $f(x) = x^2 + 1 \in \mathbb{Q}[x]$, τότε το σώμα ριζών του $f(x)$ επί του $\mathbb{Q}$ είναι το $\mathbb{Q}(i)$, ενώ αν θεωρήσουμε $f(x) \in \mathbb{R}[x]$, τότε το σώμα ριζών του $f(x)$ επί του $\mathbb{R}$ είναι το $\mathbb{C}$.

Ορισμός 6.3.1. Έστω $f(x) \in F[x]$ με σώμα ριζών E επί του F. Λέμε ότι το $f(x)$ είναι **επιλύσιμο με ριζικά** αν υπάρχει αλυσίδα υποσωμάτων

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

όπου $E \subseteq K_t$ και κάθε K_{i+1} προκύπτει από το K_i επισυνάπτοντας μια ρίζα ενός στοιχείου του K_i, δηλαδή $K_{i+1} = K_i(\beta_{i+1})$, όπου $\beta_{i+1} \in K_{i+1}$ και μια δύναμη του β_{i+1} ανήκει στο K_i.

Όταν λέμε ότι υπάρχει ένας τύπος για τις ρίζες ενός πολυωνύμου $f(x)$, εννοούμε ότι το $f(x)$ είναι επιλύσιμο με ριζικά. Αυτό γίνεται φανερό στις περιπτώσεις των πολυωνύμων δευτέρου, τρίτου, και τετάρτου βαθμού.

Αν $f(x) = x^2 + bx + c$, έστω $F = \mathbb{Q}(b, c)$. Αν $\beta = \sqrt{b^2 - 4c}$, τότε $\beta^2 \in F$. Ορίζοντας $K_1 = F(\beta)$ παρατηρούμε ότι το K_1 είναι το σώμα ριζών του $f(x)$ επί του F.

Αν $f(x) = x^3 + qx + r$, έστω $F = \mathbb{Q}(q, r)$. Ορίζουμε $\beta_1 = \sqrt{r^2 + 4q^3/27}$ και $K_1 = F(\beta_1)$. Επιπλέον, έστω $\beta_2 = \sqrt[3]{-r + \beta_1}$ και $K_2 = K_1(\beta_2)$. Τέλος, έστω $K_3 = K_2(\omega)$, όπου ω μια κυβική ρίζα της μονάδας. Παρατηρήστε ότι ο τύπος των ριζών του $f(x)$ συνεπάγεται ότι το K_3 περιέχει το σώμα ριζών E του $f(x)$. Από την άλλη, το E δεν είναι εν γένει ίσο με το K_3. Αν οι ρίζες του $f(x)$ ήταν όλες πραγματικές, τότε $E \subseteq \mathbb{R}$, ενώ $K_3 \nsubseteq \mathbb{R}$.

Αν $f(x) = x^4 + qx^2 + rx + s$, έστω $F = \mathbb{Q}(q, r, s)$. Χρησιμοποιώντας τον συμβολισμό για την ανεύρεση των ριζών του $f(x)$, υπάρχει τριώνυμο που έχει το k^2 ως ρίζα. Όπως προηγουμένως, υπάρχει αλυσίδα σωμάτων

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq K_3$$

με $k^2 \in K_3$.
Ορίζουμε $K_4 = K_3(k)$, $K_5 = K_4(\sqrt{\gamma})$, όπου $\gamma = k^2 - 4\ell$, και $K_6 = K_5(\sqrt{\delta})$, όπου $\delta = k^2 - 4m$. Τότε, το σώμα ριζών του $f(x)$ περιέχεται στο K_6.

Αντίστροφα, είναι εμφανές ότι, αν το $f(x)$ είναι επιλύσιμο με ριζικά, τότε κάθε ρίζα του $f(x)$ εκφράζεται μέσω των συντελεστών του $f(x)$ χρησιμοποιώντας τις πράξεις του σώματος και την εξαγωγή ριζών.

Ορισμός 6.3.2. Έστω E και E' σώματα. Μια απεικόνιση $\sigma : E \to E'$ τέτοια ώστε:

(i) $\sigma(1) = 1$,

(ii) $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ για κάθε $\alpha, \beta \in E$, και

(iii) $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ για κάθε $\alpha, \beta \in E$

καλείται **ομομορφισμός** σωμάτων.

Αν ο σ είναι 1-1 και επί, τότε θα λέμε ότι ο σ είναι **ισομορφισμός**. Ειδικότερα, ένας ισομορφισμός $\sigma : E \to E$ καλείται **αυτομορφισμός**.

Λήμμα 6.3.1. *Έστω $f(x) \in F[x]$, E το σώμα ριζών του $f(x)$ επί του F, και $\sigma : E \to E$ ένας αυτομορφισμός που σταθεροποιεί το F, δηλαδή $\sigma(\alpha) = \alpha$ για κάθε $\alpha \in F$. Αν το $\alpha \in E$ είναι ρίζα του $f(x)$, τότε το $\sigma(\alpha)$ είναι ρίζα του $f(x)$.*

Απόδειξη. Αν $f(x) = \sum \alpha_i x^i$, τότε

$$\begin{aligned} 0 &= \sigma(f(\alpha)) \\ &= \sigma\left(\sum \alpha_i \alpha^i\right) \\ &= \sum \sigma(\alpha_i)\sigma(\alpha)^i \\ &= \sum \alpha_i \sigma(\alpha)^i \end{aligned}$$

και έτσι το $\sigma(\alpha)$ είναι ρίζα του $f(x)$. □

Λήμμα 6.3.2. *Έστω F υπόσωμα του K, $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq K$ και $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Αν K' σώμα που περιέχει το F ως υπόσωμα, και $\sigma : E \to K'$ αυτομορφισμός που σταθεροποιεί το F με $\sigma(\alpha_i) = \alpha_i$ για κάθε i, τότε ο σ είναι η ταυτοτική απεικόνιση.*

Απόδειξη. Χρησιμοποιούμε επαγωγή επί του n. Αν $n = 1$, τότε το E περιέχει όλα τα $g(\alpha_1)/h(\alpha_1)$, όπου $g(x)$, $h(x) \in F[x]$ και $h(\alpha_1) \neq 0$. Είναι άμεσο ότι ο σ σταθεροποιεί κάθε τέτοιο στοιχείο.

Το επαγωγικό βήμα έπεται από την παρατήρηση ότι

$$F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F^*(\alpha_n)$$

όπου $F^*(\alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$. □

Αν το F είναι υπόσωμα του σώματος E, τότε το σύνολο των αυτομορφισμών του E που σταθεροποιούν το F αποτελεί μια ομάδα με πράξη τη σύνθεση.

Ορισμός 6.3.3. Έστω F υπόσωμα του E. Η **ομάδα Galois**, $\mathrm{Gal}(E/F)$, είναι η ομάδα με πράξη τη σύνθεση όλων των αυτομορφισμών του E που σταθεροποιούν το F.

Αν $f(x) \in F[x]$ και $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ το σώμα ριζών του $f(x)$ επί του F, τότε η ομάδα Galois του $f(x)$ είναι η $\mathrm{Gal}(E/F)$.

Θεώρημα 6.3.1. *Έστω $f(x) \in F[x]$ και $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ το σύνολο των διακεκριμένων ριζών του $f(x)$ στο σώμα ριζών του, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ επί του F. Τότε, η απεικόνιση*

$$\phi : \mathrm{Gal}(E/F) \to S_X \simeq S_n$$

με $\phi(\sigma) = \sigma|_X$ είναι μια εμφύτευση, δηλαδή η ϕ καθορίζεται πλήρως από τη δράση της στο X.

Απόδειξη. Αν $\sigma \in \mathrm{Gal}(E/F)$, τότε από το Λήμμα 6.3.1 έχουμε ότι $\sigma(X) \subseteq X$. Η $\sigma|_X$ είναι 1-1 και επί, επειδή η σ είναι 1-1 και το X είναι πεπερασμένο. Είναι εύκολο να δούμε ότι η ϕ είναι ομομορφισμός, και επιπλέον είναι 1-1, από το Λήμμα 6.3.2. □

Δεν είναι αναγκαίο κάθε μετάθεση των ριζών του $f(x)$ να προκύπτει από κάποιο $\sigma \in \mathrm{Gal}(E/F)$. Για παράδειγμα, αν $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$, τότε $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ και δεν υπάρχει $\sigma \in \mathrm{Gal}(E/F)$ με $\sigma(\sqrt{2}) = \sqrt{3}$.

Ορισμός 6.3.4. Αν F υπόσωμα ενός σώματος E, τότε το E είναι ένας F-διανυσματικός χώρος. Ο **βαθμός** του E επί του F, $[E : F]$, είναι η διάσταση του F-διανυσματικού χώρου E.

Πρόταση 6.3.1. *Έστω $F \subseteq E \subseteq K$ σώματα με $[K : E]$, $[E : F] < \infty$. Τότε,*

$$[K : F] = [K : E][E : F]$$

Απόδειξη. Αφήνεται ως άσκηση. □

Πρόταση 6.3.2. *Έστω $p(x) \in F[x]$ ανάγωγο πολυώνυμο βαθμού n. Αν α ρίζα του $p(x)$, τότε το $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ είναι βάση του $F(\alpha)$ ως F-διανυσματικού χώρου, και άρα $[F(a) : F] = n$.*

Απόδειξη. Αφήνεται ως άσκηση. □

Λήμμα 6.3.3. *Έστω $p(x) \in F[x]$ ανάγωγο πολυώνυμο, και α, β ρίζες του $p(x)$ σε ένα σώμα ριζών του $p(x)$ επί του F. Τότε, υπάρχει ισομορφισμός $\lambda^* : F(\alpha) \to F(\beta)$ που σταθεροποιεί το F και $\lambda^*(\alpha) = \beta$.*

Απόδειξη. Από την Πρόταση 6.3.2, κάθε στοιχείο του $F(\alpha)$ εκφράζεται μοναδικά ως

$$\alpha_0 + \alpha_1\alpha + \cdots + \alpha_{n-1}\alpha^{n-1}$$

Ορίζουμε την λ^* ως εξής:

$$\lambda^*(\alpha_0 + \alpha_1\alpha + \cdots + \alpha_{n-1}\alpha^{n-1}) = \alpha_0 + \alpha_1\beta + \cdots + \alpha_{n-1}\beta^{n-1}$$

Εύκολα, βλέπουμε ότι η λ^* είναι ομομορφισμός σωμάτων. Είναι, επιπλέον, ισομορφισμός γιατί η αντίστροφη της κατασκευάζεται όμοια. □

Σχόλιο 6.3.1. Το προηγούμενο Λήμμα μπορεί να γενικευτεί:
Έστω $\lambda : F \to F'$ ισομορφισμός σωμάτων, $p(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in F[x]$ ανάγωγο πολυώνυμο, και $p'(x) = \lambda(\alpha_0) + \lambda(\alpha_1)x + \cdots + \lambda(\alpha_n)x^n \in F'[x]$. Έστω, τέλος, α ρίζα του $p(x)$ και β ρίζα του $p'(x)$ σε αντίστοιχα σώματα ριζών. Τότε, υπάρχει ισομορφισμός $\lambda^* : F(\alpha) \to F'(\beta)$ με $\lambda^*(\alpha) = \beta$ και $\lambda^*|_F = \lambda$.

Λήμμα 6.3.4. *Έστω $f(x) \in F[x]$, και E το σώμα ριζών του $f(x)$ επί του F. Αν K ενδιάμεσο σώμα, $F \subseteq K \subseteq E$, και $\lambda : K \to K$ αυτομορφισμός του K που σταθεροποιεί το F, τότε υπάρχει αυτομορφισμός $\lambda^* : E \to E$ με $\lambda^*|_K = \lambda$.*

Απόδειξη. Χρησιμοποιούμε επαγωγή επί του $[E : F] = d$. Αν $d = 1$, τότε $E = F$, κάθε ρίζα του $f(x)$ ανήκει στο K, και μπορούμε να πάρουμε $\lambda^* = \lambda$.

Αν $d > 1$, τότε $E \neq K$ και υπάρχει ρίζα α του $f(x)$ που δεν ανήκει στο K. Τώρα, το α είναι ρίζα κάποιου ανάγωγου παράγοντα $p(x)$ του $f(x)$. Εφόσον $\alpha \notin K$, ο βαθμός του $p(x)$

είναι $k > 1$. Από το γενικευμένο Λήμμα 6.3.3 υπάρχει ισομορφισμός $\lambda_1 : K(\alpha) \to K(\beta)$ που επεκτείνει τον λ με $\lambda_1(\alpha) = \beta$.Επίσης $[E : K(\alpha)] = d/k < d$, από την Πρόταση 6.3.1.

Το E είναι το σώμα ριζών του $f(x)$ επί του $K(\alpha)$. Από την επαγωγική υπόθεση συμπεραίνουμε ότι ο λ_1, άρα και ο λ, μπορεί να επεκταθεί σε αυτομορφισμό του E. □

Σχόλιο 6.3.2. Όπως και προηγουμένως, και αυτό το Λήμμα μπορεί να γενικευθεί. Αν $f(x) \in F[x]$, τότε κάθε δύο σώματα ριζών του $f(x)$ είναι ισόμορφα. Δηλαδή, μπορούμε να μιλάμε για το σώμα ριζών του $f(x)$.

Θεώρημα 6.3.2. *Έστω p πρώτος, F σώμα που περιέχει μια πρωταρχική p-οστή ρίζα της μονάδας, έστω ω, και $f(x) = x^p - a \in F[x]$. Τότε:*

(i) Αν α ρίζα του $f(x)$, τότε το $f(x)$ είναι ανάγωγο ανν $\alpha \notin F$.

(ii) Το σώμα ριζών, E, του $f(x)$ επί του F είναι το $F(\alpha)$.

(iii) Αν το $f(x)$ είναι ανάγωγο, τότε $\mathrm{Gal}(E/F) \simeq \mathbb{Z}_p$.

Απόδειξη. (i) Αν $\alpha \in F$, τότε το $f(x)$ δεν είναι ανάγωγο, γιατί έχει το $x-\alpha$ ως παράγοντα.

Αντίστοφα, έστω ότι $f(x) = g(x)h(x)$, όπου ο βαθμός του $g(x)$ είναι $k < p$. Εφόσον οι ρίζες του $f(x)$ είναι οι $\alpha, \omega\alpha, \omega^2\alpha, \ldots, \omega^{p-1}\alpha$, κάθε ρίζα του $g(x)$ είναι της μορφής $\omega^i\alpha$ για κάποιο i.

Αν ο σταθερός όρος του $g(x)$ είναι c, τότε $c = \pm\omega^r\alpha^k$ για κάποιο r. Αφού ω, $c \in F$, έπεται ότι $\alpha^k \in F$. Αλλά $(k, p) = 1$, γιατί ο p είναι πρώτος, και έτσι $1 = ks + tp$ για κάποιους $s, t \in \mathbb{Z}$. Έτσι,

$$\alpha = \alpha^{ks+tp} = (\alpha^k)^s(\alpha^p)^t \in F$$

(ii) Άμεσο, εφόσον οι ρίζες του $f(x)$ είναι της μορφής $\omega^i\alpha$.

(iii) Αν $\sigma \in \mathrm{Gal}(E/F)$, τότε $\sigma(\alpha) = \omega^i\alpha$ για κάποιο i. Ορίζουμε

$$\phi : \mathrm{Gal}(E/F) \to \mathbb{Z}_p,\ \sigma \mapsto [i]_p$$

Εύκολα, ο ϕ είναι ομομορφισμός. Είναι 1-1 από το Λήμμα 6.3.1. Τέλος, εφόσον το $f(x)$ είναι ανάγωγο, από την υπόθεση το Λήμμα 6.3.3 μας δίνει ότι $\mathrm{Gal}(E/F) \neq 1$. Έτσι, η ϕ είναι επί, αφού η $\mathbb{Z}_p$ δεν έχει γνήσιες υποομάδες.

□

Θεώρημα 6.3.3. *Έστω $f(x) \in F[x]$, E το σώμα ριζών του $f(x)$ επί του F, και έστω ότι το $f(x)$ έχει όλες τις ρίζες του απλές. Τότε, το $f(x)$ είναι ανάγωγο ανν η* $\mathrm{Gal}(E/F)$ *δρα μεταβατικά στο σύνολο X των ριζών του $f(x)$.*

Απόδειξη. Καταρχάς, το Λήμμα 6.3.1 μας εξασφαλίζει ότι η $\mathrm{Gal}(E/F)$ δρα στο X. Αν το $f(x)$ είναι ανάγωγο, τότε το Λήμμα 6.3.3 δείχνει ότι η $\mathrm{Gal}(E/F)$ δρα μεταβατικά στο X.

Αντίστροφα, έστω ότι υπάρχει παραγοντοποίηση $f(x) = g(x)h(x) \in F[x]$. Τότε, $g(x) = \prod(x - \alpha_i)$ και $h(x) = \prod(x - \beta_i)$ επί του E. Αφού το $f(x)$ έχει απλές ρίζες, $\alpha_i \neq \beta_j$ για κάθε i, j. Αλλά η $\mathrm{Gal}(E/F)$ δρα μεταβατικά στις ρίζες του $f(x)$, άρα υπάρχει $\sigma \in \mathrm{Gal}(E/F)$ με $\sigma(\alpha_1) = \beta_1$ -άτοπο, από το Λήμμα 6.3.1. □

Σχόλιο 6.3.3. Μπορεί να αποδειχθεί ότι αν το σώμα F είναι χαρακτηριστικής 0 ή αν το F είναι πεπερασμένο, τότε κάθε ανάγωγο πολυώνυμο στο $F[x]$ έχει απλές ρίζες.

Είναι εύκολο να δούμε ότι αν α_1 μια ρίζα του $f(x)$, η σταθεροποιούσα του α_1 είναι

$$\mathrm{Gal}(E/F(\alpha_1) \leq \mathrm{Gal}(E/F)$$

και η $\mathrm{Gal}(E/F(\alpha_1)$ είναι η ομάδα Galois του $f(x)/(x-\alpha_1)$ επί του $F(\alpha_1)$.

Έτσι, το $f(x)/(x-\alpha_1)$ είναι ανάγωγο επί του $F(\alpha_1)$ ανν η $\mathrm{Gal}(E/F(\alpha_1)$ δρα μεταβατικά επί των υπολειπόμενων ριζών.

Λήμμα 6.3.5. *Έστω E σώμα ριζών επί του F για κάποιο $f(x) \in F[x]$, και K σώμα ριζών επί του E για κάποιο $g(x) \in E[x]$. Αν $\sigma \in \mathrm{Gal}(K/F)$, τότε $\sigma|_E \in \mathrm{Gal}(E/F)$.*

Απόδειξη. Αφήνεται ως άσκηση. □

Θεώρημα 6.3.4. *Έστω $F \subseteq K \subseteq E$ σώματα, όπου τα K και E είναι σώματα ριζών επί του F. Τότε, $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(E/F)$ και*

$$\mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K) \simeq \mathrm{Gal}(K/F)$$

Απόδειξη. Η

$$\Phi : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F),\ \sigma \mapsto \sigma|_K$$

είναι καλά ορισμένη από το προηγούμενο Λήμμα και ομομορφισμός.

Ο πυρήνας της Φ αποτελείται από τους αυτομορφισμούς που σταθεροποιούν το K, δηλαδή $\ker\Phi = \mathrm{Gal}(E/K)$, και έτσι η υποομάδα αυτή είναι κανονική.

Ισχυριζόμαστε ότι η Φ είναι επί. Αν $\lambda \in \mathrm{Gal}(K/F)$, τότε η λ μπορεί να επεκταθεί σε έναν αυτομορφισμό λ^* του E, γιατί το E είναι σώμα ριζών. Έτσι, $\lambda^* \in \mathrm{Gal}(E/K)$ και $\Phi(\lambda^*) = \lambda^*|_K = \lambda$. Το ζητούμενο έπεται από το 1ο Θεώρημα Ισομορφισμών. □

Λήμμα 6.3.6. *Έστω $f(x) = x^n - a \in F[x]$, E το σώμα ριζών του $f(x)$ επί του F, και $\alpha \in E$ μια n-οστή ρίζα του a. Τότε, υπάρχουν υποσώματα*

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = F(\alpha)$$

με $K_{i+1} = K_i(\beta_{i+1})$, $\beta_{i+1}^{p(i)} \in K_i$, και $p(i)$ πρώτος για κάθε i.

Απόδειξη. Αφήνεται ως άσκηση. □

Η συζήτηση που προηγήθηκε συνοψίζεται στο εξής:

Θεώρημα 6.3.5 (Galois, 1831). *Έστω $f(x) \in F[x]$ βαθμού n. Έστω, επιπλέον, ότι το F περιέχει όλες τις p-οστές ρίζες της μονάδας για κάθε πρώτο p που διαιρεί το $n!$, και έστω E το σώμα ριζών του $f(x)$ επί του F. Αν το $f(x)$ είναι επιλύσιμο με ριζικά, τότε η $G = \mathrm{Gal}(E/F)$ είναι επιλύσιμη.*

Απόδειξη. Εφόσον το $f(x)$ είναι επιλύσιμο με ριζικά, υπάρχουν υποσώματα

$$F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t$$

με $E \subseteq K_t$ και $K_{i+1} = K_i(\beta_{i+1})$, όπου $\beta_{i+1} \in K_{i+1}$ και κάποια δύναμη του β_{i+1} ανήκει στο K_i.

Από το προηγούμενο Λήμμα, μπορούμε να υποθέσουμε ότι κάποια πρώτη δύναμη του β_{i+1} ανήκει στο K_{i+1}. Αν ορίσουμε $H_i = \mathrm{Gal}(K_t/K_i)$, τότε

$$1 = G_t \leq G_{t-1} \leq \cdots \leq G_0 = G$$

Αφού, το F περιέχει p-οστές ρίζες της μονάδας, το Θεώρημα 6.3.2 μας δίνει ότι το K_{i+1} είναι σώμα ριζών επί του K_i. Επιπλέον, μπορεί να αποδειχθεί ότι υπάρχει τέτοιος "πύργος" σωμάτων στον οποίο το K_t είναι σώμα ριζών κάποιου πολυωνύμου επί του F.

Από το προηγούμενο Θεώρημα

$$H_{i+1} = \mathrm{Gal}(K_t/K_{i+1}) \lhd \mathrm{Gal}(K_t/K_i) = H_i$$

και

$$H_{i+1}/H_i \simeq \mathrm{Gal}(K_{i+1}/K_i) \simeq \mathbb{Z}_p$$

από το Θεώρημα 6.3.2. □

Παρατηρήσεις 6.3.1. (i) Δείξαμε ότι η $\mathrm{Gal}(K_t/F)$ είναι επιλύσιμη. Από το Θεώρημα 6.3.4 $\mathrm{Gal}(K_t/E) \lhd \mathrm{Gal}(K_t/F)$ και $\mathrm{Gal}(K_t/F)/\mathrm{Gal}(K_t/E) \simeq \mathrm{Gal}(E/F)$, άρα και η $\mathrm{Gal}(E/F)$ είναι επιλύσιμη.

(ii) Η υπόθεση ότι η F περιέχει ρίζες της μονάδας μπορεί να παραλειφθεί.

(iii) Αν το σώμα F είναι χαρακτηριστικής 0, τότε ισχύει και το αντίστροφο του Θεωρήματος 6.3.5, και αποδείχθηκε, επίσης, από τον Galois.

Οι P. Ruffini (1799) και N.H. Abel (1824) απέδειξαν[2] την μη ύπαρξη τύπου που δίνει τις ρίζες ενός τυχόντος πολυωνύμου βαθμού 5, δίνοντας τέλος στην αναζήτηση, σχεδόν τριών αιώνων, γενίκευσης του έργου των Scipione, Tartaglia, Cardano και Lodovici.

Σε σύγχρονη γλώσσα, έδειξαν ότι η ομάδα Galois ενός πολυωνύμου 5ου βαθμού είναι η S_5, η οποία δεν είναι επιλύσιμη. Το 1829, ο Abel απέδειξε ότι ένα πολυώνυμο του οποίου η ομάδα Galois είναι μεταθετική είναι επιλύσιμο με ριζικά -εξού και οι αβελιανές ομάδες.

6.4 Ασκήσεις

1. Δείξτε ότι οι S_3, S_4 είναι επιλύσιμες.
2. Αν H p-υποομάδα μιας πεπερασμένης ομάδας G και $p \big| |G/H|$, τότε $H < N_G(H)$. [Υπόδειξη: Θεωρήστε τη δράση της H στο G/H. Τι σημαίνει ότι μια τροχιά έχει ένα στοιχείο;]
3. Αν G ομάδα με $|G| < 100$ και $|G| \neq 60$, τότε η G είναι επιλύσιμη.
4. Να εξετασθεί αν μια ομάδα G με $|G| = 144$ είναι επιλύσιμη.
5. Μια επιλύσιμη ομάδα G έχει συνθετική σειρά ανν είναι πεπερασμένη.
6. Αν $M, N \leq G$ και οι M, N είναι επιλύσιμες με $M \lhd G$, τότε η MN είναι επιλύσιμη.
7. Αν $M, N \lhd G$ και οι $G/M, G/N$ είναι επιλύσιμες, τότε η $G/M \cap N$ είναι επιλύσιμη.
8. Με δεδομένο ότι ο αριθμός των στοιχείων σε μια κλάση συζυγίας μιας πεπερασμένης ομάδας δε μπορεί να είναι δύναμη πρώτου μεγαλύτερη του 1, αποδείξτε ότι αν p και q πρώτοι, τότε κάθε ομάδα τάξης $p^m q^n$ είναι επιλύσιμη.
9. Αποδείξτε ότι τα παρακάτω είναι ισοδύναμα:

[2] Στην πραγματικότητα, ούτε η απόδειξη του Ruffini ούτε του Abel ήταν αυστηρά σωστές, αλλά η απόδειξη του Abel έγινε δεκτή από τους σύγχρονούς του, σε αντίθεση με αυτή του Ruffini.

(i) Κάθε ομάδα περιττής τάξης είναι επιλύσιμη.

(ii) Κάθε πεπερασμένη απλή ομάδα είναι περιττής τάξης.

10. Μια πεπερασμένη επιλύσιμη ομάδα G περιέχει κανονική αβελιανή p-ομάδα για κάποιο πρώτο p.

11. Έστω G πεπερασμένη ομάδα και $a, b \in G$ έτσι ώστε τα $o(a), o(b), o(ab)$ να είναι σχετικά πρώτα ανα ζεύγη. Τότε η G δεν είναι επιλύσιμη.
[Υπόδειξη: Θεωρήστε τις $H = \langle a, b\rangle$ και H/H'.]

12. Αν G επιλύσιμη ομάδα και $|G| \leq 200$, τότε $|G| = 60, 120, 168$ ή 180.

13. (i) Αν η G είναι μια απλή ομάδα τάξεως $2^3 \cdot 7^2$ και $H \leq G$, τότε $[G : H] \geq 14$.

(ii) Να εξετασθεί αν μια ομάδα τάξεως $2^3 \cdot 7^2$ είναι επιλύσιμη.

14. Μια πεπερασμένα παραγόμενη επιλύσιμη ομάδα της οποίας κάθε στοιχείο έχει πεπερασμένη τάξη είναι πεπερασμένη.

15. Αν $K \underset{\text{π.α.}}{\leq} \Lambda \underset{\text{π.α.}}{\leq} M$, τότε $K \underset{\text{π.α.}}{\leq} M$.

16. Αποδείξτε ότι $G^{(n)} \underset{\text{π.α.}}{\leq} G$ για κάθε n.

17. Αποδείξτε ότι η $Z(G)$ δεν είναι αναγκαστικά πλήρως αναλλοιώτη υποομάδα της G.
[Υπόδειξη: Θεωρήστε την $G = \mathbb{Z}_2 \times S_3$.]

18. Να βρεθεί η παράγωγος σειρά της S_4.

Κεφάλαιο 7

Μηδενοδύναμες Ομάδες

7.1 Μηδενοδύναμες ομάδες

Έστω G ομάδα και H, $K \leq G$. Ορίζουμε

$$[H, K] := \langle [h, k] : h \in H, k \in K \rangle$$

Ορισμός 7.1.1. Μια κανονική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

λέγεται **κεντρική σειρά** της G αν $G_i \lhd G$ και $G_{i+1}/G_i \subseteq Z(G/G_i)$ για κάθε i, όπου $Z(G/G_i)$ το κέντο της ομαδας-πηλίκο G/G_i.

Παρατήρηση 7.1.1. Έστω

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

κανονική σειρά μιας ομάδας G. Τότε $[G_{i+1}, G] \leq G_i$ ανν $G_{i+1}/G_i \leq Z(G/G_i)$.

Πράγματι,

$$\begin{aligned} z_{i+1}G_i \in Z(G/G_i) &\Leftrightarrow z_{i+1}G_i gG_i = gG_i z_{i+1}G_i,\ \forall g \in G \\ &\Leftrightarrow z_{i+1}gG_i = gz_{i+1}G_i,\ \forall g \in G \\ &\Leftrightarrow z_{i+1}^{-1}g^{-1}z_{i+1}g \in G_i,\ \forall g \in G \\ &\Leftrightarrow [z_{i+1}, g] \in G_i,\ \forall g \in G \end{aligned}$$

Ορισμός 7.1.2. Μια ομάδα G λέγεται **μηδενοδύναμη** αν επιδέχεται κεντρικής σειράς.

Παρατήρηση 7.1.2. Αν η G είναι μηδενοδύναμη, τότε $Z(G) \neq 1$.

Πράγματι, αν $G \neq 1$, τότε $1 \neq G_1 \subseteq Z(G/G_0) = Z(G)$.

Παραδείγματα 7.1.1. (i) Κάθε αβελιανή ομάδα είναι μηδενοδύναμη.

(ii) Κάθε κεντρική σειρά είναι επιλύσιμη σειρά. Αρα, κάθε μηδενοδύναμη ομάδα είναι επιλύσιμη.

(iii) Γνωρίζουμε ότι $Z(S_n) = 1$ για κάθε $n \geq 3$. Οι S_3 και S_4, λοιπόν, παρότι είναι επιλύσιμες, δεν είναι μηδενοδύναμες.

7.2 Ανωτέρα και κατωτέρα κεντρική σειρά

Ορισμός 7.2.1. Έστω G ομάδα. Ορίζουμε την **ανωτέρα κεντρική σειρά** της G ως την αύξουσα ακολουθία υποομάδων

$$1 = Z^0(G) \leq Z(G) = Z^1(G) \leq Z^2(G) \leq \cdots \leq Z^n(G) \leq \cdots$$

που ορίζεται επαγωγικά ως εξής: $Z^0(G) = 1$ και $Z^{i+1}(G)$ η υποομάδα της G που περιέχει την $Z^i(G)$ και αντιστοιχεί στο κέντρο της $G/Z^i(G)$ (σύμφωνα με το Θεώρημα της Αντιστοιχίας). Δηλαδή, η $Z^{i+1}(G)$ ορίζεται από την σχέση

$$Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$$

Από το Θεώρημα της Αντιστοιχίας και τον τρόπο ορισμού των όρων της κεντρικής σειράς, έπεται επαγωγικά, ότι $Z^i(G) \subseteq Z^{i+1}(G)$ και $Z^i(G) \lhd G$.

Έστω G ομάδα και

$$1 = Z^0(G) \lhd Z^1(G) \lhd \cdots \lhd Z^i(G) \lhd Z^{i+1}(G) \lhd \cdots$$

η ανωτέρα κεντρική σειρά της G.

Παρατηρήσεις 7.2.1. (i) Η παραπάνω "σειρά" δεν καταλήγει απαραιτήτως στην G, π.χ. αν $Z(G) = 1$.

(ii) Εξ' ορισμού η ανωτέρα κεντρική σειρά είναι κεντρική (με την έννοια του ορισμού 7.1.1), δηλαδή $Z^{i+1}(G)/Z^i(G) \subseteq Z(G/Z^i(G))$.

(iii) Αν συμβεί $Z^k(G) = G$ για κάποιο k, τότε η σειρά

$$1 = Z^0(G) \lhd Z^1(G) \lhd \cdots \lhd Z^k(G) = G$$

είναι κεντρική σειρά για την G, και συνεπώς η G είναι μηδενοδύναμη.

Παράδειγμα 7.2.1. Έστω

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z} \right\} \leq GL_3(\mathbb{Z})$$

Τότε,

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\} \leq G$$

Ψάχνουμε $Z^2(G)$ ώστε $Z(G/Z(G)) = Z^2(G)/Z(G)$.

Παρατηρούμε ότι ο

$$\phi : G \to \mathbb{Z} \times \mathbb{Z}$$
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a, c)$$

είναι επιμορφισμός και $\ker \phi = Z(G)$. Συνεπώς,

$$G/Z(G) \simeq \mathbb{Z} \times \mathbb{Z}$$

Αφού η $\mathbb{Z}\times\mathbb{Z}$ είναι αβελιανή, έπεται ότι και η $G/Z(G)$ είναι αβελιανή. Συνεπώς, $Z(G/Z(G)) = G/Z(G)$ και άρα $Z^2(G) = G$.

Η ανωτέρα κεντρική σειρά της G είναι η

$$1 = Z^0(G) \lhd Z(G) = Z^1(G) \lhd G = Z^2(G)$$

η οποία είναι και κεντρική σειρά της G. Τελικά, η G είναι μηδενοδύναμη.

Πρόταση 7.2.1. *Κάθε πεπερασμένη p-ομάδα είναι μηδενοδύναμη.*

Απόδειξη. Έστω G ομάδα με $|G| = p^n$, $n \geq 1$. Κάθε μη-τετριμμένο πηλίκο της G έχει μη-τετριμμένο κέντρο ως p-ομάδα.

Άρα, αν $Z^i(G) \neq G$, τότε $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G)) \neq 1$ και έτσι $Z^i(G) \subset Z^{i+1}(G)$. Αφού η G είναι πεπερασμένη, υπάρχει n ώστε $Z^n(G) = G$, και συνεπώς η G είναι μηδενοδύναμη. □

Υπενθυμίζουμε ότι αν G ομάδα και H, K υποομάδες της G, με $[H, K]$ συμβολίζουμε την υποομάδα της G που παράγεται από τους μεταθέτες $[h, k]$, $h \in H$, $k \in K$.

Ορισμός 7.2.2. Έστω G ομάδα. Ορίζουμε την **κατωτέρα κεντρική σειρά** της G ως την φθίνουσα ακολουθία κανονικών υποομάδων

$$\cdots \lhd \gamma_{n+1}(G) \lhd \gamma_n(G) \lhd \cdots \lhd \gamma_2(G) = G' \lhd \gamma_1(G) = G$$

που ορίζεται επαγωγικά ως εξής: $\gamma_1(G) = G$ και $\gamma_{n+1}(G) = [\gamma_n(G), G]$.

Παρατηρήσεις 7.2.2. (i) Για να δείξουμε ότι $\gamma_n(G) \lhd G$ για κάθε n, χρησιμοποιούμε επαγωγή επί του n. Για $n = 1$ το ζητούμενο είναι άμεσο.

Αν $\gamma_n(G) \lhd G$ και $g \in G$, τότε για $\alpha \in \gamma_n(G)$ και $\beta \in G$, έχουμε ότι

$$\tau_g[\alpha, \beta] = [\underbrace{\tau_g(\alpha)}_{\in\gamma_n(G)}, \underbrace{\tau_g(\beta)}_{\in G}] \in \gamma_{n+1}(G)$$

άρα $\tau_g(\gamma_{n+1}(G)) \subseteq \gamma_{n+1}(G)$, που σημαίνει ότι $\gamma_{n+1}(G) \lhd G$.

(ii) Αν $\alpha \in \gamma_n(G)$ και $\beta \in G$, τότε $[\alpha, \beta] = \underbrace{\alpha^{-1}}_{\in\gamma_n(G)} \underbrace{\beta^{-1}\alpha\beta}_{\in\gamma_n(G)}$, δηλαδή $\gamma_{n+1}(G) \subseteq \gamma_n(G)$ και η ακολουθία είναι πράγματι φθίνουσα.

(iii) Αν $\gamma_n(G) = 1$ για κάποιο n, τότε η G είναι μηδενοδύναμη.

Πράγματι, στην περίπτωση αυτή, η σειρά

$$1 = \gamma_n(G) \lhd \gamma_{n-1}(G) \lhd \cdots \lhd \gamma_1(G) = G$$

είναι κεντρική σειρά της G, αφού εξ' ορισμού

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \Leftrightarrow \gamma_i(G)/\gamma_{i+1}(G) \subseteq Z(G/\gamma_{i+1}(G))$$

Πρόταση 7.2.2. *Έστω*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

μια κεντρική σειρά μιας μηδενοδύναμης ομάδας G. Τότε:

(i) $\gamma_i(G) \subseteq G_{n-i+1}$ για κάθε i, και άρα $\gamma_{n+1}(G) = 1$.

(ii) $G_i \subseteq Z^i(G)$ *για κάθε* i*, και άρα* $Z^n(G) = G$*.*

(iii) $\gamma_{m+1}(G) = 1$ *ανν* $Z^m(G) = G$*.*

Απόδειξη. Χρησιμοποιούμε επαγωγή επί του i.

(i) Για $i = 1$, έχουμε $\gamma_1(G) = G = G_n$.

Έστω ότι $\gamma_i(G) \subseteq G_{n-i+1}$. Επειδή $G_{n-i+1}/G_{n-i} \subseteq Z(G/G_{n-i})$, έχουμε ότι $[G_{n-i+1}, G] \subseteq G_{n-i}$. Άρα

$$\gamma_{i+1}(G) = [\gamma_i(G), G] \subseteq [G_{n-i+1}, G] \subseteq G_{n-i}$$

(ii) Για $i = 0$ το ζητούμενο προφανώς ισχύει.

Έστω ότι $G_i \subseteq Z^i(G)$. θα δείξουμε ότι $G_{i+1} \subseteq Z^{i+1}(G)$.Έστω $g_{i+1} \in G_{i+1}$ και $g \in G$. Έχουμε ότι $G_{i+1}/G_i \subseteq Z(G/G_i)$, άρα $g_{i+1}g \equiv gg_{i+1} \mod G_i$, και έτσι $g_{i+1}g \equiv gg_{i+1} \mod Z^i(G)$.

Δηλαδή, $g_{i+1}Z^i(G) \in Z(G/Z^i(G)) = Z^{i+1}(G)/Z^i(G)$ και τελικά $g_{i+1} = \underbrace{z_{i+1}}_{\in Z^{i+1}(G)} \underbrace{z_i}_{\in Z^i(G)} \in Z^{i+1}(G)$. Αφού το g_{i+1} είναι τυχόν στοιχείο της G_{i+1}, έπεται ότι $G_{i+1} \subseteq Z^{i+1}(G)$.

(iii) Αν $\gamma_{m+1}(G) = 1$, στη θέση της αρχικής κεντρικής σειράς θεωρούμε την κατωτέρα κεντρική σειρά

$$1 = \gamma_{m+1}(G) \lhd \gamma_m(G) \lhd \cdots \lhd \gamma_1(G) = G_n = G$$

και εφαρμόζοντας το (iv) έχουμε ότι

$$G = \gamma_1(G) = \gamma_{m-m+1}(G) \subseteq Z^m(G)$$

Δηλαδή, $Z^m(G) = G$. Ομοίως αποδεικνύεται η άλλη κατεύθυνση.

□

Ορισμός 7.2.3. Έστω G μηδενοδύναμη ομάδα. Το ελάχιστο m για το οποίο $Z^m(G) = G$ ή ισοδύναμα $\gamma_{m+1}(G) = 1$, λέγεται **κλάση μηδενοδυναμίας** της G.

Από την προηγούμενη Πρόταση προκύπτει ότι η κλάση μηδενοδυναμίας μιας μηδενοδύναης ομάδας G είναι το ελάχιστο μήκος κεντρικής σειράς.

Παραδείγματα 7.2.1. (i) Έστω R δακτύλιος με μονάδα και $I \leq R$ υποδακτύλιος του R. Ορίζουμε

$$I^m = \{\omega \in I : \omega = \sum_{i=1}^{\rho_\omega} \omega_i, \quad \omega_i = x_{i_1}x_{i_2}\cdots x_{i_m}, x_{i_j} \in I\}$$

Τότε $I^m \leq I$.

Έστω $x \in I$ και $a = 1 + x$. Τότε $(1 + x)(1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1}) = 1$. Άρα το $1 + x$ είναι αντιστρέψιμο στοιχείο του δακτυλίου. Άρα $I^n = 0$.

Έστω $x, y \in I$. Τότε $(1 + x)(1 + y) = 1 + \underbrace{x + y + xy}_{\in I}$ και άρα αν ορίσουμε $G = 1 + I$, τότε η G είναι ομάδα και η

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = 1 \qquad (*)$$

είναι κεντρική σειρά της G, δηλαδή $[G_i, G] \leq G_{i+1}$.

Έστω $y_i \in I^i, y \in I$. Τότε

$$\begin{aligned}(1+y_i)(1+y)(1+y_i)^{-1}(1+y)^{-1} &= (1+y_i)(1+y)((1+y_i)]^{-1}\\ &= (1+y_i)(1+y)[(1+y)(1+y_i))^{-1}\\ &= (1+\underbrace{y_i+y+y_iy}_{a})(1+\underbrace{y+y_i+yy_i}_{b})^{-1}\\ &= (1+a)(1+b)^{-1}\\ &= (1+a)(1-b+b^2-\cdots+(-1)^{n-1}b^{n-1})\\ &= 1+(a-b)\underbrace{(1-b+b^2-\cdots+(-1)^{n-2}b^{n-2})}_{\omega}+(-1)^{n-1}\underbrace{ab^{n-1}}_{\in I^n}\\ &= (1+a)(y_iy-yy_i)\omega \in 1+I^{i+1} \subseteq G_{i+1}\end{aligned}$$

(ii) Έστω R μεταθετικός δακτύλιος με μονάδα, και

$$U_n(R) = \left\{ \begin{pmatrix} 1 & r_{12} & \cdots & r_{1,n} \\ 0 & 1 & \cdots & r_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} : r_{i,j} \in R \right\}$$

η ομάδα των άνω τριγωνικών $n \times n$ πινάκων με στοιχεία από τον R, με μονάδες στην κύρια διαγώνιο.

Τότε,

$$Z(U_n(R)) = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 & r_{1,n} \\ 0 & 1 & 0 & \cdots & r_{2,n} \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} : r_{i,j} \in R \right\}$$

$$Z^2(U_n(R)) = \left\{ \begin{pmatrix} 1 & 0 & \cdots & r_{1,n-1} & r_{1,n} \\ 0 & 1 & \cdots & 0 & r_{2,n} \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} : r_{ij} \in R \right\}$$

,

$$Z^{n-2}(U_n(R)) = \left\{ \begin{pmatrix} 1 & 0 & r_{1,3} & \cdots & r_{1,n} \\ 0 & 1 & 0 & \cdots & r_{2,n} \\ 0 & 0 & 1 & \cdots & r_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} : r_{ij} \in R \right\}$$

και $Z^{n-1}(U_n(R)) = U_n(R)$. Δηλαδή, η $U_n(R)$ είναι μηδενοδύναμη ομάδα κλάσεως $n-1$.

Παρατήρηση 7.2.1. Από το προηγούμενο Παράδειγμα έπεται ότι υπάρχουν μηδενοδύναμες ομάδες κλάσεως c, για κάθε $c \in \mathbb{N}$.

Στη περίπτωση που $R = \mathbb{Z}_p$, τότε η $U_n(\mathbb{Z}_p)$ είναι πεπερασμένη p-ομάδα τάξης $p^{1+2+\cdots+(n-1)} = p^{\frac{n(n-1)}{2}}$, δηλαδή υπάρχουν πεπερασμένες μηδενοδύναμες ομάδες κλάσεως c, για κάθε $c \in \mathbb{N}$.

Αν $R = \mathbb{Z}$, τότε μπορεί να δειχθεί ότι η $U_n(\mathbb{Z})$ είναι ελευθέρα στρέψεως και πεπερασμένα παραγόμενη μηδενοδύναμη ομάδα.

Σημειώνουμε χωρίς απόδειξη το παρακάτω σχετικό θεώρημα:

Θεώρημα 7.2.1 (Hall, 1969). *Μια πεπερασμένα παραγόμενη, ελευθέρα στρέψης μηδενοδύναμη ομάδα είναι ισόμορφη με υποομάδα της $U_n(\mathbb{Z})$ για κάποιο n.*

Θεώρημα 7.2.2. *(i) Κάθε υποομάδα H μιας μηδενοδύναμης ομάδας G είναι μηδενοδύναμη.*

(ii) Αν η G είναι μηδενοδύναμη και $N \lhd G$, τότε η G/N είναι μηδενοδύναμη.

(iii) Ένα ευθύ γινόμενο $G_1 \times G_2 \times \cdots \times G_k$ μηδενοδύναμων ομάδων είναι μηδενοδύναμη ομάδα.

Απόδειξη. (i) Μπορούμε εύκολα να δούμε ότι $\gamma_i(H) \subseteq \gamma_i(G)$ για κάθε i, χρησιμοποιώντας επαγωγή επί του i.

Αφού η G είναι μηδενοδύναμη, υπαρχει n με $\gamma_n(G) = 1$ και έτσι $\gamma_n(H) = 1$, δηλαδή η H είναι μηδενοδύναμη.

(ii) Έστω $\pi : G \to G/N$ η φυσική προβολή.

Τότε,

$$\begin{aligned}\pi(\gamma_{i+1}(G)) &= \pi([\gamma_i(G), G]) \\ &= [\pi(\gamma_i(G), \pi(G)] \\ &= [\gamma_i(\pi(G)), \pi(G)] \\ &= \gamma_{i+1}(\pi(G)),\end{aligned}$$

όπου η προτελευταία ισότητα προκύπτει μέσω επαγωγής επί του i, όπως πριν.

(iii) Αρκεί να δείξουμε το ζητούμενο για $k = 2$. Πάλι με επαγωγή διαπιστώνουμε ότι ισχύει $\gamma_i(G_1 \times G_2) \subseteq \gamma_i(G_1) \times \gamma_i(G_2)$, για κάθε i.

Εφόσον οι G_1 και G_2 είναι μηδενοδύναμες, υπάρχουν n και m έτσι ώστε $\gamma_n(G_1) = 1 = \gamma_m(G_2)$. Για $k \geq \max\{m, n\}$, έχουμε $\gamma_k(G_1 \times G_2) = 1$, και έτσι η $G_1 \times G_2$ είναι μηδενοδύναμη.

□

Σχόλιο 7.2.1. Σε αντίθεση με τις επιλύσιμες ομάδες, επεκτάσεις μηδενοδύναμων ομάδων δεν είναι εν γένει μηδενοδύναμες. Εφόσον $Z(S_3) = 1$, έχουμε ότι η S_3 δεν είναι μηδενοδύναμη, παρότι είναι επέκταση μηδενοδύναμων ομάδων.

Ορισμός 7.2.4. Έστω G ομάδα. Μια υποομάδα H της G λέγεται **υποκανονική** αν υπάρχει κανονική "σειρά" της G με αρχή την H, δηλαδή

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$$

Θεώρημα 7.2.3. *Έστω G μηδενοδύναμη ομάδα. Τότε κάθε υποομάδα H της G είναι υποκανονική.*

Απόδειξη. Αφού η G είναι μηδενοδύναμη, υπάρχει n τέτοιο ώστε $Z^n(G) = G$, και η ανωτέρα κεντρική σειρά είναι η

$$1 = Z^0(G) \lhd Z(G) \lhd \cdots \lhd Z^n(G) = G$$

Έτσι, λαμβάνουμε την

$$H = HZ^0(G) \leq HZ(G) \leq \cdots \leq HZ^n(G) = G$$

Θα δείξουμε ότι $HZ^i(G) \lhd HZ^{i+1}(G)$ για κάθε i.
Έστω $z_{i+1} \in Z^{i+1}(G)$. Αφού $Z^{i+1}(G)/Z^i(G) = Z(G/Z^i(G))$, ισχύει $z_{i+1}g \equiv gz_{i+1} \mod Z^i(G)$ για κάθε $g \in G$, ισοδύναμα $z_{i+1}^{-1}gz_{i+1} \in gZ^i(G)$ για κάθε $g \in G$.

Έτσι, $z_{i+1}HZ^i(G)z_{i+1}^{-1} \subseteq HZ^i(G)$.
Αν $h \in H$, τότε $hHZ^i(G)h^{-1} = hHh^{-1}hZ^i(G)h^{-1} = HZ^i(G)$, αφού $Z^i(G) \lhd G$. □

Θεώρημα 7.2.4. *Έστω G ομάδα τέτοια ώστε κάθε υποομάδα H της G είναι υποκανονική. Αν $H < G$, τότε $H < N_G(H)$.*

Απόδειξη. Έστω $H \leq G$. Επειδή η H είναι υποκανονική υποομάδα της G, υπάρχει

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $H_0 < H_1$. Τότε, $H < H_1 \subseteq N_G(H)$ και άρα $H < N_G(H)$. □

Θεώρημα 7.2.5. *Έστω G πεπερασμένη ομάδα. Τότε τα ακόλουθα είναι ισοδύναμα:*

(i) H G είναι μηδενοδύναμη.

(ii) Κάθε υποομάδα H της G είναι υποκανονική.

(iii) Αν $H < G$, τότε $H < N_G(H)$.

(iv) Κάθε μεγιστική υποομάδα είναι κανονική.

(v) Κάθε Sylow υποομάδα της G είναι κανονική.

(vi) H G είναι το ευθύ γινόμενο των Sylow υποομάδων της.

(vii) Για κάθε $m \Big| |G|$ υπάρχει $K \lhd G$ με $|K| = m$.

Απόδειξη. Οι συνεπαγωγές (i)⇒(ii)⇒(iii) έπονται από τα δυο προηγούμενα θεωρήματα.
(iii)⇒(iv): Αν η $M < G$ είναι μεγιστική , τότε $M \neq N_G(M)$ και $M \lhd N_G(M) = G$.
(iv)⇒(v): Έστω P Sylow υποομάδα της G έτσι ώστε $N_G(P) < M$. Τότε, $M \lhd G$ και

$$P \lhd N_G(P) \subseteq M \lhd G$$

Για κάθε $g \in G$, οι P, gpg^{-1} είναι Sylow υποομάδες της M.

Άρα, υπάρχει $x \in M$ με $gPg^{-1} = xPx^{-1}$. Δηλαδή, $x^{-1}g \in N_G(P) \subseteq M$, άρα $g \in M$-άτοπο, γιατί $M < G$.
(v)⇒(vi): Έχει αποδειχθεί.
(vi)⇒(i): Κάθε Sylow υποομάδα είναι μηδενοδύναμη ως πεπερασμένη p-ομάδα, άρα η G είναι μηδενοδύναμη ως ευθύ γινόμενο μηδενοδύναμων ομάδων.
(vi)⇒(vii): Έστω

$$G = P_1 \times P_2 \times \cdots \times P_k$$

όπου P_i είναι η Sylow p_i υποομάδα της G. Έστω $m = \prod_{i=1}^{k} p_i^{\sigma_i} \Big| |G|$, $\sigma_i \leq a_i$. Για κάθε i υπάρχει $A_i \lhd P_i$ με $|A_i| = p_i^{\sigma_i}$. Τότε, αν

$$\overline{A} = A_1 \times A_2 \times \cdots \times A_k$$

έχουμε $|\overline{A}| = m$ και $\overline{A} \lhd G$.
(vii)⇒(vi): Άμεσο. □

Παράδειγμα 7.2.2. Έστω G μηδενοδύναμη ομάδα τάξεως $6 = 2 \cdot 3$.

Αν P Sylow 2-υποομάδα της G, τότε $P = \mathbb{Z}_2$, και αν Q Sylow 3-υποομάδα της G, τότε $Q = \mathbb{Z}_3$.

Από το προηγούμενο Θεώρημα, $G = \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6$. Συνεπώς, υπάρχει μόνο μια μηδενοδύναμη ομάδα τάξεως 6.

Το ίδιο ισχύει για ομάδες τάξης pq, όπου p, q είναι πρώτοι με $p \neq q$.

Πρόταση 7.2.3. *Αν η G είναι μηδενοδύναμη και $1 \neq N \lhd G$, τότε $N \cap Z(G) \neq 1$.*

Απόδειξη. Εφόσον η G είναι μηδενοδύναμη υπάρχει κεντρική σειρά

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G,$$

ισοδύναμα $[G_i, G] \leq G_{i-1}$ για κάθε i.

Εφόσον $N \neq 1$, υπάρχει i με $N \cap G_i = 1$ και $N \cap G_{i+1} \neq 1$, άρα

$$\begin{aligned}[N \cap G_{i+1}, G] &\leq N \cap [G_{i+1}, G] \\ &\leq N \cap G_i \\ &= 1\end{aligned}$$

οπότε $[\underbrace{N \cap G_{i+1}}_{\neq 1}, G] = 1$.

Αν $1 \neq \omega \in N \cap G_{i+1}$, τότε $\omega g \omega^{-1} g^{-1} = 1$ για κάθε $g \in G$, ισοδύναμα $\omega g = g\omega$ για κάθε $g \in G$, ισοδύναμα $\omega \in Z(G) \cap N$, και έτσι $N \cap Z(G) \neq 1$. □

Παράδειγμα 7.2.3. Βρίσκουμε τις κανονικές υποομάδες της S_n.
Ξέρουμε ότι η A_n είναι απλή για κάθε $n \geq 5$. Έστω $n \geq 5$.

Επειδή $[S_n : A_n] = 2$, έχουμε $A_n \lhd S_n$.

Έστω $N \lhd S_n$, τότε $N \cap A_n \lhd A_n$. Όμως η A_n είναι απλή, άρα $N \cap A_n = A_n$ ή 1.

- Αν $N \cap A_n = A_n$, τότε $A_n \leq N$, άρα $A_n = N$ ή $A_n < N$.

  Αν $A_n < N$, τότε $|N| \geq 2|A_n|$ και $|S_n| = 2|A_n|$, άρα $N = S_n$.

- Αν $N \cap A_n = 1$, τότε $N, A_n \leq S_n$ και $|NA_n| = |N||A_n|$, άρα $N = 1$ ή $|N| = 2$. Αν $|N| = 2$, τότε $N = \langle \omega \rangle \lhd S_n$ με $o(\omega) = 2$ και $\sigma\omega\sigma^{-1} \in N$ για κάθε $\sigma^{-1} \in S_n$, δηλαδή $\sigma\omega\sigma^{-1} = \omega$ για κάθε $\sigma \in S_n$. Τότε, $\sigma\omega = \omega\sigma$ για κάθε $\sigma \in S_n$, οπότε $\omega \in Z(S_n) = 1$.

  Άρα δεν υπάρχει κανονική υποομαδα της S_n με τάξη 2 διότι αυτή θα ήταν υποομάδα του κέντρου.

Άρα οι μόνες κανονικές υποομάδες της S_n είναι οι $1, A_n, S_n$ για $n \geq 5$.

Για $n = 4$, οι κανονικές υποομάδες της S_4 είναι οι $1, A_4, S_4, V$, όπου

$$V = \{1, (12)(34), (13)(24), (14)(32)\} \leq S_4$$

7.3 Ασκήσεις

1. Έστω $H, K \leq G$ και
$$[H, K] = \langle [h, k] : h \in H, k \in K \rangle$$
Να δείξετε ότι $[H, K] = [K, H]$ και $[H, K] \lhd \langle H, K \rangle$.
[Υπόδειξη: $[a, bc] = [a, b][a, c]^b$ και $[ab, c] = [b, c]^a[a, c]$, όπου $x^b = bxb^{-1}$.]

2. Έστω $N \leq G$. Τότε $N \lhd G$ ανν $[G, N] \leq N$.

3. Αν $N \lhd G$, $A, B \leq G$, τότε
$$[AN/N, BN/N] = [A, B]N/N$$

4. Αν H, K, Λ, M ομάδες, τότε
$$[H \times K, \Lambda \times M] = [H, \Lambda] \times [K, M]$$

5. Κάθε όρος της ανωτέρας κεντρικής σειράς είναι χαρακτηριστική υποομάδα της G.

6. Κάθε όρος της κατωτέρας κεντρικής σειράς είναι πλήρως αναλλοίωτη υποομάδα της G, $\gamma_i(G) \underset{\pi.\alpha.}{\leq} G$.

7. Έστω G πεπερασμένη μηδενοδύναμη ομάδα και $H \leq G$ με $[G : H] < \infty$. Να αποδειχθεί ότι $g^n \in G$ για κάθε $g \in G$.

8. Να αποδειχθεί ότι η D_n είναι μηδενοδύναμη ανν $n = 2^k$.

9. Αν $H \leq Z(G)$ και η G/H είναι μηδενοδύναμη, τότε η G είναι μηδενοδύναμη.

10. Αν P είναι μια Sylow p-υποομάδα μιας μηδενοδύναμης ομάδας G, τότε $Z(P) \leq Z(G)$.

11. Να εξεταστεί αν επιλέπτυνση κεντρικής σειράς μιας ομάδας G είναι κεντρική σειρά της G.

12. Μια πεπερασμένη μηδενοδύναμη ομάδα έχει κεντρική σειρά με πηλίκα τάξης p για κάποιο πρώτο p.

13. Αν η $\mathrm{Aut}(G)$ είναι μηδενοδύναμη, τότε η G είναι μηδενοδύναμη.

14. Έστω G πεπερασμένα παραγόμενη μηδενοδύναμη ομάδα. Αν $H \leq G$, τότε η H είναι πεπερασμένα παραγόμενη.

15. Έστω G πεπερασμένη ομάδα. Αποδείξτε ότι η G είναι μηδενοδύναμη ανν για κάθε α, $\beta \in G$ με $(o(\alpha), o(\beta)) = 1$, ισχύει $\alpha\beta = \beta\alpha$.

16. Έστω G μηδενοδύναμη ομάδα κλάσεως $c > 1$. Για κάθε $\alpha \in G$, η υποομάδα $H = \langle \alpha, G' \rangle$ είναι μηδενοδύναμη κλάσεως μικρότερης του c.

17. Σε μια μηδενοδύναμη, ελευθέρα στρέψης ομάδα G η εξαγωγή των ριζών -όταν αυτές υπάρχουν- είναι μοναδική. Δηλαδή, αν $\alpha^n = \beta^n$, για $n > 0$, τότε $\alpha = \beta$.
[Υπόδειξη: $\alpha, \beta\alpha\beta^{-1} \in \langle \alpha, G' \rangle$.]

18. Έστω G μηδενοδύναμη ομάδα κλάσης 2 και $g \in G$. Τότε, η συνάρτηση

$$\phi : G \to G, \quad x \mapsto [g, x]$$

είναι ομομορφισμός.

Συμπεράνετε ότι $C_G(g) \lhd G$.

[Υπόδειξη: $[g, xy] = [g, x][g, y]$ ανν $[x, g^{-1}]y^{-1}[g^{-1}, x]y = 1$.]

19. *(Mal'cev) Έστω G μηδενοδύναμη ομάδα της οποίας το κέντρο $Z(G)$ είναι ομάδα ελευθέρα στρέψης. Τότε:

(i) Κάθε πηλίκο $Z^{n+1}(G)/Z^n(G)$ της ανωτέρας κεντρικής σειράς είναι ομάδα ελευθέρα στρέψης.

(ii) Η G είναι ελευθέρα στρέψης.
[Υπόδειξη: Θεωρήστε ομομορφισμό $Z^{n+1}(G)/Z^n(G) \to Z^n(G)/Z^{n-1}(G)$, χρησιμοποιώντας την προηγούμενη άσκηση.]