834. Θεωρία Ομάδων

Τμήμα Μαθηματικών

Πανεπιστήμιο Αθηνών
Αθήνα, 2013

Μήνυμα του καθηγητή

"Προσοχή, τα κεφάλαια 8 και 9 αποτελούν κακή μεταφορά ("αντιγραφή" με πολλά λάθη και ελλείψεις) μέρους μεταπτυχιακού μαθήματος που έκανα, από το άτομο που "πέρασε" σε αρχείο tex τις σημειώσεις. Αν σας ενδιαφέρουν και αυτά μπορείτε να τα βρείτε τις σημειώσεις μου στην eclass στα μεταπτυχιακά. Τα κεφάλαια από 1 εώς 7 τα έχω διορθώσει και έχουν περάσει οι διορθώσεις στο κείμενο από αυτόν που έγραφε τις σημειώσεις σε tex, αλλά αυτή τη στιγμή δεν έχω στη διάθεσή μου το αρχείο tex προκειμένου να επέμβω στο κείμενο. Στη θέση σας θα περιοριζόμουν λοιπόν στα κεφάλαια από 1 εώς 7."

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,

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

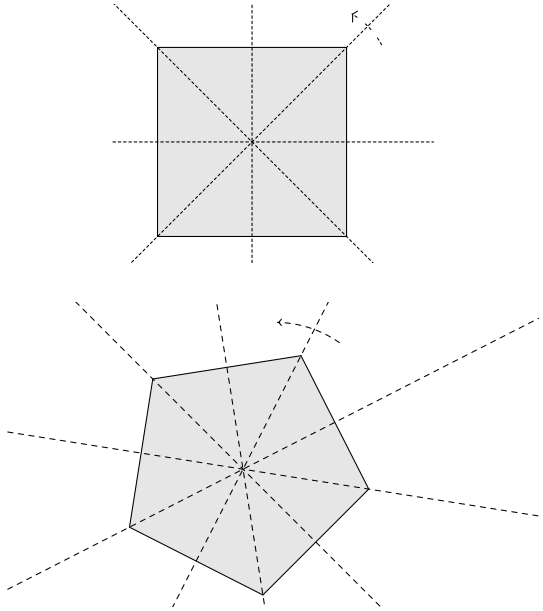
είναι ομάδα με πράξη τη σύνθεση.

(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.

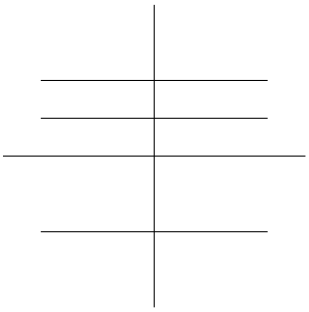
□

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

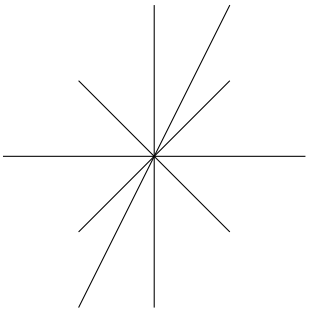
$$a \sim b \iff b^{-1}a \in H$$

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 ανν* $\ker\phi = \{1\}$.

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 $\rho_H(g) = 1 \Leftrightarrow g \cdot xH = xH \quad \forall x \in G \Leftrightarrow g \in xHx^{-1} \quad \forall x \in G \Leftrightarrow g \in \bigcap_{x \in G} xHx^{-1}$, 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.]

Κεφάλαιο 8

Πολυκυκλικές και Προσεγγιστικά Πεπερασμένες Ομάδες

8.1 Πολυκυκλικές ομάδες

Ορισμός 8.1.1. Μια ομάδα G λέγεται **πολυκυκλική** αν έχει κανονική σειρά της οποίας κάθε πηλίκο είναι κυκλική ομάδα.

Δηλαδή, υπάρχει κανονική σειρά

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

έτσι ώστε η G_{i+1}/G_i να είναι κυκλική για κάθε i.

Μια τέτοια σειρά θα λέγεται **πολυκυκλική σειρά**.

Παρατήρηση 8.1.1. Κάθε πολυκυκλική ομάδα είναι επιλύσιμη.

Θεώρημα 8.1.1. *Κάθε πολυκυκλική ομάδα είναι πεπερασμένα παραγόμενη.*

Απόδειξη. Έστω G πολυκυκλική ομάδα και

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

μια πολυκυκλική σειρά της.

Για κάθε $i = 0, 1, \ldots, n-1$, έστω $G_{i+1}/G_i = \langle x_i G \rangle$. Αν $g \in G$, τότε $g \in G_i$ για κάποιο i και

$$\begin{aligned} g &= x_i^{k_i} \underbrace{g_{i-1}}_{\in G_{i-1}} \\ &= x_i^{k_i} x_{i-1}^{k_{i-1}} \underbrace{g_{i-1}}_{\in G_{i-2}} \\ &\vdots \\ &= x_i^{k_i} x_{i-1}^{k_{i-1}} \cdots x_0^{k_0} \end{aligned}$$

Άρα, κάθε στοιχείο της G γράφεται ως

$$x_{n-1}^{k_{n-1}} x_{n-2}^{k_{n-2}} \cdots x_0^{k_0}$$

Δηλαδή, το $\{x_0, x_1, \ldots, x_{n-1}\}$ είναι ένα πεπερασμένο σύνολο γεννητόρων της G, άρα η G είναι πεπερασμένα παραγόμενη. □

Παρατήρηση 8.1.2. Αν G πολυκυκλική ομάδα, με όλα τα στοιχεία πεπερασμένης τάξης, τότε η G είναι πεπερασμένη.

Πράγματι, αφού κάθε x_i είναι πεπερασμένης τάξης, το $x_i^{k_i}$ έχει πεπερασμένες "επιλογές", και έτσι η G είναι πεπερασμένη.

Θεώρημα 8.1.2. *Η κλάση των πολυκυκλικών ομάδων είναι κλειστή ως προς υποομάδες, πηλίκα, και επεκτάσεις.*

Απόδειξη. Έστω

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

πολυκυκλική σειρά της G.

(i) Έστω $H \leq G$. Η

$$1 = H \cap G_0 \lhd H \cap G_1 \lhd \cdots \lhd H \cap G_n = H$$

είναι πολυκυκλική σειρά της H, άρα η H είναι πολυκυκλική.

Πράγματι, για κάθε πηλίκο ισχύει $(H \cap G_{i+1})/(H \cap G_i) \hookrightarrow G_{i+1}/G_i$, η οποία είναι κυκλική.

(ii) Έστω $N \lhd G$ και G/N η ομάδα πηλίκο. Τότε, αν $\pi : G \to G/N$, η σειρά

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

είναι πολυκυκλική σειρά της G/N, άρα η G/N είναι πολυκυκλική.

Πράγματι, η $\pi(G_{i+1})/\pi(G_i)$ είναι ισόμορφη με πηλίκο της G_{i+1}/G_i και κάθε πηλίκο κυκλικής ομάδας είναι κυκλική.

(iii) Έστω $N \lhd G$ και N, G/N πολυκυκλικές ομάδες. Αν

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

πολυκυκλική σειρά της N και

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

πολυκυκλική σειρά της G/N, όπου $G_i \lhd G_{i+1}$ και $G_i \supseteq N$, τότε η

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_m = N = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

είναι πολυκυκλική σειρά της G.

□

Παρατήρηση 8.1.3. Κάθε υποομάδα πολυκυκλικής ομάδας είναι πεπερασμένα παραγόμενη.

Θεώρημα 8.1.3. *Μια ομάδα είναι πολυκυκλική ανν είναι επιλύσιμη και κάθε υποομάδα της είναι πεπερασμένα παραγόμενη.*

Απόδειξη. Αν η G είναι πολυκυκλική, είδαμε προηγουμένως ότι είναι επιλύσιμη και κάθε υποομάδα της είναι πεπερασμένα παραγόμενη.

Αντίστροφα, έστω G επιλύσιμη ομάδα έτσι ώστε κάθε υποομάδα της να είναι πεπερασμένα παραγόμενη.

Παίρνουμε επιλύσιμη σειρά

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

της G. Από την υπόθεση, κάθε G_i είναι πεπερασμένα παραγόμενη ομάδα, και έτσι κάθε πηλίκο G_{i+1}/G_i είναι αβελιανή πεπερασμένα παραγόμενη ομάδα.

Συνεπώς, κάθε G_{i+1}/G_i είναι (πεπερασμένο) ευθύ άθροισμα κυκλικών ομάδων.

Έπεται ότι μπορούμε να επιλεπτύνουμε την αρχική κανονική σειρά και να προκύψει κανονική σειρά με κυκλικά πηλίκα. Δηλαδή, η G θα είναι πολυκυκλική. □

Ισχύει το εξής διάγραμμα

$$\{\text{π.π. αβελιανές}\} \subsetneq \{\text{π.π. μηδενοδύναμες}\} \subsetneq \{\text{πολυκυκλικές}\} \subsetneq \{\text{π.π. επιλύσιμες}\}$$

Παραδείγματα πεπερασμένα παραγόμενων μηδενοδύναμων ομάδων που δεν είναι αβελιανές συναντάμε σε ομάδες πινάκων.

Ένα παράδειγμα πολυκυκλικής ομάδας, που δεν είναι μηδενοδύναμη είναι η S_3, αφού η

$$1 \lhd A_3 \lhd S_3$$

είναι πολυκυκλική σειρά.

Τέλος, δίνουμε ένα παράδειγμα πεπερασμένα παραγόμενης επιλύσιμης ομάδας η οποία δεν είναι πολυκυκλική.

Έστω $N = \bigoplus_{-\infty}^{\infty} \mathbb{Z}$ και $H = \langle 1 \rangle \simeq \mathbb{Z}$. Παίρνουμε δράση με αυτομορφισμούς της H στην N ως εξής: $1 \cdot (x_i)_{i\in\mathbb{Z}} = (x_{i-1})_{i\in\mathbb{Z}}$, δηλαδή μεταθέτουμε μια θέση δεξιά.

Έστω $G = N \overset{\phi}{\rtimes} H$ το αντίστοιχο ημιευθύ γινόμενο. Τότε, η G είναι επιλύσιμη ως επέκταση επιλύσιμων, ενώ δεν είναι πολυκυκλική, γιατί περιέχει υποομάδα, η οποία δεν είναι πεπερασμένα παραγόμενη.

Επιπλέον, η G είναι πεπερασμένα παραγόμενη. Αν $t = ((0), 1)$ και $x = ((\delta_{i_0})_{i\in\mathbb{Z}}, 0)$, όπου $\delta_{i_0} = 1$ αν $i = 0$ και 0 διαφορετικά, τότε $G = \langle t, x \rangle$.

Πρόταση 8.1.1. *Σε μια πολυκυκλική ομάδα G, το πλήθος των πηλίκων μιας πολυκυκλικής σειράς που είναι άπειρες κυκλικές δεν εξαρτάται από την πολυκυκλική σειρά, δηλαδή είναι αναλλοίωτο της ομάδας και ονομάζεται* ***αριθμός του Hirsoh****, και συμβολίζεται με $h(G)$.*

Απόδειξη. Ο ισχυρισμός προκύπτει από τις ακόλουθες παρατηρήσεις:

- Κανονικές σειρές έχουν ισόμορφες επιλεπτύνσεις.
- Μια επιλέπτυνση πολυκυκλικής σειράς έχει το ίδιο πλήθος άπειρων κυκλικών πηλίκων με την αρχική σειρά.

  Πράγματι, έστω $H \lhd K$ και $K/H \simeq \mathbb{Z}$. Αν $H \lhd \Lambda \lhd K$ με $H \neq \Lambda \neq K$, τότε $\Lambda/H \lneq K/H$, άρα είναι άπειρη κυκλική, $\Lambda/H = m\mathbb{Z}$.

  Επίσης, αφού $K/H = \mathbb{Z}$, το πηλικό $\frac{K/H}{\Lambda/H} \simeq K/\Lambda \simeq \mathbb{Z}_m$ είναι πεπερασμένο.

□

Ορισμός 8.1.2. Μια πολυκυκλική ομάδα G λέγεται **πολυάπειρη κυκλική** (ή πολυ-$\mathbb{Z}$), αν έχει μια κανονική σειρά της οποίας κάθε πηλίκο είναι άπειρη κυκλική ή αν είναι τετριμμένη.

Παρατήρηση 8.1.4. Η κλάση των πολυάπειρων κυκλικών ομάδων είναι κλειστή ως προς υποομάδες.

Θεώρημα 8.1.4. *Έστω G πολυάπειρη κυκλική ομάδα. Τότε :*

(i) Η G περιέχει πολυάπειρη κυκλική κανονική υποομάδα πεπερασμένου δείκτου.

(ii) Η G περιέχει άπειρη κανονική αβελιανή υποομάδα, ελευθέρα στρέψης.

Απόδειξη. (i) Έστω

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

πολυκυκλική σειρά της G. Θα δείξουμε με επαγωγή επί του n, ότι κάθε G_n περιέχει πολυ-$\mathbb{Z}$, κανονική υποομάδα πεπερασμένου δείκτη.

Για $n = 0$, $G_0 = 1$ και η 1 είναι πολυ-$\mathbb{Z}$.

Έστω ότι $N \lhd G_{n-1}$ με N πολυ-$\mathbb{Z}$ και $[G : N] < \infty$. Τότε, η N περιέχει χαρακτηριστική υποομάδα M πεπερασμένου δείκτη στην G_{n-1}. Άρα, $M \lhd G_n$ και η M είναι πολυ-$\mathbb{Z}$, ως υποομάδα της N.

Αν η G_n/G_{n-1} είναι πεπερασμένη, τότε η M είναι η ζητούμενη υποομάδα της G_n, γιατί $[G_n : M] < \infty$.

Αν $G_n/G_{n-1} = \langle xG_{n-1}\rangle \simeq \mathbb{Z}$, τότε $x \notin G_{n-1} \supseteq M$. Παίρνουμε $H = \langle x\rangle M$. Η υποομάδα H είναι πολυ-$\mathbb{Z}$, γιατί η M είναι πολυ-$\mathbb{Z}$ και $H/M = \langle xM\rangle \simeq \mathbb{Z}$, αφού $x \notin M$.

Επίσης, η H είναι πεπερασμένου δείκτη στην G_n. Πράγματι, εφόσον $[G_{n-1} : M] < \infty$, έχουμε ότι $G_{n-1} = \bigsqcup_{i=1}^{k} M\alpha_i$, όπου $\alpha_i \in G_{n-1}$ και

$$G_n \ni g = x^i \underbrace{g_{n-1}}_{\in G_{n-1}} = x_i \cdot \mu \cdot \alpha_\lambda \in H\alpha_\lambda$$

Έπεται ότι $[G_n : H] \leq [G_{n-1} : M] < \infty$.

Έστω K η κανονική υποομάδα πεπερασμένου δείκτη στην G, που περιέχεται στην H. Τότε, η K είναι πολυ-$\mathbb{Z}$, ως υποομάδα της H, $K \lhd G_n$ και $[G_n : K] < \infty$.

(ii) Έστω N η κανονική υποομάδα της G που είναι πολυ-$\mathbb{Z}$ και $[G_n : N] < \infty$. Η υποομάδα N είναι επιλύσιμη. Άρα, αν $N^{(i)}$, ο i-όρος της παραγώγου σειράς, έχουμε ότι $N^{(d)} = 1$ και $N^{(d-1)} \neq 1$, για κάποιο d.

Έπεται ότι η $N^{(d-1)}$ είναι αβελιανή και $N^{(d-1)} \lhd G$, γιατί η $N^{(d-1)}$ είναι χαρακτηριστική στην $N \lhd G$.

Η υποομάδα N είναι ελευθέρα στρέψης, ως επέκταση υποομάδων ελευθέρας στρέψης.

Έτσι, η $N^{(d-1)}$ είναι ελευθέρα στρέψης. ως υποομάδα της N, αβελιανή, $N^{(d-1)} \lhd G$ και άπειρη.

□

Πρόταση 8.1.2. *Έστω G πολυκυκλική ομάδα και $H, N \leq G$ με $N \lhd G$. Τότε, οι H, N, G/N είναι πολυκυκλικές και $h(H) \leq h(G)$, $h(G) = h(N) + h(G/N)$.*

Επιπλέον, $h(H) = h(G)$ ανν $[G : H] < \infty$.

Απόδειξη. Αν

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

πολυκυκλική σειρά της G, τότε η

$$1 = H \cap G_0 \lhd H \cap G_1 \lhd \cdots \lhd H \cap G_n = H$$

είναι πολυκυκλική σειρά της H, αφού $(H \cap G_{i+1})/(H \cap G_i) \hookrightarrow G_{i+1}/G_i$.

Έπεται ότι $h(H) \leq h(G)$.

Αν

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

πολυκυκλική σειρά της N και

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

πολυκυκλική σειρά της G/N, τότε η

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_m = N = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

είναι πολυκυκλική σειρά της G.

Εφόσον $G_{i+1}/G_i \simeq \frac{G_{i+1}/N}{G_i/N}$, έχουμε ότι $h(G) = h(N) + h(G/N)$.

Έστω, τώρα, ότι $[G : H] < \infty$. Η υποομάδα H περιέχει κανονική υποομάδα της G, πεπερασμένου δείκτη, έστω N. Τότε,

$$\begin{aligned} h(H) &= h(N) + h(H/N) \\ &= h(N) + h(G/N) \\ &= h(G) \end{aligned}$$

Αντίστροφα, έστω ότι $h(H) = h(G)$. Θα δείξουμε ότι $[G : H] < \infty$, με επαγωγή στο $h(G)$.

Αν $h(G) = 0$, δηλαδή αν η G είναι πεπερασμένη, τότε το ζητούμενο είναι άμεσο. Έστω, λοιπόν, ότι η G είναι άπειρη.

Από το προηγούμενο θεώρημα, η G περιέχει κανονική, αβελιανή, ελευθέρα στρέψης υποομάδα N. Παρατηρούμε ότι, $h(H \cap N) \leq h(N)$, και $h(H/H \cap N) \leq h(G/N)$, αφού $H/H \cap N \hookrightarrow G/N$.

Άρα,

$$\begin{aligned} h(H) &= h(H \cap N) + h(H/H \cap N) \\ &\leq h(N) + h(G/N) \\ &= h(G) \end{aligned}$$

Εφόσον $h(H) = h(G)$, έπεται ότι $h(N) = h(H \cap N)$. Αυτό σημαίνει ότι η $N/H \cap N$ είναι πεπερασμένη.

Πράγματι, αν υποθέσουμε ότι η $N/H \cap N$ είναι άπειρη, τότε $N/H \cap N = \mathbb{Z} \oplus A$, γιατί η $N/H \cap N$ είναι πεπερασμένα παραγόμενη αβελιανή ομάδα.

Άρα, $h(N/H \cap N) > 0$ και

$$h(N) = h(H \cap N) + h(N/H \cap N) > h(H \cap N)$$

άτοπο.

Εφόσον η $H \cap N$ είναι πεπερασμένου δείκτη στην N, η $H \cap N$ περιέχει χαρακτηριστική υποομάδα M στην N, με $[N : M] < \infty$. Άρα, $M \lhd G$ και $M \subseteq H$.

Η M είναι άπειρη, ως ομάδα πεπερασμένου δείκτη στην άπειρη N. Άρα, $h(M) > 0$ και

$$\begin{aligned} h(H/M) &= h(H) - h(M) \\ &= h(G) - h(M) \\ &= h(G/M) \\ &< h(G) \end{aligned}$$

Από την επαγωγική υπόθεση, $[G/M : H/M] < \infty$ και από το Θεώρημα της Αντιστοιχίας, $[G : H] < \infty$. □

Παρατήρηση 8.1.5. Όλα τα παραπάνω γενικεύονται για ομάδες που περιέχουν πολυκυκλική υποομάδα πεπερασμένου δείκτη.

Παράδειγμα 8.1.1. Έστω G ομάδα και $H \leq G$ πολυκυκλική με $[G : H] < \infty$. Ορίζουμε $h(G) = h(H)$.

Αν H_1, H_2 πολυκυκλικές πεπερασμένου δείκτη στην G, τότε $h(H_1) = h(H_2)$.

Πράγματι, η $H_1 \cap H_2$ είναι πεπερασμένου δείκτη στην G, και πεπερασμένου δείκτη στις H_1 και H_2, άρα

$$h(H_1) = h(H_1 \cap H_2) = h(H_2)$$

Αναφέρουμε χωρίς απόδειξη τα εξής τρία σημαντικά θεωρήματα:

Θεώρημα 8.1.5 (Mal'cev, 1951). *Μια επιλύσιμη $\mathbb{Z}$-γραμμική ομάδα, δηλαδή $G \hookrightarrow GL_n(\mathbb{Z})$, είναι πολυκυκλική.*

Θεώρημα 8.1.6 (Auslandor-Swan, 1967). *Κάθε ομάδα που περιέχει πολυκυκλική υποομάδα πεπερασμένου δείκτη, είναι $\mathbb{Z}$-γραμμική.*

Σχόλιο 8.1.1. Το Θεώρημα Auslandor-Swan είναι ουσιαστικά το αντίστροφο του Θεωρήματος Mal'cev.

Θεώρημα 8.1.7 (Tits, 1972). *Έστω G γραμμική ομάδα επί ενός σώματος F.*

(i) Αν $\chi(F) = 0$, τότε η G περιέχει είτε επιλύσιμη ομάδα πεπερασμένου δείκτη, είτε ελεύθερη ομάδα διάστασης 2.

(ii) Αν $\chi(F) \neq 0$, και η G είναι πεπερασμένα παραγόμενη, τότε η G περιέχει είτε επιλύσιμη ομάδα πεπερασμένου δείκτη, είτε ελεύθερη ομάδα διάστασης 2.

8.2 Προσεγγιστικά πεπερασμένες ομάδες

Ορισμός 8.2.1. Μια ομάδα G λέγεται **προσεγγιστικά πεπερασμένη**, αν για κάθε $g \in G$ υπάρχει πεπερασμένη ομάδα K και ομομορφισμός $\phi : G \to K$ με $\phi(g) \neq 1$.

Παρατήρηση 8.2.1. Τα παρακάτω είναι ισοδύναμα, για μια ομάδα G:

(i) Η G είναι προσεγγιστικά πεπερασμένη.

(ii) Για κάθε $g \in G$, υπάρχει $N \lhd G$ με $[G : N] < \infty$ και $g \notin N$.

(iii) Για κάθε $g \in G$, υπάρχει $H \leq G$ με $[G : H] < \infty$ και $g \notin H$.

(iv) Η τομή όλων των υποομάδων πεπερασμένου δείκτη είναι τετριμμένη.

(v) Η τομή όλων των κανονικών υποομάδων πεπερασμένου δείκτη είναι τετριμμένη.

Πρόταση 8.2.1. *Έστω $H \leq G$. Τότε:*

(i) Αν η G είναι προσεγγιστικά πεπερασμένη, τότε η H είναι προσεγγιστικά πεπερασμένη.

(ii) Αν η H είναι πεπερασμένου δείκτη στην G και είναι προσεγγιστικά πεπερασμένη, τότε η G είναι προσεγγιστικά πεπερασμένη

Απόδειξη. Η απόδειξη αφήνεται ως άσκηση. □

Παραδείγματα 8.2.1. (i) Κάθε πεπερασμένη ομάδα είναι προσεγγιστικά πεπερασμένη.

(ii) Η $\mathbb{Z}$ είναι προσεγγιστικά πεπερασμένη.

Αν $0 \neq n \in \mathbb{Z}$, τότε υπάρχει πρώτος $p \nmid n$ και $n \notin p\mathbb{Z}$. Ο ζητούμενος ομομορφισμός είναι ο

$$\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z},\ n \mapsto [n]_p$$

(iii) Αν $G_1, G_2, \ldots, G_n$ προσεγγιστικά πεπερασμένες ομάδες, τότε η $G = G_1 \times G_2 \times \cdots \times G_n$ είναι προσεγγιστικά πεπερασμένη.

Πράγματι, αν $g \neq 1$, και $g = g_1 g_2 \cdots g_n$, όπου $g_i \in G_i$, τότε υπάρχει i_0 με $g_{i_0} \neq 1$ και ο ζητούμενος ομομορφισμός είναι ο

$$G \to G_{i_0} \xrightarrow{\phi} K$$

$$g \mapsto g_{i_0} \mapsto \phi(g_{i_0}) \neq 1$$

Από το παράδειγμα (iii) προκύπτει άμεσα ότι:

Πρόταση 8.2.2. *Κάθε πεπερασμένα παπαραγόμενη αβελιανή ομάδα είναι προσεγγιστικά πεπερασμένη.*

Λήμμα 8.2.1. *Έστω A πεπερασμένα παραγόμενη αβελιανή ομάδα και $A^n = \{\alpha^n : \alpha \in A\}$. Η A^n είναι χαρακτηριστική υποομάδα της A, τέτοια ώστε:*

(i) $[A : A^n] < \infty$ για κάθε n, και

(ii) $\bigcap_{n \geq 1} A^n = 1$.

Απόδειξη. Εφόσον η A είναι πεπερασμένα παραγόμενη αβελιανή, τότε $A = \prod_{i=1}^{k} A_i$, όπου κάθε A_i είναι κυκλική, άπειρη ή πεπερασμένη.

(i) Έχουμε $A^n = \prod_{i=1}^{k} A_i^n$ και άρα η $A/A^n = \prod_{i=1}^{k} A_i/A_i^n$ είναι πεπερασμένη, γιατί κάθε A_i/A_i^n είναι πεπερασμένη ομάδα.

(ii) Ισχύει $\bigcap_{n\geq 1} A^n = \prod_{i=1}^{k} \bigcap_{n\geq 1} A_i^n = 1$, γιατί $\bigcap_{n\geq 1} A_i^n = 1$, αφού κάθε A_i είναι κυκλική.

Πράγματι, αν $A_i = \mathbb{Z}$, τότε

$$\bigcap_{n\geq 1} A_i^n = \bigcap_{n\geq 1} n\mathbb{Z} = 1$$

ενώ αν $A_i = \mathbb{Z}_m$, τότε

$$\bigcap_{n\geq 1} A_i^n = \bigcap_{n\geq 1} n\mathbb{Z}_m \subseteq m\mathbb{Z}_m = 1$$

□

Θεώρημα 8.2.1. *Κάθε πολυκυκλική ομάδα G είναι προσεγγιστικά πεπερασμένη.*

Απόδειξη. Με επαγωγή στο $h(G)$.

Αν $h(G) = 0$, τότε η G είναι πεπερασμένη.

Έστω, λοιπόν, ότι η G είναι άπειρη και έστω A κανονική, άπειρη, ελευθέρα στρέψης, αβελιανή υποομάδα της G. Εφόσον η G είναι πολυκυκλική, η A είναι πεπερασμένα παραγόμενη, άρα $\bigcap_{n\geq 1} A^n = 1$ και $[A : A^n] < \infty$, για κάθε n.

Εφόσον, η A είναι άπειρη, κάθε A^n είναι άπειρη και κανονική στην G, γιατί $A^n \trianglelefteq A \triangleleft G$. Συνεπώς, $h(G/A^n) < h(G)$, γιατί $h(G) = h(A^n) + h(G/A^n)$. Από την επαγωγική υπόθεση, η G/A^n είναι προσεγγιστικά πεπερασμένη ομάδα για κάθε n.

Έστω $g \in G$ με $1 \neq g$. Εφόσον $\bigcap_{n\geq 1} A^n = 1$, υπάρχει n_0 έτσι ώστε $g \notin A^{n_0}$ και η G/A^{n_0} είναι προσεγγιστικά πεπερασμένη. Άρα, υπάρχει ομομορφισμός $\phi : G/A^{n_0} \to K$, όπου K πεπερασμένη ομάδα, με $\phi(gA^{n_0}) \neq 1$.

Παίρνουμε τον ομομορφισμό

$$G \xrightarrow{\pi} G/A^{n_0} \xrightarrow{\phi} K$$

$$g \mapsto gA^{n_0} \mapsto \phi(gA^{n_0}) \neq 1$$

και άρα, η G είναι προσεγγιστικά πεπερασμένη. □

Θεώρημα 8.2.2. *Η ομάδα $GL_n(\mathbb{Z})$ είναι προσεγγιστικά πεπερασμένη.*

Απόδειξη. Έστω $g \in GL_n(\mathbb{Z})$ με $g = (\alpha_{ij}) \neq I_n$. Έστω $m \in \mathbb{Z}$ με $m > \max_{i,j} |a_{ij}|$.

Η φυσική προβολή $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ επάγει ομομορφισμό

$$\phi : GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}_m)$$

Από την επιλογή του m, $\phi(g) \neq I_n$, δηλαδή η $GL_n(\mathbb{Z})$ είναι προσεγγιστικά πεπερασμένη. □

Θεώρημα 8.2.3 (Mal'cev). *Έστω R πεπερασμένα παραγόμενη ακέραια περιοχή. Τότε, η ομάδα $GL_n(R)$ είναι προσεγγιστικά πεπερασμένη.*

Σχέδιο απόδειξης. Ισχύουν τα εξής, για κάθε πεπερασμένα παραγόμενη ακέραια περιοχή R:

(i) Η τομή όλων των μεγιστικών ιδεωδών είναι τετριμμένη.

(ii) Αν $\mathcal{M}$ μεγιστικό ιδεώδες του R, τότε ο $R/\mathcal{M}$ είναι πεπερασμένο σώμα.

Αν $g \in GL_n(R)$ με $g \neq I_n$, τότε $g - I_n \neq 0$ και άρα κάποιο στοιχείο r του πίνακα $g - I$ είναι διάφορο του μηδενός.

Τότε, από το (i), υπάρχει μεγιστικό ιδεώδες $\mathcal{M}$, με $r \notin \mathcal{M}$ και $R/\mathcal{M}$ πεπερασμένο σώμα, από το (ii).

Η φυσική προβολή $R \to R/\mathcal{M}$ επάγει ομομορφισμό

$$\phi : GL_n(R) \to GL_n(R/\mathcal{M})$$

με $\phi(g) \neq I_n$. □

Θεώρημα 8.2.4. *Κάθε πεπερασμένα παραγόμενη υποομάδα Γ της $GL_n(F)$, όπου F σώμα, είναι προσεγγιστικά πεπερασμένη.*

Απόδειξη. Έστω ότι $\Gamma = \langle g_1, g_2, \ldots, g_k \rangle$.

Έστω R ο υποδακτύλιος του F που παράγεται από τα στοιχεία των πινάκων $g_1, g_2, \ldots, g_k$ μαζί με το I.

Έτσι, $\Gamma \leq GL_n(R)$ και από το προηγούμενο θεώρημα η $GL_n(R)$ είναι προσεγγιστικά πεπερασμένη.

Τελικά, η Γ είναι προσεγγιστικά πεπερασμένη. □

Ένα σημαντικό αποτέλεσμα των προηγούμενων θεωρημάτων είναι το εξής:

Πόρισμα 8.2.1. *Η θεμελιώδης ομάδα μιας κλειστής υπερβολικής πολλαπλότητας διάστασης n, είναι προσεγγιστικά πεπερασμένη.*

Σχέδιο απόδειξης. Εμφυτευούμε τη θεμελιώδη ομάδα της πολλαπλότητας, $\pi(\mathcal{M})$, στην ομάδα ισομετριών του n-διάστατου υπερβολικού χώρου, $\mathrm{Isom}(H^n)$, η οποία είναι υποομάδα της $GL_n(\mathbb{R})$. □

8.2.1 Τα προβλήματα λέξης και Burnside

Υπάρχουν πολλοί λόγοι για την μελέτη της έννοιας "προσεγγιστικά πεπερασμένη ομάδα". Θα αναφερθούμε σε δύο:

(i) **Το πρόβλημα της λέξης**(Dehn [1912]): Έστω G μια ομάδα η οποία δίνεται από μια πεπερασμένη παράσταση $G = \langle X|R \rangle$.
Υπάρχει αλγόριθμος ο οποίος αποφαίνεται πότε μια δοθείσα λέξη στο αλφάβητο X αναπαριστά το τετριμμένο στοιχείο, 1_G, ή όχι;

Η απάντηση δόθηκε από τον Nobikov, το 1955, και γενικά είναι όχι.[1]

Το πρόβλημα έχει λύση, όμως, στην περίπτωση των προσεγγιστικά πεπερασμένων ομάδων.

Θεώρημα 8.2.5. *Μια πεπερασμένα παριστώμενη, προσεγγιστικά πεπερασμένη ομάδα, έχει επιλύσιμο πρόβλημα λέξης.*

(ii) **Το ασθενές πρόβλημα του Burnside**[1902]: Αν G είναι μια πεπερασμένα παραγόμενη ομάδα της οποίας κάθε στοιχείο έχει πεπερασμένη τάξη, τότε είναι η G απαραιτήτως πεπερασμένη;

Η απάντηση και εδώ είναι γενικά όχι (Gohad-Shafarevich [1964]). Η απάντηση, όμως, είναι καταφατική για τις υποομάδες της $GL_n(F)$, όπου F ένα σώμα.

[1] Να επισημάνουμε ότι υπάρχουν και τα αντίστοιχα προβλήματα του ισομορφισμού και του ομομορφισμού, με τα ίδια αποτελέσματα.

Το πρόβλημα του Burnside: Αν η G είναι μια πεπερασμένα παραγόμενη ομάδα εκθέτου N, δηλαδή $g^N = 1$ για κάθε $g \in G$, είναι η G απαραιτήτως πεπερασμένη;

Η απάντηση είναι ναι για $N = 2, 3, 4, 6$, και όχι για "αρκετά" μεγάλο περιττό N.

Το περιορισμένο πρόβλημα του Burnside:Έστω K και N θετικοί ακέραιοι. Υπάρχει (άνω) φράγμα στις τάξεις των πεπερασμένων ομάδων εκθέτου N, με K γεννήτορες;
Είναι το πλήθος $B(N, K)$ των πεπερασμένων ομάδων εκθέτου N που παράγονται από K στοιχεία πεπερασμένο;

Αποτελέσματα των Hall-Higman μαζί με την ταξινόμηση των πεπερασμένων απλών ομάδων, ανάγουν το πρόβλημα στην περίπτωση όπου το N είναι δύναμη πρώτου.

Το 1950, ο Kostrikim απέδειξε ότι η απάντηση είναι θετική όταν ο N είναι πρώτος. Το 1991 ο Zelmanov απέδειξε ότι η απάντηση είναι θετική γενικά.

Έπεται, λοιπόν, το ακόλουθο:

Θεώρημα 8.2.6. *Μια πεπερασμένα παραγόμενη, προσεγγιστικά πεπερασμένη ομάδα, πεπερασμένου εκθέτη είναι πεπερασμένη.*

Απόδειξη. Έστω G προσεγγιστικά πεπερασμένη ομάδα, πεπερασμένου εκθέτου N, που παράγεται από K το πλήθος στοιχεία. Τότε, κάθε ομάδα πηλίκο παράγεται από το πολύ K το πλήθος στοιχεία και είναι εκθέτου N.

Από το αποτέλεσμα του Zelmanov, το $B(N, K)$ είναι πεπερασμένο. Αυτό σημαίνει ότι η G έχει πεπερασμένα το πλήθος, πεπερασμένα πηλίκα.

Άτοπο, γιατί η G είναι προσεγγιστικά πεπερασμένη. □

8.3 Ασκήσεις

1. Μια ομάδα G λέγεται **Hopfian** αν δεν είναι ισόμορφη με γνήσιο πηλίκο της, ή ισοδύναμα αν $\phi : G \to G$ επιμορφισμός, τότε η ϕ είναι επιμορφισμός.

   Αποδείξτε ότι κάθε πεπερασμένα παραγόμενη προσεγγιστικά πεπερασμένη ομάδα είναι Hopfian.

2. Αν G πεπερασμένα παραγόμενη και προσεγγιστικά πεπερασμένη ομάδα, τότε η $\mathrm{Aut}(G)$ είναι προσεγγιστικά πεπερασμένη.

3. (i) Αν $G_1, G_2, \ldots, G_n$ προσεγγιστικά πεπερασμένες p-ομάδες, τότε η $G = G_1 \times G_2 \times \cdots \times G_n$ είναι προσεγγιστικά πεπερασμένη p-ομάδα.

   (ii) Κάθε πεπερασμένα παραγόμενη ελευθέρα στρέψης αβελιανή ομάδα είναι προσεγγιστικά πεπερασμένη p-ομάδα, για κάθε πρώτο p.

   (iii) Αν G πεπερασμένα παραγόμενη ελευθέρα στρέψης μηδενοδύναμη ομάδα, τότε η G είναι προσεγγιστικά πεπερασμένη p-ομάδα, για κάθε πρώτο p.

Κεφάλαιο 9

Ελεύθερες Ομάδες

9.1 Ελεύθερες αβελιανές ομάδες

Ορισμός 9.1.1. Μια αβελιανή ομάδα F λέμε ότι είναι **ελεύθερη διάστασης** n αν είναι ευθύ άθροισμα n αντιτύπων της άπειρης κυκλικής $\mathbb{Z}$.

Δηλαδή, υπάρχουν $x_i \in F$, $i = 1, 2, \ldots, n$ με

$$F = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \cdots \oplus \langle x_n \rangle$$

και $\langle x_i \rangle \simeq \mathbb{Z}$ για κάθε i.

Το $\{x_1, x_2, \ldots, x_n\}$ λέγεται **βάση** της F και λέμε ότι η F είναι ελεύθερη επί του $\{x_1, x_2, \ldots, x_n\}$.

Παρατήρηση 9.1.1. Έστω F ελεύθερη αβελιανή ομάδα διάστασης $\operatorname{rank}(F) = n$. Τότε,

$$F = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n}$$

και

$$2F = 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}$$

Έτσι,

$$\begin{aligned} F/2F &= \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z} \\ &= \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2 \end{aligned}$$

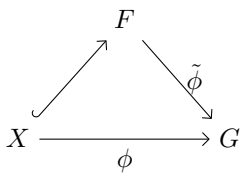
Τελικά, $|F/2F| = 2^n$, ή αλλιώς $\dim_{\mathbb{Z}_2} F/2F = n$.

Πρόταση 9.1.1. *Έστω F_1 και F_2 ελεύθερες αβελιανές ομάδες διάστασεων n_1 και n_2 αντίστοιχα. Τότε, $F_1 \simeq F_2$ ανν $n_1 = n_2$.*

Απόδειξη. Αν $F_1 \simeq F_2$ από την προηγούμενη παρατήρηση, $2^{n_1} = 2^{n_2}$, δηλαδή $n_1 = n_2$.

Το αντίστροφο είναι άμεσο. □

Θεώρημα 9.1.1 (Καθολική ιδιότητα). *Έστω F ελεύθερη αβελιανή ομάδα με βάση $\{x_1, x_2, \ldots, x_n\}$. Τότε, για κάθε αβελιανή ομάδα G και απεικόνιση $\phi : X = \{x_1, x_2, \ldots, x_n\} \to G$, υπάρχει μοναδικός ομομορφισμός $\tilde{\phi} : F \to G$ που επεκτείνει την ϕ.*



Απόδειξη. Έστω $x \in F$. Το x γράφεται κατά μοναδικό τόπο ως $x = \sum_{i=1}^{n} m_i x_i$. Ορίζουμε $\tilde{\phi}(x) = \sum_{i=1}^{n} m_i \phi(x_i)$.

Εύκολα δείχνουμε ότι η $\tilde{\phi}$ είναι ομορφισμός. Εξ' ορισμού $\tilde{\phi}(x_i) = \phi(x_i)$ για κάθε i.

Η $\tilde{\phi}$ είναι μοναδική, γιατί καθορίζεται πλήρως από τα $\phi(x_i)$, και καθιστά το παραπάνω διάγραμμα μεταθετικό. □

Παρατήρηση 9.1.2. Το n δεν είναι αναγκαστικά πεπερασμένο.

Πόρισμα 9.1.1. *Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι πηλίκο ελεύθερης αβελιανής ομάδας.*

Απόδειξη. Έστω ότι $G = \langle g_1, g_2, \ldots, g_n \rangle$.

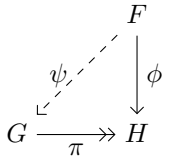
Παίρνουμε $F = \mathbb{Z}^1 \oplus \mathbb{Z}^2 \oplus \cdots \oplus \mathbb{Z}^n$, όπου $\mathbb{Z}^i = \langle x_i \rangle \simeq \mathbb{Z}$ και την απεικόνιση

$$\phi : \{x_1, x_2, \ldots, x_n\} \to G, \quad x_i \mapsto g_i$$

Από την καθολική ιδιότητα, υπάρχει $\tilde{\phi} : F \to G$ με $\tilde{\phi}(x_i) = \phi(x_i) = g_i$, για κάθε i.

Η $\tilde{\phi}$ είναι επί, γιατί τα $g_i = \tilde{\phi}(x_i)$ παράγουν την G. □

Θεώρημα 9.1.2 (Προβολική ιδιότητα). *Έστω $\pi : G \to H$ επιμορφισμός ομάδων. Αν F ελεύθερη αβελιανή ομάδα και $\phi : F \to H$ ομομορφισμός, τότε υπάρχει ομομορφισμός $\psi : F \to G$ έτσι ώστε $\phi = \pi \circ \psi$.*



Απόδειξη. Έστω $X = \{x_i\}_{i \in I}$ βάση της F. Αφού η π είναι επί, για κάθε $x_i \in X$, υπάρχει $g_i \in G$ με $\phi(x_i) = \pi(g_i)$.

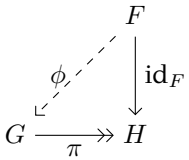
Παίρνουμε την απεικόνιση $x_i \mapsto g_i$, η οποία λόγω της καθολικής ιδιότητας επεκτείνεται σε ομομορφισμό $\psi : F \to G$.

Το διάγραμμα είναι μεταθετικό, γιατί $\pi \circ \psi(x_i) = \pi(g_i) = \phi(x_i)$ για κάθε i. □

Ορισμός 9.1.2. Μια αβελιανή ομάδα λέγεται **προβολική** αν ικανοποιεί το συμπέρασμα του παραπάνω θεωρήματος.

Λήμμα 9.1.1. *Έστω F ελεύθερη αβελιανή ομάδα, G αβελιανή ομάδα και $\pi : G \to F$ επιμορφισμός. Τότε, $G = \ker \pi \oplus H$, όπου $H \simeq F$.*

Απόδειξη. Από την προβολική ιδιότητα των ελεύθερων αβελιανών ομάδων, υπάρχει ομομορφισμός $\phi : F \to G$ με $\pi \circ \phi = \mathrm{id}_F$.



Έπεται ότι η ϕ είναι 1-1 και $\phi(F) = \mathrm{im}\, F \simeq F$. Θα δείξουμε ότι $G = \ker \pi \oplus \mathrm{im}\, \phi$.

Έχουμε ότι $\ker\pi \cap \operatorname{im}\phi = \{0\}$. Πράγματι, έστω $g \in \ker\pi \cap \operatorname{im}\phi$. Τότε, $\pi(g) = 0$ και $g = \phi(x)$, για κάποιο $x \in F$. Έτσι, $0 = \pi(g) = (\pi \circ \phi)(x) = x$, άρα $x = 0$ και $g = \phi(0) = 0$.

Παρατηρούμε, επιπλέον, ότι $\pi((\phi \circ \pi)(g)) = \pi(g)$, άρα $g - \phi(\pi(g)) \in \ker\pi$.

Τελικά, $g = g - \phi(\pi(g)) + \phi(\pi(g)) \in \ker\pi \oplus \operatorname{im}\phi$. □

Πρόταση 9.1.2. *Έστω F μια ελεύθερη αβελιανή ομάδα διάστασης n. Αν $\{0\} \subsetneq H \leq F$, τότε η H είναι ελεύθερη αβελιανή ομάδα διάστασης $\leq n$.*

Απόδειξη. Με επαγωγή επί του n.

Αν $n = 1$, τότε η F είναι η άπειρη κυκλική, η H είναι και αυτή η άπειρη κυκλική και $\operatorname{rank}(H) = 1 = \operatorname{rank}(F)$.

Έστω $n > 1$. Τότε, $F = K \oplus \mathbb{Z}$, όπου K ελεύθερη αβελιανή ομάδα διάστασης $n-1$. Παίρνουμε τον φυσικό επιμορφισμό $\pi : F \to F/K = \mathbb{Z}$. Τότε, $K = \ker\pi$.

Αν $H \subseteq \ker\pi$, τότε από την επαγωγική υπόθεση η H είναι ελεύθερη αβελιανή ομάδα διάστασης $\leq \operatorname{rank}(K) = n - 1 < n$.

Αν $H \nsubseteq \ker\pi$, τότε $\pi(H) \neq 0$ και έτσι $\pi(H) \simeq \mathbb{Z}$. Παίρνουμε τον περιορισμό $\pi|_H : H \to \pi(H) \simeq \mathbb{Z}$. Από το προηγούμενο λήμμα $H = \ker(\pi|_H) \oplus \operatorname{im}\phi$.

Όμως, $\ker(\pi|_H) = H \cap K \leq K$ και από την επαγωγική υπόθεση η $\ker(\pi|_H)$ είναι ελεύθερη αβελιανή ομάδα διάστασης $\leq n-1$.

Αφού $\operatorname{im}\phi \simeq \mathbb{Z}$, έπεται ότι η H είναι ελεύθερη αβελιανή διάστασης $\leq n$. □

Πόρισμα 9.1.2. *Αν μια πεπερασμένα παραγόμενη αβελιανή ομάδα παράγεται από n το πλήθος στοιχεία, τότε κάθε υποομάδα της μπορεί να παραχθεί από n το πολύ στοιχεία.*

Απόδειξη. Έστω $G = \langle g_1, g_2, \ldots, g_n\rangle$. Τότε, υπάρχει επιμορφισμός $\pi : F \to G$, όπου F ελεύθερη αβελιανή ομάδα διάστασης n.

Αν $H \leq G$, από το Θεώρημα της Αντιστοιχίας, $H = \Lambda/\ker\pi$, όπου $\ker\pi \leq \Lambda \leq F$. Από την προηγούμενη πρόταση, η Λ είναι ελεύθερη αβελιανή διάστασης $\leq n$.

Άρα, έπεται ότι η επιμορφική εικόνα της $\Lambda/\ker\pi = H$ μπορεί να παραχθεί από n το πολύ στοιχεία. □

9.2 Ελεύθερα γινόμενα

Έστω G_α, $\alpha \in J$ μια οικογένεια ομάδων.

Μια **λέξη μήκους** n στο **αλφάβητο** $\bigsqcup_{\alpha\in J} G_\alpha$ είναι μια πεπερασμένη ακολουθία $(g_1, \ldots, g_n)$, όπου $g_i \in \bigsqcup_{\alpha\in J} G_\alpha$.

Μια λέξη $(g_1, \ldots, g_n)$, με $g_i \in G_{\alpha_i}$ λέγεται **ανηγμένη** αν διαδοχικά g_i ανήκουν σε διαφορετικές ομάδες και $g_i \neq 1_{\alpha_i}$ για κάθε i. Δηλαδή $\alpha_i \neq \alpha_{i+1}$ και $g_i \neq 1_{\alpha_i}$ για κάθε i.

Η **κενή λέξη** $\emptyset$ είναι η ανηγμένη (μοναδική) λέξη μήκους 0.

Μια **στοιχειώδης αναγωγή** είναι μια από τις παρακάτω δυο "δράσεις":

$$(g_1, \ldots, g_i, g_{i+1}, \ldots, g_n) \mapsto (g_1, \ldots, g_i \cdot g_{i+1}, \ldots, g_n), \text{ αν } \alpha_i = \alpha_{i+1}$$

και

$$(g_1, \ldots, g_i, 1_\alpha, g_{i+1}, \ldots, g_n) \mapsto (g_1, \ldots, g_i, g_{i+1}, \ldots, g_n)$$

Έστω W το σύνολο των ανηγμένων λέξεων στο $\bigsqcup_\alpha G_\alpha$ και $\mathcal{P}(W)$ η ομάδα μεταθέσεων του W.

Για κάθε $\alpha \in J$ και $g \in G_\alpha$ ορίζουμε μετάθεση $\mathcal{L}_g^\alpha \in \mathcal{P}(W)$ ως εξής:
Αν $g = 1_\alpha$, τότε $\mathcal{L}_g^\alpha = \mathrm{id}_W$. Αν $g \neq 1_\alpha$, τότε

$$\mathcal{L}_g^\alpha(g_1, \ldots, g_n) = \begin{cases} (g, g_1, \ldots, g_n) & , \alpha \neq \alpha_1 \\ (gg_1, \ldots, g_n) & , \alpha = \alpha_1 \wedge gg_1 \neq 1_\alpha \\ (g_1, \ldots, g_n & , \alpha = \alpha_1 \wedge gg_1 = 1_\alpha \end{cases}$$

Ορίζουμε, επίσης, $\mathcal{L}_g^\alpha(\emptyset) = (g)$.
Παρατηρούμε, διακρίνοντας περιπτώσεις, ότι

$$\mathcal{L}_{g'g}^\alpha = \mathcal{L}_{g'}^\alpha \circ \mathcal{L}_g^\alpha, \ \forall\, g', g \in G_\alpha \qquad (1)$$

Συνεπώς, $\mathcal{L}_{g^{-1}}^\alpha \circ \mathcal{L}_g^\alpha = \mathcal{L}_g^\alpha \circ \mathcal{L}_{g^{-1}}^\alpha = \mathrm{id}_W$. Έπεται ότι η $\mathcal{L}_g^\alpha$ είναι 1-1 και επί, δηλαδή, πράγματι, $\mathcal{L}_g^\alpha \in \mathcal{P}(W)$.
Η απεικόνιση

$$i_\alpha : G_\alpha \to \mathcal{P}(W), \ i_\alpha(g) = \mathcal{L}_g^\alpha$$

είναι μονομορφισμός.

Πράγματι, ομομορφισμός είναι λόγω της (1). Για το 1-1, βλέπουμε ότι αν $g \in G_\alpha \backslash \{1_\alpha\}$, τότε $i_\alpha(g)(\emptyset) = \mathcal{L}_g^\alpha(\emptyset) = (g)$. Άρα $\mathcal{L}_g^\alpha \neq \mathrm{id}_W$, και έτσι η i_α είναι 1-1.

Ορισμός 9.2.1. Το **ελεύθερο γινόμενο** των G_α, $\alpha \in J$, είναι η υποομάδα της $\mathcal{P}(W)$ που παράγεται από τις υποομάδες $i_\alpha(G_\alpha)$, $\alpha \in J$, και συμβολίζεται με $\underset{\alpha \in J}{*} G_\alpha$, δηλαδή

$$\underset{\alpha \in J}{*} G_\alpha = \langle i_\alpha(G_\alpha) : \alpha \in J \rangle \leq \mathcal{P}(W)$$

Οι ομάδες G_α λέγονται (ελεύθεροι) **παράγοντες** του ελεύθερου γινομένου.

Βλέπουμε, τώρα, τις βασικές ιδιότητες του ελεύθερου γινομένου.
Παρατηρούμε ότι

$$i_\alpha(G_\alpha) \cap i_\beta(G_\beta) = 1, \ \forall\, \alpha \neq \beta \qquad (1)$$

Πράγματι, αν $g \in G_\alpha \backslash \{1_\alpha\}$ και $h \in G_\beta \backslash \{1_\beta\}$, τότε $i_\alpha(g)(\emptyset) = (g) \neq (h) = i_\beta(h)(\emptyset)$. Άρα, $i_\alpha(g) \neq i_\beta(h)$.
Εφόσον, η $\underset{\alpha \in J}{*} G_\alpha$ παράγεται από τις εικόνες $i_\alpha(G_\alpha)$, $\alpha \in J$, κάθε $g \in \underset{\alpha \in J}{*} G_\alpha$ γράφεται ως γινόμενο στοιχείων των $i_\alpha(G_\alpha)$, όπου $\alpha \in J$.

Δηλαδή,

$$g = i_{\alpha_1}(g_1) i_{\alpha_2}(g_2) \cdots i_{\alpha_n}(g_n), \ g_i \in G_{\alpha_i}$$

Αν διαδοχικά g_i ανήκουν στον ίδιο παράγοντα, έστω ότι $\alpha_i = \alpha_{i+1}$, τότε το γινόμενο $i_{\alpha_i}(g_i) i_{\alpha_{i+1}}(g_{i+1})$ μπορεί να αντικατασταθεί -λόγω της (1)- από το $i_{\alpha_i}(g_i g_{i+1})$.

Συνεπώς, κάθε στοιχείο $g \in \underset{\alpha \in J}{*} G_\alpha$ με $g \neq 1$, μπορεί να γραφεί ως πεπερασμένο γινόμενο στοιχείων των $i_\alpha(G_\alpha)$, $\alpha \in J$, σε **ανηγμένη μορφή** (κανονική μορφή), δηλαδή

$$g = i_{\alpha_1}(g_1) i_{\alpha_2}(g_2) \cdots i_{\alpha_k}(g_k), \ g_i \in G_{\alpha_i} \wedge a_i \neq a_{i+1}, \ g_i \neq 1_{\alpha_i} \forall i$$

Έτσι, διαδοχικοί όροι του γινομένου προέρχονται από διαφορετικούς παράγοντες G_α και $g_i \neq 1$ για κάθε i.

Επιπλέον, η ανηγμένη μορφή ενός στοιχείου είναι μοναδική.
Αν

$$\begin{aligned} g &= i_{\alpha_1}(g_1) i_{\alpha_2}(g_2) \cdots i_{\alpha_k}(g_k) \\ &= i_{\beta_1}(h_1) i_{\beta_2}(h_2) \cdot i_{\beta_m}(h_m) \end{aligned}$$

δύο ανηγμένες εκφράσεις του $g \neq 1$, τότε

$$\begin{aligned} g(\emptyset) &= i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k)(\emptyset) \\ &= \mathcal{L}_{g_1}^{\alpha_1} \circ \mathcal{L}_{g_2}^{\alpha_2} \circ \cdots \circ \mathcal{L}_{g_k}^{\alpha_k} \\ &= (g_1, g_2, \ldots, g_k) \end{aligned}$$

και

$$\begin{aligned} g(\emptyset) &= i_{\beta_1}(h_1)i_{\beta_2}(h_2)\cdots i_{\beta_m}(h_m)(\emptyset) \\ &= \mathcal{L}_{h_1}^{\beta_1} \circ \mathcal{L}_{h_2}^{\beta_2} \circ \cdots \circ \mathcal{L}_{h_m}^{\beta_m} \\ &= (h_1, h_2, \ldots, h_m) \end{aligned}$$

Έπεται ότι $m = k$ και $\alpha_i = \beta_i$, $g_i = h_i$ για κάθε i.

Αν

$$g = i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k),\ k > 0$$

σε ανηγμένη μορφή, τότε $g \neq 1$.

Πράγματι, $g(\emptyset) = (g_1, g_2, \ldots, g_k) \in W$, και έτσι $g \neq 1 = \mathrm{id}_W$.

Μπορούμε να ορίσουμε απεικόνιση $\phi : \underset{\alpha\in J}{*} G_\alpha \to W$ ως εξής:

Αν $g \in \underset{\alpha\in J}{*} G_\alpha \backslash \{1\}$ και

$$g = i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_k}(g_k)$$

σε ανηγμένη μορφή, τότε

$$\phi(g) = g(\emptyset) = (g_1, g_2, \ldots, g_k) \in W$$

και $\phi(1) = \emptyset$.

Εύκολα, η ϕ είναι 1-1 και επί.

Συνεπώς, μέσω της ϕ, μπορούμε να σκεφτόμαστε τα στοιχεία του ελεύθερου γινομένου ως ανηγμένες λέξεις στο $\bigsqcup_\alpha G_\alpha$.

Το γινόμενο δυο ανηγμένων λέξεων είναι η ανηγμένη λέξη που προκύπτει από την παράθεση των λέξεων με στοιχειώδεις αναγωγές

$$\underbrace{(g_1, g_2, \ldots, g_k)}_{\in W}\underbrace{(h_1, h_2, \ldots, h_m)}_{\in W} \rightsquigarrow (g_1, g_2, \ldots, g_k, h_1, h_2, \ldots, h_m) \rightsquigarrow \text{ ανηγμένη λέξη}$$

Η κενή λέξη είναι το 1 και

$$(g_1, g_2, \ldots, g_k)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_k^{-1})$$

Πρόταση 9.2.1. *Έστω G_α, $\alpha \in J$, οικογένεια ομάδων και $G = \underset{\alpha\in J}{*} G_\alpha$. Τότε:*

(i) Για κάθε $\alpha \in J$ υπάρχει εμφύτευση $i_\alpha : G_\alpha \hookrightarrow \underset{\alpha\in J}{*} G_\alpha$.

Άρα, μπορούμε να παίρνουμε τους παράγοντες G_α ως υποομάδες της G.

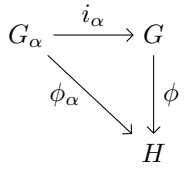
(ii) $G = \langle i_\alpha(G_\alpha) : \alpha \in J\rangle$.

(iii) Κάθε $g \in G\backslash\{1\}$ γράφεται κατά μοναδικό τρόπο ως γινόμενο στοιχείων των $i_\alpha(G_\alpha)$ σε ανηγμένη μορφή:

$$g = i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_n}(g_n)$$

όπου $g_i \in G_{\alpha_i}$, $g_i \neq 1_{\alpha_i}$ και $\alpha_i \neq \alpha_{i+1}$ για κάθε i.

Θεώρημα 9.2.1 (Καθολική ιδιότητα). *Έστω G_α, $\alpha \in J$, μια οικογένεια ομάδων και $G = \underset{\alpha\in J}{*} G_\alpha$ το ελεύθερό τους γινόμενο. Τότε, για κάθε ομάδα H και κάθε οικογένεια ομομορφισμών $\phi_\alpha : G_\alpha \to H$, $\alpha \in J$, υπάρχει μοναδικός ομομορφισμός $\phi : G \to H$ με $\phi \circ i_\alpha = \phi_\alpha$ για κάθε $\alpha \in J$.*



Απόδειξη. Εφόσον οι εικόνες $i_\alpha(G_\alpha)$, $\alpha \in J$, παράγουν την G και θέλουμε $\phi \circ i_\alpha = \phi_\alpha$, ο ϕ είναι πλήρως καθορισμένος.

Ορίζουμε, λοιπόν, τον ϕ ως εξής: Αν $g \in G\backslash\{1\}$, τότε το g γράφεται κατά μοναδικό τρόπο σε ανηγμένη μορφή

$$g = i_{\alpha_1}(g_1) i_{\alpha_2}(g_2) \cdots i_{\alpha_n}(g_n)$$

όπου $k > 0$, $g_i \neq 1$ και τα g_i, g_{i+1} δεν ανήκουν στον ίδιο παράγοντα G_α για κάθε i. Ορίζουμε, τότε,

$$\phi(g) = \phi_{\alpha_1}(g_1)\phi_{\alpha_2}(g_2) \cdots \phi_{\alpha_n}(g_n)$$

και $\phi(1) = 1$.

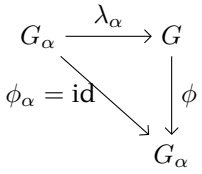
Εύκολα, ο ϕ είναι ομομορφισμός -μοναδικός ως προς αυτή την ιδιότητα- και εξ' ορισμού $\phi \circ i_\alpha = \phi_\alpha$. □

Θεώρημα 9.2.2. *Έστω G_α, $\alpha \in J$, οικογένεια ομάδων, G ομάδα και $\lambda_\alpha : G_\alpha \to G$ οικογένεια ομομορφισμών με την ακόλουθη ιδιότητα: για κάθε ομάδα H και κάθε οικογένεια ομομορφισμών $\phi_\alpha : G_\alpha \to H$, υπάρχει μοναδικός ομομορφισμός $\phi : G \to H$, με $\phi \circ \lambda_\alpha = \phi_\alpha$ για κάθε α.*

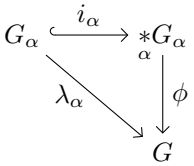
Τότε, η G είναι ισόμορφη με το ελεύθερο γινόμενο $\underset{\alpha\in J}{*} G_\alpha$, των G_α, $\alpha \in J$.

Απόδειξη. Παρατηρούμε, καταρχάς, ότι κάθε λ_α είναι μονομορφισμός.

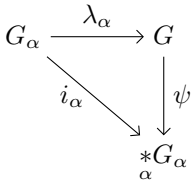
Πράγματι, αν $H = G_\alpha$, $\phi_\alpha : G_\alpha \to G_\alpha$ η ταυτοτική, και $\phi_\beta : G_\beta \to G_\alpha$ ο τετριμμένος ομομορφισμός για κάθε $\beta \neq \alpha$, τότε από την υπόθεση υπάρχει ϕ ώστε $\phi \circ \lambda_\alpha = \phi_\alpha = \mathrm{id}_\alpha$, άρα η λ_α είναι 1-1.



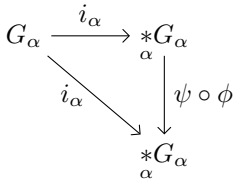
Από την καθολική ιδιότητα του ελεύθερου γινομένου $\underset{\alpha\in J}{*} G_\alpha$, υπάρχει μοναδικός ομομορφισμός $\phi : \underset{\alpha\in J}{*} G_\alpha \to G$ με $\phi \circ i_\alpha = \lambda_\alpha$.



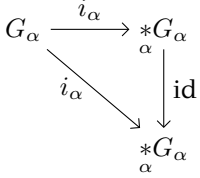
Επίσης, από την υπόθεση, υπάρχει μοναδικός ομομορφισμός $\psi : G \to \underset{\alpha\in J}{*} G_\alpha$, με $\psi \circ \lambda_\alpha = i_\alpha$.



Παρατηρούμε ότι, $\psi \circ \phi \circ i_\alpha = \psi \circ \lambda_\alpha = i_\alpha$. Δηλαδή,



Όμως, ισχύει ότι



Από την μοναδικότητα, αφού $\mathrm{id}_{\underset{\alpha\in J}{*} G_\alpha} \circ i_\alpha = i_\alpha$, έπεται ότι $\psi \circ \phi = id_{\underset{\alpha\in J}{*} G_\alpha}$.

Ομοίως, $\phi \circ \psi = \mathrm{id}_{\underset{\alpha\in J}{*} G_\alpha}$. Άρα, η ϕ είναι ισομορφισμός με $\phi^{-1} = \psi$. □

Πρόταση 9.2.2. *Έστω G_α, $\alpha \in J$, υποομάδες μιας G, με $G_\alpha \cap G_\beta = 1$ για $\alpha \neq \beta$. Τα ακόλουθα είναι ισοδύναμα:*

(i) Η G είναι το ελεύθερο γινόμενο των G_α.

(ii) Κάθε στοιχείο $g \neq 1$ της G γράφεται κατά μοναδικό τρόπο ως

$$g = g_1 g_2 \cdots g_n$$

με $n > 0$, $g_i \neq 1$ και $\alpha_i \neq \alpha_{i+1}$ για κάθε i.

(iii) Η G παράγεται από τις υποομάδες G_α και το 1 δεν μπορεί να γραφεί ως γινόμενο $g_1 g_2 \cdots g_n$ με $n > 0$, $g_i \neq 1$ και $\alpha_i \neq \alpha_{i+1}$ για κάθε i.

Απόδειξη. (i) $\Rightarrow$ (ii) Αποδείχθηκε προηγουμένως.

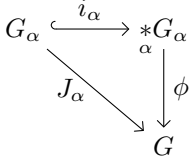
(ii) $\Rightarrow$ (iii) Έστω $g_1 g_2 \cdots g_n = 1$, όπου $g_i \in G_{\alpha_i}$ με $g_i \neq 1$ και $\alpha_i \neq \alpha_{i+1}$ για κάθε i.

Τότε, $g_1^{-1} = g_2 \cdots g_n$. Άτοπο, από την μοναδικότητα.

Η G παράγεται από τις G_α, αφού κάθε στοιχείο της G γράφεται κατά μοναδικό τρόπο ως γινόμενο στοιχείων των G_α.

(iii) $\Rightarrow$ (i) Έστω $J_\alpha : G_\alpha \to G$ η αντίστοιχη ένθεση για κάθε α.

Από την καθολική ιδιότητα του $\underset{\alpha}{*} G_\alpha$, υπάρχει μοναδικός ομομορφισμός $\phi : \underset{\alpha}{*} G_\alpha \to G$ με $\phi \circ i_\alpha = J_\alpha$.



Εφόσον οι $J_\alpha(G_\alpha) = G_\alpha$ παράγουν την G, ο ϕ είναι επί.

Έστω $g \in \ker\phi$ με $g \neq 1$. Τότε, το g γράφεται κατά μοναδικό τρόπο σε ανηγμένη μορφή. Δηλαδή,

$$g = i_{\alpha_1}(g_1)i_{\alpha_2}(g_2)\cdots i_{\alpha_n}(g_n)$$

όπου $n > 0$, $g_i \neq 1$ και $\alpha_i \neq \alpha_{i+1}$ για κάθε i. Τότε,

$$\begin{aligned} 1 =& \phi(g) \\ &= \phi \circ i_{\alpha_1}(g_1)\phi \circ i_{\alpha_2}(g_2)\cdots\phi \circ i_{\alpha_n}(g_n) \\ &= J_{\alpha_1}(g_1)J_{\alpha_2}(g_2)\cdots J_{\alpha_n}(g_n) \\ &= g_1g_2\cdots g_n \end{aligned}$$

άτοπο, από την υπόθεση.

Έτσι, $\ker\phi = 1$ και η ϕ είναι ισομορφισμός. □

Παρατήρηση 9.2.1. Έστω $\phi : G \to H$ ομομορφισμός. Αν $N \lhd G$ με $N \subseteq \ker\phi$, τότε υπάρχει μοναδικός ομομορφισμός $\tilde{\phi} : G/N \to H$ με $\tilde{\phi} \circ \pi = \phi$.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow^{\phi} & \downarrow{\scriptstyle \tilde{\phi}} \\ & & H \end{array}$$

Η $\tilde{\phi}$ ορίζεται $\tilde{\phi}(gN) = \phi(g)$ για κάθε $g \in G$.

Αν $xN = gN$, τότε $g^{-1}x \in N \subseteq \ker\phi$, άρα $\phi(g^{-1}x) = 1$. Έτσι, $\phi(g) = \phi(x)$ και η $\tilde{\phi}$ είναι καλα ορισμένη. Εύκολα φαίνεται ότι, η $\tilde{\phi}$ είναι ομομορφισμός.

Πρόταση 9.2.3. *Έστω $G = G_1 * G_2$ και $N_i \lhd G_i$, $i = 1, 2$. Αν N είναι η μικρότερη κανονική υποομάδα της G που περιέχει τις N_1 και N_2, τότε $G/N \simeq G_1/N_1 * G_2/N_2$.*

Απόδειξη. Θα δείξουμε ότι G/N ικανοποιεί την καθολική ιδιότητα.

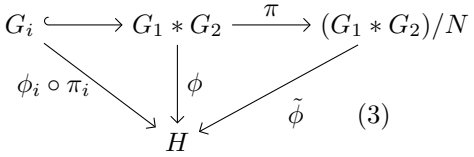
Εφόσον η N_1 περιέχεται στην $N = \ker\pi$, υπάρχει $\lambda_1 : G_1/N_1 \to (G_1 * G_2)/N$ με $\lambda_1 \circ \pi_1 = \pi$.

$$\begin{array}{ccc} G_1 & \xrightarrow{\pi_1} & G_1/N_1 \\ & \searrow^{\pi} & \downarrow{\scriptstyle \lambda_1} \\ & & (G_1 * G_2)/N \end{array} \qquad (1)$$

Ομοίως, υπάρχει $\lambda_2 : G_2/N_2 \to (G_1 * G_2)/N$ με $\lambda_2 \circ \pi_2 = \pi$.

$$\begin{array}{ccc} G_2 & \xrightarrow{\pi_2} & G_2/N_2 \\ & \searrow^{\pi} & \downarrow{\scriptstyle \lambda_2} \\ & & (G_1 * G_2)/N \end{array} \qquad (2)$$

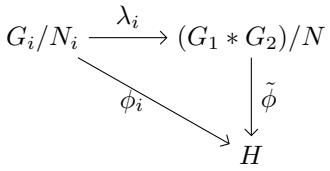
Έστω H ομάδα και $\phi_i : G_i/N_i \to H$ ομομορφισμοί για $i = 1, 2$. Από την καθολική ιδιότητα του ελεύθερου γινομένου $G_1 * G_2$, υπάρχει μοναδικός ομομορφισμός $\phi : G_1 * G_2 \to H$ με $\phi \circ i_j = \phi_j \circ \pi_j$, όπου i_j οι αντίστοιχες ενθέσεις $G_j \subseteq G_1 * G_2$, $j = 1, 2$.



(3)

Παρατηρούμε ότι $N_i \subseteq \ker \phi$, γιατί $\phi(N_i) = \phi_i \circ \pi_i(N_i) = 1$, άρα $N \subseteq \ker \phi$ και έτσι υπάρχει $\tilde{\phi} : (G_1 * G_2)/N \to H$ με $\tilde{\phi} \circ \pi = \phi$.

Θέλουμε να δείξουμε ότι το παρακάτω διάγραμμα είναι μεταθετικό



Πράγματι, έχουμε ότι

$$\begin{aligned}\tilde{\phi} \circ \lambda_i(g_1N_1) &= \tilde{\phi} \circ \lambda_i \circ \pi_1(g_1) \\ &\overset{(1)}{=} \tilde{\phi} \circ \pi(g_1) \\ &\overset{(3)}{=} \phi(g_1) \\ &\overset{(2)}{=} \phi_1 \circ \pi_1(g_1) \\ &= \phi(g_1N_1)\end{aligned}$$

δηλαδή $\tilde{\phi} \circ \lambda_1 = \phi_1$. Ομοίως, $\tilde{\phi} \circ \lambda_2 = \phi_2$.

Για την μοναδικότητα της $\tilde{\phi}$: Έστω $\psi : (G_1 * G_2)/N \to H$ με $\psi \circ \lambda_i = \phi_i$.

Θα δείξουμε ότι $\tilde{\phi} = \psi$. Αρκεί να δείξουμε ισότητα σε ένα σύνολο γεννητόρων.

Έστω $g_1 \in G_1$. Τότε

$$\begin{aligned}\tilde{\phi}(g_1N) = \tilde{\phi} \circ \pi(g_1) &\overset{(3)}{=} \phi(g_1) \\ &\overset{(2)}{=} \phi_1 \circ \pi_1(g_1) = \psi \circ \lambda_1 \circ \pi_1(g_1) \\ &\overset{(1)}{=} \psi \circ \pi(g_1) = \psi(g_1N)\end{aligned}$$

Ομοίως, $\tilde{\phi}(g_2N) = \psi(g_2N)$ για $g_2 \in G_2$.

Τελικά, $\tilde{\phi} = \psi$. □

Πόρισμα 9.2.1. *Αν $N_\alpha \lhd G_\alpha$ και N η κανονική κλειστότητα της $\bigcup_\alpha N_\alpha$ στο $\underset{\alpha}{*}G_\alpha$, τότε $\underset{\alpha}{*}G/N \simeq \underset{\alpha}{*}G_\alpha/N_\alpha$.*

Πόρισμα 9.2.2. *Αν $G = A * B$ και N η κανονική υποομάδα που παράγεται από την A, τότε $G/N \simeq B$.*

9.3 Ελεύθερες ομάδες

Ορισμός 9.3.1. Έστω X ένα μη κενό σύνολο. Για κάθε $\alpha \in X$ παίρνουμε την άπειρη κυκλική ομάδα $\langle \alpha \rangle$ που παράγεται από το α.

Η **ελεύθερη ομάδα** επί του X είναι το ελεύθερο γινόμενο των ομάδων $\langle\alpha\rangle$, $\alpha \in X$ και συμβολίζεται με $F(X)$.

Δηλαδή, η $F(X)$ είναι ένα ελεύθερο γινόμενο αντιτύπων της άπειρης κυκλικής $\mathbb{Z}$, ένα αντίτυπο για κάθε στοιχείο του X,

$$F(X) = \underset{\alpha\in X}{*}\langle\alpha\rangle = \underset{\alpha\in X}{*}\mathbb{Z}_\alpha,\ \mathbb{Z}_\alpha = \mathbb{Z}$$

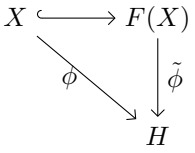
Ορίζουμε, επίσης, $F(\emptyset) = \{1\}$.

Το X λέγεται **βάση** της $F(X)$ και το $|X|$ **διάσταση** της $F(X)$.

Παρατηρήσεις 9.3.1. (i) Κάθε ελεύθερη ομάδα είναι ελευθέρα στέψης, αφού η $\mathbb{Z}$ είναι ελευθέρα στρέψης.

(ii) Αν $F(X) \neq \mathbb{Z}$, τότε $Z(F(X)) = 1$.

Θεώρημα 9.3.1 (Κανονική συνθήκη). *Έστω X σύνολο και $F(X)$ η ελεύθερη ομάδα επί του X. Τότε, για κάθε ομάδα H και κάθε απεικόνιση $\phi : X \to H$ υπάρχει μοναδικός ομομορφισμός $\tilde{\phi} : F(X) \to H$ που επεκτείνει την ϕ.*



Απόδειξη. Το ζητούμενο έπεται από την κανονική συνθήκη του ελεύθερου γινομένου, αφού η απεικόνιση $\phi : X \to H$ επάγει οικογένεια ομομορφισμών $\phi_\alpha : \langle\alpha\rangle \to X$, $\alpha \in X$. □

Πρόταση 9.3.1. *Η διάσταση μιας ελεύθερης ομάδας είναι καλά ορισμένη, δηλαδή $F(X_1) \simeq F(X_2)$ ανν $|X_1| = |X_2|$.*

Απόδειξη. Αν $|X_1| = |X_2|$, τότε υπάρχει 1-1 και επί απεικόνιση $\phi : X_1 \to X_2$. Από το προηγούμενο θεώρημα, η ϕ επάγει ομομορφισμό $\tilde{\phi} : F(X_1) \to F(X_2)$, ο οποίος είναι ισομορφισμός, με $\tilde{\phi}^{-1} = \tilde{\phi^{-1}}$.

Αντίστροφα, έστω ότι $F(X_1) \simeq F(X_2)$, δηλαδή $\underset{\alpha\in X_1}{*}\mathbb{Z} \simeq \underset{\alpha\in X_2}{*}\mathbb{Z}$. Τότε, $\underset{\alpha\in X_1}{*}\mathbb{Z}/(\underset{\alpha\in X_1}{*}\mathbb{Z})' \simeq \underset{\alpha\in X_2}{*}\mathbb{Z}/(\underset{\alpha\in X_2}{*}\mathbb{Z})'$ και άρα $\bigoplus_{\alpha\in X_1}\mathbb{Z} \simeq \bigoplus_{\alpha\in X_2}\mathbb{Z}$. Εφόσον οι προηγούμενες ομάδες είναι ελεύθερες αβελιανές, έπεται ότι $|X_1| = |X_2|$. □

Πρόταση 9.3.2. *Έστω X υποσύνολο μιας ομάδας G. Τα ακόλουθα είναι ισοδύναμα:*

(i) Η G είναι ελεύθερη με βάση το X.

(ii) Κάθε μη-τετριμμένο στοιχείο της G μπορεί να γραφεί κατά μοναδικό τρόπο ως

$$x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_k}^{\varepsilon_k}$$

όπου $k > 0$, $1 \neq x_{i_j} \in X$, $\varepsilon_j \in \mathbb{Z}_+$ και $x_{i_j} \neq 1$, $x_{i_j} \neq x_{i_{j+1}}$ για κάθε j.

(iii) Η G παράγεται από το X και το 1 δε μπορεί να γραφεί ως $x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \cdots x_{i_k}^{\varepsilon_k}$, όπου $k > 0$, $1 \neq x_{i_j} \in X$, $\varepsilon_j \in \mathbb{Z}_+$ και $x_{i_j} \neq 1$, $x_{i_j} \neq x_{i_{j+1}}$ για κάθε j.

Απόδειξη. Προκύπτει άμεσα από την αντίστοιχη πρόταση για ελεύθερα γινόμενα, αφού κάθε στοιχείο της $\langle x\rangle$, $x \in X$, είναι x^ε, $\varepsilon \in \mathbb{Z}$. □

Έστω G ομάδα και R υποσύνολο της G. Συμβολίζουμε με $\langle\langle R\rangle\rangle$ την κανονική υποομάδα της G που παράγεται από το R. Δηλαδή, το $\langle\langle R\rangle\rangle$ είναι η τομή όλων των κανονικών υποομάδων της G που περιέχουν το R, ή ισοδύναμα τα γινόμενα συζυγών στοιχείων του $R^{\pm 1}$.

Ορισμός 9.3.2. Έστω G ομάδα. Λέμε ότι η G έχει **παράσταση** $\langle X|R\rangle$ αν $G = F(X)/\langle\langle R\rangle\rangle$. Το X είναι το σύνολο γεννητόρων και το R το σύνολο των σχέσεων.

Δηλαδή, αν X ένα συνολο παίρνουμε το $F(X)$ και για $R \subseteq F(X)$, ορίζουμε

$$\langle X|R\rangle = F(X)/\langle\langle R\rangle\rangle$$

Η G λέγεται **πεπερασμένα παραγόμενη**, αν τα σύνολα X και R είναι πεπερασμένα.

Πρόταση 9.3.3. *Κάθε ομάδα G έχει μια παράσταση.*

Απόδειξη. Έστω X σύνολο γεννητόρων της G. Έστω $X_0 = \{(x,0) : x \in X\}$ και $F(X_0)$ η ελεύθερη ομάδα επί του X_0 -στην ουσία $X \equiv X_0$, αφού $(x,0) \mapsto x$.

Από την κανονική συνθήκη των ελεύθερων ομάδων η απεικόνιση $\phi : X_0 \to X \hookrightarrow G$ με $(x,0) \mapsto x$ επεκτείνεται σε ομομορφισμό $\tilde{\phi} : F(X_0) \to G$.

Επιπλέον, ο $\tilde{\phi}$ είναι επί, γιατί $\tilde{\phi}(X_0) = X$ το σύνολο γεννητόρων της G. Έτσι,

$$G \simeq F(X_0)/\ker\tilde{\phi}$$

Για $R = \ker\tilde{\phi}$, έχουμε ότι $G = \langle X|R\rangle$. □

Θεώρημα 9.3.2 (Van Dyck). *Έστω $G = \langle X|R\rangle$ και H μια άλλη ομάδα. Κάθε απεικόνιση $\phi : X \to H$ τέτοια ώστε $\phi(r) = 1$ για κάθε $r \in R$, μπορεί να επεκταθεί σε ομομορφισμό $\tilde{\phi} : G \to H$.*

Απόδειξη. Η κανονική συνθήκη των ελεύθερων ομάδων μας δίνει ομομορφισμό $\phi_1 : F(X) \to H$ που επεκτείνει την ϕ.

Εφόσον $\phi(r) = 1$ για κάθε $r \in R$, έχουμε ότι $\langle\langle R\rangle\rangle \subseteq \ker\phi$, και έτσι επάγεται ομομορφισμός $\tilde{\phi} : G = F(X)/\langle\langle R\rangle\rangle \to H$. □

Παραδείγματα 9.3.1. (i) Εύκολα βλέπουμε ότι $\mathbb{Z}_n = \langle x|x^n = 1\rangle = \mathbb{Z}/n\mathbb{Z}$.

(ii) Έχουμε ότι μια παράσταση της $\mathbb{Z}^n$ είναι η

$$\langle x_1, x_2, \ldots, x_n|[x_i, x_j] = 1,\ \forall i,j\rangle$$

Πράγματι, έστω $F = F(\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n})$ η ελεύθερη ομάδα επί του $\{\bar{x_1}, \bar{x_2}, \ldots, \bar{x_n}\}$ και

$$N = \langle\langle [x_i, x_j],\ i,j\rangle\rangle$$

Αρκεί να δείξουμε ότι $F/N \simeq \mathbb{Z}^n$.

Από το προηγούμενο θεώρημα, έχουμε επιμορφισμό $\phi : F/N \to \mathbb{Z}^n$, με $\phi(\bar{x_i}) = x_i$.

Εφόσον οι γεννήτορες $\bar{x_i}N$ της F/N μετατίθενται, γιατί $[\bar{x_i}, \bar{x_j}] \in N$, η ομάδα F/N είναι αβελιανή.

Έστω $g \in F/N$ με $\phi(g) = 1$. Τότε,

$$\begin{aligned} g &= \bar{x_1}^{\varepsilon_1} N \bar{x_2}^{\varepsilon_2} N \cdots \bar{x_n}^{\varepsilon_n} N \\ &= \bar{x_1}^{\varepsilon_1} \bar{x_2}^{\varepsilon_2} \cdots \bar{x_n}^{\varepsilon_n} N \end{aligned}$$

Αν $\phi(g) = 1$, τότε $\bar{x_1}^{\varepsilon_1}\bar{x_2}^{\varepsilon_2}\cdots\bar{x_n}^{\varepsilon_n} = 1 \in \mathbb{Z}^n$, άρα $\varepsilon_1 = \varepsilon_2 = \cdots = \varepsilon_n = 0$ και $g = 1$.

Δηλαδή $\ker\phi = 1$ και η ϕ είναι ισομορφισμός.

(iii) Ισχύει ότι

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle \alpha, \beta | a^2 = b^2 = 1,\ [\alpha, \beta] = 1 \rangle$$

Πράγματι, έστω $F = F(\bar{\alpha}, \bar{\beta})$ και $N = \langle\langle \alpha^2, \beta^2, [\alpha, \beta] \rangle\rangle \lhd F$.

Θα δείξουμε ότι $G = F/N \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Από το Θεώρημα Van Dyck έχουμε επιμορφισμό $\phi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$.

Η G είναι αβελιανή, γιατί οι γεννήτορες $\bar{\alpha}N$ και $\bar{\beta}N$ μετατιθένται και κάθε γεννήτορας είναι τάξεως 2, αφού $\bar{\alpha}^2, \bar{\beta}^2 \in N$.

Έπεται ότι η G έχει το πολύ 4 στοιχεία. Όμως, η $\phi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ είναι επί, άρα $|G| = 4$ και $\ker \phi = 1$.

(iv) Αν $G_1 = \langle X_1 | R_1 \rangle$ και $G_2 = \langle X_2 | R_2 \rangle$, τότε $G_1 * G_2 = \langle X_1 \sqcup X_2 | R_1 \sqcup R_2 \rangle$.

(v) Ισχύει ότι

$$D_n = \langle \alpha, \beta | \alpha^2 = 1, \beta^n = 1, \alpha^{-1}\beta\alpha = \beta^{-1} \rangle$$

(vi) Η άπειρη διεδρική $D_\infty = \mathrm{Isom}()$. Χάθηκε στη διαδρομή.

Λήμμα 9.3.1 (Ping-Pong). *Έστω G μια ομάδα, η οποία δρα σε ένα σύνολο M. Έστω H_1 και H_2 δύο υποομάδες της G με $|H_1| \geq 3$ και $|H_2| \geq 2$ και έστω H η υποομάδα της G που παράγεται από τις H_1 και H_2.*

Υποθέτουμε ότι υπάρχουν δύο μη-κενά υποσύνολα S_1 και S_2 του M έτσι ώστε :

(i) $S_2 \not\subseteq S_1$,

(ii) $\alpha S_2 \subseteq S_1$ *για κάθε* $\alpha \in H_1$, *και*

(iii) $\beta S_1 \subseteq S_2$ *για κάθε* $\beta \in H_2$.

Τότε, η H είναι το ελεύθερο γινόμενο των H_1 και H_2, δηλαδή

$$\langle H_1, H_2 \rangle = H_1 * H_2$$

Απόδειξη. Αρκεί να δείξουμε ότι κάθε ανηγμένη λέξη στις H_1 και H_2 είναι διαφορετική από 1.

Διακρίνουμε περιπτώσεις:

- Αν

$$\omega = \alpha_1\beta_1\alpha_2\beta_2 \cdots \alpha_n\beta_n\alpha_{n+1}$$

όπου $\alpha_i \in H_1 \backslash \{1\}$ και $\beta_i \in H_2 \backslash \{1\}$, τότε

$$\begin{aligned} \omega S_2 &= \alpha_1\beta_1\alpha_2\beta_2 \cdots \alpha_n\beta_n \underbrace{\alpha_{n+1}S_2}_{\in S_1} \\ &\subseteq \alpha_1\beta_1\alpha_2\beta_2 \cdots \alpha_n\beta_n S_1 \\ &\subseteq S_1 \end{aligned}$$

Εφόσον $S_2 \not\subseteq S_1$, το ω δρα μη-τετριμμένα και έτσι $\omega \neq 1$.

- Αν
$$\omega = \beta_1\alpha_1\beta_2\alpha_2\cdots\beta_n\alpha_n\beta_{n+1}$$
όπου $\alpha_i \in H_1\backslash\{1\}$ και $\beta_i \in H_2\backslash\{1\}$.
Έστω $\alpha \in H_1\backslash\{1\}$. Από την προηγούμενη περίπτωση έχουμε ότι
$$\begin{aligned}\alpha^{-1}\omega\alpha &= \alpha^{-1}\beta_1\alpha_1\beta_2\alpha_2\cdots\beta_n\alpha_n\beta_{n+1}\alpha \\ &\neq 1\end{aligned}$$
και συνεπώς $\omega \neq 1$.

- Αν
$$\omega = \alpha_1\beta_1\alpha_2\beta_2\cdots\alpha_n\beta_n$$
όπου $\alpha_i \in H_1\backslash\{1\}$ και $\beta_i \in H_2\backslash\{1\}$, τότε παινοντας $\alpha \in H_1\backslash\{1,,\alpha_1\}$ έχουμε
$$\alpha^{-1}\omega\alpha = \alpha^{-1}\alpha_1\beta_1\alpha_2\beta_2\cdots\alpha_n\beta_n\alpha$$
και από την πρώτη περίπτωση $\alpha^{-1}\omega\alpha \neq 1$, οπότε $\omega \neq 1$.
Ομοίως, $\omega \neq 1$, αν $\omega = \beta_1\alpha_1\beta_2\alpha_2\cdots\beta_n\alpha_n$.

□

Παράδειγμα 9.3.1. Οι πίνακες $A = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ και $B = \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ παράγουν μια ελεύθερη ομάδα διάστασης 2 στην $SL_2(\mathbb{Z})$.

Πράγματι, έστω
$$H_1 = \langle A\rangle = \left\{\begin{pmatrix}1 & 2k\\ 0 & 1\end{pmatrix}\right\}$$
και
$$H_2 = \langle B\rangle = \left\{\begin{pmatrix}1 & 0\\ 2k & 1\end{pmatrix}\right\}$$
Έστω, επιπλέον
$$S_1 = \left\{\begin{pmatrix}x\\ y\end{pmatrix} \in \mathbb{R}^2 : |x| > |y|\right\}$$
και
$$S_2 = \left\{\begin{pmatrix}x\\ y\end{pmatrix} \in \mathbb{R}^2 : |x| < |y|\right\}$$
Τότε, $S_2 \nsubseteq S_1$, αφού είναι ξένα μεταξύ τους. Επίσης, $H_1S_2 \subseteq S_1$ και $H_2S_1 \subseteq S_2$.

Έστω $\begin{pmatrix}x\\ y\end{pmatrix} \in S_2$, δηλαδή $|x| > |y|$. Τότε,
$$\begin{pmatrix}1 & 2k\\ 0 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}x+2ky\\ y\end{pmatrix} \in S_1$$
Πράγματι,
$$\begin{aligned}|2ky + x| &\geq |2ky| - |x| \\ &> 2|y| - |y| \\ &= |y|\end{aligned}$$
Ομοίως, αποδεικνύεται ότι $H_2S_1 \subseteq S_2$.

Έτσι,
$$\langle\langle A\rangle, \langle B\rangle\rangle = \langle A, B\rangle = \langle A\rangle * \langle B\rangle \simeq \mathbb{Z}\times\mathbb{Z}$$

9.4 Γράφημα Cayley

Ορισμός 9.4.1. Έστω G μια πεπερασμένα παραγόμενη ομάδα και $S = \{s_1, s_2, \ldots, s_n\}$ ένα πεπερασμένο σύνολο γεννητόρων της G.
Το **γράφημα Cayley**, $\Gamma(G, S)$, της G ως προς το σύνολο γεννητόρων S ορίζεται ως εξής:

Το σύνολο κορυφών είναι τα στοιχεία της ομάδας G. Για κάθε $g \in G$ και κάθε $s \in S$ υπάρχει μια γεωμετρική (ή θετική) ακμή από το g στο gs, και η αντίστροφη της.

Δύο κορυφές g και h συνδέονται με μια ακμή ανν $g^{-1}h \in S^{\pm 1}$.
Ισχύουν τα εξής:

- Εφόσον το S παράγει την G, το $\Gamma(G, S)$ είναι συνεκτικό.
- Το $\Gamma(G, S)$ περιέχει κυκλώματα της μορφής  ή ανν $S \cap S^{-1} \neq \emptyset$.
- Από κάθε κορυφή "φυτρώνουν" $2n$ ακμές, εκ των οποίων οι n φεύγουν και οι άλλες n έρχονται.
- Το $\Gamma(G, S)$ γίνεται μετρικός χώρος ως εξής:

  Κάθε ακμή έχει μήκος 1.

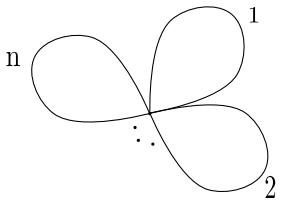
  Η απόσταση δύο κορυφών είναι το ελάχιστο μήκος των μονοπατιών που τις συνδέουν,

$$d_s(g, h) = \|g^{-1}h\| = \min\{n : g^{-1}h = s_{i_1}^{\varepsilon_1} s_{i_2}^{\varepsilon_2} \cdots s_{i_n}^{\varepsilon_n},\ s_{i_j} \in S, \varepsilon_j \in \{\pm 1\}\}$$

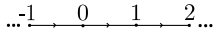
- Η φυσική δράση της G στο $\Gamma(G, S)$, με $g : x \mapsto gh$, είναι δράση με ισομετρίες.

  Επιπλέον, η δράση είναι ελεύθερη και μεταβατική στις κορυφές.

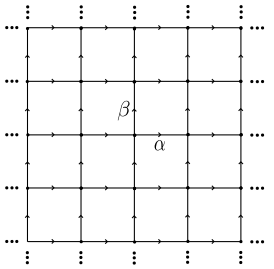
- Το γράφημα πηλίκο $\Gamma(G, S)/G$ αποτελείται από μία κορυφή και n ακμές, μια για κάθε γεννήτορα. Δηλαδή, το γράφημα πηλίκο είναι



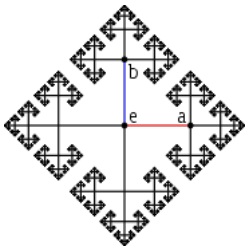
Παραδείγματα 9.4.1. (i) Έστω $G = (\mathbb{Z}, +)$ και $S = \{1\}$. Τότε, το γράφημα Cayley της G είναι το



(ii) Έστω $G = \mathbb{Z} \oplus \mathbb{Z}$ και $S = \{(1, 0), (0, 1)\}$. Τότε, το γράφημα Cayley της G είναι το

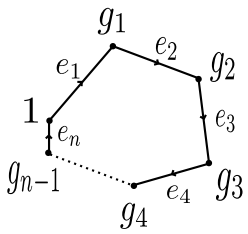


(iii) Έστω $G = F(a, b)$, ελεύθερη ομάδα επί του $\{a, b\}$. Τότε, το γράφημα Cayley της G είναι το



Πρόταση 9.4.1. *Έστω G ομάδα. Τότε, το $\Gamma(G, S)$ είναι δέντρο ανν η G είναι ελεύθερη με βάση το S.*

Απόδειξη. Έστω $p = e_1 e_2 \cdots e_n$ ένα κλειστό μονοπάτι (χωρίς παλινδρομίσεις) στο $\Gamma(G, S)$ ελάχιστου μήκους, δηλαδή p κύκλωμα.



Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι η αρχή και το τέλος του p είναι το 1.

Εφόσον οι κορυφές 1 και g_1 συνδέονται στο $\Gamma(G, S)$ με μια ακμή, έχουμε ότι $g = s_1^{\varepsilon_1} \in S^{\pm 1}$. Για τον ίδιο λόγο $g_1^{-1} g_2 = s_2^{\varepsilon_2} \in S^{\pm 1}$, και έτσι $g_2 = s_q^{\varepsilon_1} s_2^{\varepsilon_2}$.

Γενικότερα, $g_i^{-1} g_{i+1} = s_{i+1}^{\varepsilon_{i+1}}$, οπότε

$$g_{+1} = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_{i+1}^{\varepsilon_{i+1}},\ s_j^{\varepsilon_j} \in S^{\pm 1}$$

Θα έχουμε, λοιπόν,

$$1 = g_n = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n},\ s_j \in S, \varepsilon_j \in \{\pm 1\} \qquad (\Lambda)$$

και αντίστροφα κάθε (ανηγμένη) λέξη ίση με 1 δίνει κλειστό μονοπάτι στο $\Gamma(G, S)$.

Εφόσον το p έχει επιλεγεί με ελάχιστο μήκος, η λέξη (Λ) είναι ανηγμένη.

Έτσι, το $\Gamma(G, S)$ είναι δέντρο ανν το $\Gamma(G, S)$ δεν έχει κυκλώματα ανν κάθε ανηγμένη λέξη στο S είναι διάφορη του 1 ανν η G είναι ελεύθερη με βάση το S. □

Πόρισμα 9.4.1. *Μια ελεύθερη ομάδα δρα ελεύθερα επί ενός δέντρου.*

Απόδειξη. Αν $G = F(S)$, τότε η G δρα ελεύθερα στο δέντρο $\Gamma(G, S)$. □

Μάλιστα, ισχύει και το αντίστροφο:

Θεώρημα 9.4.1. *Μια ομάδα είναι ελεύθερη ανν δρα ελεύθερα ("χωρίς αντιστροφές") επί ενός δέντρου.*

Θεώρημα 9.4.2 (Nielsen-Schreier). *(i) Κάθε υποομάδα ελεύθερης ομάδας είναι ελεύθερη.*

(ii) Αν η G είναι ελεύθερη ομάδα διάστασης k και H υποομάδα της G πεπερασμένου δείκτη n, τότε η H είναι ελεύθερη διάστασης $n(k-1)+1$.

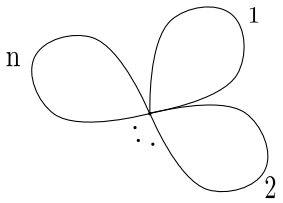
Σχέδιο απόδειξης. (i) Έστω F ελεύθερη και $H \subseteq F$.

Έστω X γράφημα με $\pi(X, \cdot) = F$.

Θεωρούμε τον χώρο επικάλυψης X_H που αντιστοιχεί στην υποομάδα H, $\rho : X_H \to X$ την προβολή επικάλυψης και $\rho_*(\pi_1(X_H, \sim^*)) = H$. Άρα, εφόσον η ρ_* είναι 1-1, $H = \pi_1(X_H, \sim^*)$.

Όμως, το X_H είναι γράφημα, άρα η $\pi_1(X_H, \sim^*)$ είναι ελεύθερη, και έτσι η H είναι ελεύθερη.

(ii) Έστω X το



Τότε, $\pi_1(X, \sim) \simeq G = F_k$. Θεωρούμε τον χώρο επικάλυψης X_H που αντιστοιχεί στην υποομάδα H και $\rho_H : X_H \to X$ την αντίστοιχη προβολή.

Εφόσον $[G : H] = n$, κάθε νήμα της ρ (δηλαδή $\rho^{-1}(x)$) έχει n στοιχεία.

Συνεπώς, το X_H είναι γράφημα με n κορυφές και nk ακμές. Άρα,

$$\begin{aligned}
\text{rank}(H) &= \text{rank}(\pi_1(X_H, \cdot)) \\
&= \#\text{ακμών που δεν ανήκουν σε μέγιστο δέντρου} \\
&= nk - (\#\text{ακμών ενός μέγιστου δέντρου}) \\
&= nk - (n-1) \\
&= n(k-1) + 1
\end{aligned}$$

□

9.5 Ελεύθερα γινόμενα με αμάλγαμα

Έστω X τοπολογικός χώρος και $X_1, X_2 \subseteq X$ ανοικτά, κατά τόξα συνεκτικά, τοπικά κατά τόξα συνεκτικά υποσύνολα του X με $X_1 \cap X_2$ κατά τόξα συνεκτικό σύνολο.

Υποθέτουμε ότι $X = X_1 \cap X_2$ και ότι οι ενθέσεις $X_1 \hookrightarrow X$, $X_2 \hookrightarrow X$ επάγουν μονομορφισμούς

$$\phi_i : \pi_1(X_i, x_0) \to \pi_1(X, x_0)$$

όπου $x_0 \in X_1 \cap X_2$.

Τότε, από το Θεώρημα Seifert-Van Kampen, έχουμε

$$\pi_1(X, x_0) = (\pi_1(X_1, x_0) * \pi_1(X_2, x_0))/N$$

όπου $N = \langle\langle \phi_1^{-1}(\gamma) \cdot \phi_2(\gamma) \rangle\rangle$, και $\gamma \in \pi_1(X_1 \cap X_2, x_0)$.

Συμβολίζουμε

$$\pi_1(X, x_0) = (\pi_1(X_1, x_0) * \pi_1(X_2, x_0))/\pi_1(X_1 \cap X_2, x_0)$$

Αν η τομή $X_1 \cap X_2$ είναι απλά συνεκτικός χώρος, τότε η $\pi_1(X, x_0)$ είναι το ελεύθερο γινόμενο των $\pi_1(X_1, x_0)$ και $\pi_1(X_2, x_0)$, δηλαδή

$$\pi_1(X, x_0) = \pi_1(X_1, x_0) * \pi_1(X_2, x_0)$$

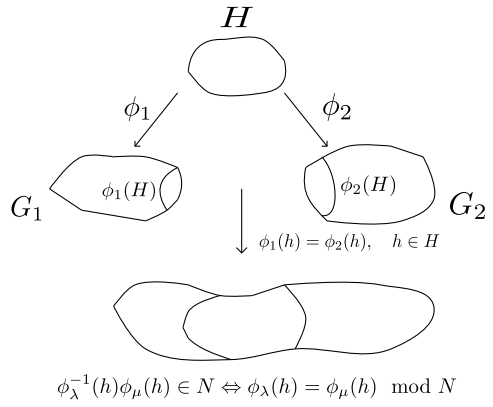
Ορισμός 9.5.1. Έστω G_λ, $\lambda \in \Lambda$, οικογένεια ομάδων, H ομάδα και $\phi_\lambda : H \to G_\lambda$ οικογένεια μονομορφισμών. Το **ελεύθερο γινόμενο** των ομάδων με **αμαλγαματοποιημένη** υποομάδα H, που συμβολίζεται με $\underset{\lambda}{*} G_\lambda$, είναι η ομάδα πηλίκο $*G_\lambda / N$ που προκύπτει από το ελεύθερο γινόμενο $\underset{\lambda}{*} G_\lambda$, όπου N είναι η κανονική υποομάδα που παράγεται από τα στοιχεία $\phi_\lambda^{-1}(h)\phi_\mu(h)$, $h \in H$, $\lambda, \mu \in \Lambda$, δηλαδή

$$\underset{H}{*} G_\lambda = \underset{\lambda \in \Lambda}{*} G_\lambda / \langle\langle \phi_\lambda^{-1}(h)\phi_\mu(h) \ : \ \lambda, \mu \in \Lambda, \ h \in H \rangle\rangle$$

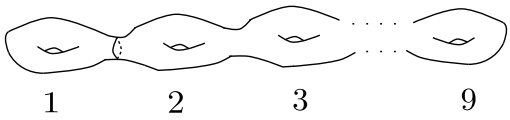
Στην περίπτωση που $\Lambda = \{1, 2\}$, συμβολίζουμε πιο απλά με $G_1 \underset{H}{*} G_2$.

Παρατήρηση 9.5.1. Η ομάδα $\underset{H}{*} G_\lambda$ εξαρτάται από τις εμφυτεύσεις ϕ_λ, $\lambda \in \Lambda$.

Παραδείγματα 9.5.1. (i) Κάθε ελεύθερο γινόμενο είναι ελεύθερο γινόμενο με αμάλγαμα $\{1\}$.



(ii) Έστω S_9 προσανατολισμένη επιφάνεια γένους 9, δηλαδή



Τότε, $\pi_1(S_9) = F_2 \underset{\mathbb{Z}}{*} F_{2(9-1)}$.

(iii) Η ομάδα $SL(2, \mathbb{Z})$ μπορεί να υλοποιηθεί ως $SL(2, \mathbb{Z}) = \mathbb{Z}_6 \underset{\mathbb{Z}_2}{*} \mathbb{Z}_4$, όπου

$$\mathbb{Z}_6 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \right\rangle, \mathbb{Z}_4 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle, \mathbb{Z}_2 = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$$

Αν $\phi_i : H \to G_i$, $i = 1, 2$ μονομορφισμοί, τότε

$$G = G_1 \underset{H}{*} G_2 = G_1 \underset{\phi(H_1) = \phi(H_2)}{*} G_2$$

Επίσης, μπορούμε να υποθέσουμε ότι $H \leq G_1$ και $\phi : H \to G_2$ μονομορφισμός.

$$G_1 \geq \phi_1(H) \xrightarrow{\phi_1^{-1}} H \xrightarrow{\phi_2} G_2$$
$$\phi_2 \circ \phi_1^{-1}$$

Στην συνέχεια, παίρνουμε την περίπτωση δύο παραγόντων G_1 και G_2 με $H \leq G_1$, $\phi : H \to G_2$ μονομορφισμός, και $G = G_1 \underset{H}{*} G_2$ το αντίστοιχο ελεύθερο γινόμενο με αμάλγαμα.

Έστω $\pi : G_1 * G_2 \to G_1 \underset{H}{*} G_2$ η φυσική προβολή, με $\ker \pi = \langle\langle \phi(h) : h \in H \rangle\rangle$.

Παίρνουμε T_1 και T_2 σύνολα αντιπροσώπων δεξιών συμπλόκων της H στην G_1 και της $\phi(H)$ στην G_2 αντίστοιχα, έτσι ώστε $1 \in T_1$ και $1 \in T_2$.

Αν $g \in G_1 \underset{H}{*} G_2$ με $g \neq 1$, τότε

$$g = \pi(x) = \pi(x_1 x_2 \cdots x_n) = \pi(x_1)\pi(x_2) \cdots \pi(x_n)$$

όπου $x_1 x_2 \cdots x_n$ η ανηγμένη μορφή του x στο $G_1 * G_2$.

Από όλες τις εκφράσεις του g ως

$$g = \pi(g_1)\pi(g_2) \cdots \pi(g_k)$$

με $g_i \in G_1 \cup G_2$, παίρνουμε μια ελάχιστου μήκους. Έστω ότι αυτή είναι

$$g = \pi(g_1)\pi(g_2) \cdots \pi(g_n)$$

όπου $g_i \in G_1 \cup G_2$.

Από την επιλογή της παραπάνω έκφρασης, διαδοχικά g_i ανήκουν σε διαδοχικούς παράγοντες και $g_i \notin \pi(H) = \pi(\phi(H))$ για κάνενα i, εκτός αν $n = 1$ και $g \in \pi(H)$.

Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $g_1 \in G_1$ και $g_n \in G_2$. Έχουμε

$$g = \pi(g_1)\pi(g_2) \cdots \pi(g_n)$$

με $g_n = \phi(h_n) \cdot \bar{g}_n$, όπου $h_n \in H$ και $\bar{g}_n \in T_2$.

Τότε,

$$\begin{aligned}
g &= \pi(g_1)\pi(g_2) \cdots \pi(g_n) \\
&= \pi(g_1)\pi(g_2) \cdots \pi(\phi(h_n) \cdot \bar{g}_n) \\
&= \pi(g_1)\pi(g_2) \cdots \pi(\phi(h_n)) \cdot \pi(\bar{g}_n) \\
&= \pi(g_1)\pi(g_2) \cdots \pi(h_n) \cdot \pi(\bar{g}_n) \\
&= \pi(g_1)\pi(g_2) \cdots \pi(g_{n-1}h_n) \cdot \pi(\bar{g}_n) \\
&= \pi(g_1)\pi(g_2) \cdots \pi(h_{n-1}\bar{g}_{n-1}) \cdot \pi(\bar{g}_n), \quad h_{n-1} \in H,\ \bar{g}_{n-1} \in T_1 \\
&\vdots \\
&= \pi(g_0)\pi(\bar{g}_1) \cdots \pi(\bar{g}_n)
\end{aligned}$$

όπου $g_0 \in H$, $\bar{g}_1, \bar{g}_3, \cdots \in T_1 \backslash \{1\}$ και $\bar{g}_2, \bar{g}_4, \cdots \in T_2 \backslash \{1\}$, εκτός εαν $g = \pi(g_0) \in \pi(H)$.

Ορισμός 9.5.2. Μια **H-κανονική μορφή** είναι μια ακολουθία $(x_0, x_1, \ldots, x_n)$ έτσι ώστε:

(i) $x_0 \in H$,

(ii) $x_i \in T_1 \backslash \{1\}$ ή $T_2 \backslash \{1\}$ για $i \geq 0$, και

(iii) διαδοχικοί όροι x_i, x_{i+1} ανήκουν σε διαφορετικά σύνολα αντιπροσώπων.

Ομοίως, ορίζονται και οι $\phi(H)$-κανονικές μορφές.

Θεώρημα 9.5.1. *Κάθε στοιχείο g της $G_1 \underset{H}{*} G_2$ γράφεται κατά μοναδικό τρόπο ως*

$$g = \pi(x_0)\pi(x_1)\cdots\pi(x_n)$$

όπου $(x_0, x_1, \ldots, x_n)$ είναι μια H-κανονική μορφή.

Απόδειξη. Η ύπαρξη της γραφής εξασφαλίζεται από τα σχόλια που προηγήθηκαν.

Για την μοναδικότητα: Κάθε $g_1 \in G_1$ γράφεται κατά μοναδικό τρόπο ως $g_1 = \underline{g}_1\overline{g}_1$, όπου $\underline{g}_1 \in H$ και $\overline{g}_1 \in T_1$. Ομοίως, κάθε $g_2 \in G_2$ γράφεται κατά μοναδικό τρόπο ως $g_2 = \underline{g}_2\overline{g}_2$, όπου $\underline{g}_2 \in \phi(H)$ και $\overline{g}_2 \in T_2$. □

Έστω W_H το σύνολο των H-κανονικών μορφών και $W_{\phi(H)}$ το σύνολο των $\phi(H)$-κανονικών μορφών.

Η απεικόνιση

$$\phi_* : W_h \to W_{\phi(H)}, \quad (x_0, x_1, \ldots, x_n) \mapsto (\phi(x_0), x_1, \ldots, x_n)$$

είναι 1-1 και επί.

Ορίζουμε δράση της G_1 στο W_H ως εξής: για $g \in G_1$ και $w = (x_0, x_1, \ldots, x_n)$, όπου $n \geq 1$, έχουμε

$$g \cdot w = \begin{cases} (gx_0, x_1, \ldots, x_n) & , g \in H \\ (\underline{gx_0}, \overline{gx_0}, x_1, \ldots, x_n) & , g \notin H,\ x_1 \in G_2 \\ (\underline{gx_0x_1}, \overline{gx_0x_1}, x_2, \ldots, x_n) & , g \notin H,\ x_1 \in G_1,\ gx_0x_1 \notin H \\ (gx_0x_1, x_2, \ldots, x_n) & , g \notin H,\ x_1 \in G_1,\ gx_0x_1 \in H \end{cases}$$

και

$$g \cdot x_0 = \begin{cases} (gx_0) & , g \in H \\ (\underline{gx_0}, \overline{gx_0}) & , g \notin H \end{cases}$$

Ομοίως, ορίζεται δράση της G_2 στο $W_{\phi(H)}$, η οποία μέσω της ϕ_* επάγει δράση της G_2 στο W_H : αν $g \in G_2$ και $w \in W_H$, τότε $g \cdot w = \phi_*^{-1}(g \cdot \phi_*(w))$.

Από την κανονική συνθήκη του $G_1 * G_2$, οι παραπάνω δράσεις επεκτείνονται σε δράση της $G_1 * G_2$ στο W_H.

Παρατηρούμε ότι $h \cdot w = \phi(h) \cdot w$ για κάθε $h \in H$ και $w \in W_H$. Δηλαδή, κάθε στοιχείο $h^{-1}\phi(h)$ ανήκει στον πυρήνα της δράσης. Αυτό σημαίνει ότι επάγεται δράση της $G = G_1 \underset{H}{*} G_2$ στο W_H με $\pi(x) \cdot w = x \cdot w$,

$$G_1 \underset{H}{*} G_2 = G_1 * G_2/N, \quad N = \ker \pi = \langle\langle h^{-1}\phi(h) \rangle\rangle$$

Έστω $g \in G_1 \underset{H}{*} G_2$ και $g = \pi(x_0)\pi(x_1)\cdots\pi(x_n)$, όπου $(x_0, x_1, \ldots, x_n)$ μια H-κανονική μορφή. Τότε,

$$\begin{aligned} g \cdot (1) &= \pi(x_0, x_1, \ldots, x_n) \cdot (1) \\ &= x_0x_1\cdots x_n(1) \\ &= x_0x_1\cdots x_{n-1}(1, x_n) \\ &= x_0x_1\cdots x_{n-2}(1, x_{n-1}, x_n) \\ &\vdots \\ &= x_0(1, x_1, \ldots, x_n) \\ &= (x_0, x_1), \ldots, x_n) \end{aligned}$$

Δηλαδή, η κανονική μορφή $(x_0, x_1, \ldots, x_n)$ είναι πλήρως καθορισμένη από το g και έχουμε την μοναδικότητα.

Παρατήρηση 9.5.2. Η παραπάνω δράση εμφυτεύει την $G_1 \underset{H}{*} G_2$ στην S_{W_H}.

Πράγματι, αν $g \neq 1$ και $g = \pi(x_0)\pi(x_1)\cdots\pi(x_n)$, όπου $(x_0, x_1, \ldots, x_n) \in W_H$, τότε $x_i \neq 1$ για κάποιο i, και έτσι $g \cdot (1) \neq 1$. Δηλαδή, το g δεν ανήκει στον πυρήνα της δράσης.

Πόρισμα 9.5.1. *Ο κανονικός επιμορφισμός $\pi : G_1 * G_2 \to G_1 \underset{H}{*} G_2$ επάγει εμφυτεύσεις των ομάδων G_1 και G_2 στην G.*

Επιπλέον, η G παράγεται από τις $\pi(G_1)$ και $\pi(G_2)$ και $\pi(G_1) \cap \pi(G_2) = \pi(H)$.

Απόδειξη. Έστω $g \in G_1 \cap N$, όπου $N = \ker \pi$. Τότε, $g_1 = \underline{g}_1\overline{g}_1$, όπου $\underline{g}_1 \in H$ και $\overline{g}_1 \in T_1$, και $\pi(g_1) = \pi(\underline{g}_1\overline{g}_1) = \pi(1) = 1$. Από την μοναδικότητα της κανονικής μορφής $\underline{g}_1 = \overline{g}_1 = 1$ και έτσι $g_1 = 1$.

Ομοίως, $G_2 \cap N = 1$.

Οι $\pi(G_1)$, $\pi(G_2)$ παράγουν την G, γιατί οι G_1, G_2 παράγουν την $G_1 * G_2$.

Έστω $g \in \pi(G_1) \cap \pi(G_2)$. Τότε, $g = \pi(g_1) = \pi(g_2)$, με $g_1 \in G_1$ και $g_2 \in G_2$.

Αν $g \notin \pi(H)$, τότε $g_1 = h_1\overline{g}_1$, όπου $h_1 \in H$, $\overline{g}_1 \in T_1\backslash\{1\}$ και $g_2 = \phi(h_2)\overline{g}_2$, όπου $h_2 \in H$, $\overline{g}_2 \in T_2\backslash\{1\}$.

Έτσι, $\pi(g_1) = \pi(g_2)$, δηλαδή $\pi(h_1\overline{g}_1) = \pi(\phi(h_2)\overline{g}_2)$, και άρα $\overline{g}_1 = \overline{g}_2$ -άτοπο. □

Παρατήρηση 9.5.3. Μπορούμε, λοιπόν, να ταυτίσουμε τις ομάδες G_i με τις $\pi(G_i)$ και την H με την $\pi(H)$.

Έτσι, οι G_1, G_2 παράγουν την $G_1 \underset{H}{*} G_2$, $G_1 \cap G_2 = H$ και κάθε $g \in G_1 \underset{H}{*} G_2$ μπορεί να ταυτιστεί με την κανονική του μορφή, $g = x_0x_1\cdots x_n$.

9.6 HNN επεκτάσεις

Έστω H, G ομάδες και ϕ_1, $\phi_2 : H \to G$ ομομορφισμοί. Αν $A = \phi_1(H)$ και $B = \phi_2(H)$, τότε A, $B \leq G$ και ο $\phi : A \to B$, με $\phi = \phi_2 \circ \phi_1^{-1}$, είναι ισομορφισμός.

Έστω, λοιπόν, G ομάδα, A, B υποομάδες της G και $\phi : A \to B$ ισομορφισμός. Γενικά ο ϕ δεν επάγεται από αυτομορφισμό της G. Είναι, όμως, δυνατό να εμφυτεύσουμε την G σε μια άλλη ομάδα $\tilde{G}$ έτσι ώστε ο ισομορφισμός ϕ να επάγεται από εσωτερικό αυτομορφισμό της $\tilde{G}$. Δηλαδή, οι A και B να είναι συζυγείς στην $\tilde{G}$.

Παραδείγματα 9.6.1. (i) Αν G μηδενοδύναμη, μη-αβελιανή, ελευθέρα στρέψης, τότε $Z(G) \neq 1$ και $Z(G) < G$. Αν $A = \langle g \rangle$, όπου $g \in Z(G)$, και $B = \langle x \rangle$, όπου $x \notin Z(G)$, τότε $A \simeq B \simeq \mathbb{Z}$, αλλά δεν υπάρχει $\phi \in \mathrm{Aut}(G)$ με $\phi(A) = B$.

(ii) Αν $G = \mathbb{Z}$, δύο οποιεσδήποτε υποομάδες της είναι άπειρες κυκλικές, αλλά δεν προκύπτουν απαραίτητα από αυτομορφισμό της G, αφού οι πιθανοί αυτομορφισμοί είναι δύο, ο ταυτοτικός και αυτός που στέλνει ένα στοιχείο στο αντίστροφό του.

Ορισμός 9.6.1. Έστω G ομάδα, A, B υποομάδες της G, και $\phi : A \to B$ ισομορφισμός. Έστω $\langle t \rangle$ η άπειρη κυκλική που παράγεται από ένα νέο στοιχείο t. Η **HNN επέκταση** της G ως προς A, B και ϕ ειναι η ομάδα πηλίκο $G*_A$, ή $G*_A^{\phi}$, του ελεύθερου γινομένου $G * \langle t \rangle$ προς την κανονική υποομάδα που παράγεται από τα στοιχεία $\{t^{-1}\alpha t : \alpha \in A\}$.

Συμβολίζουμε, επίσης,

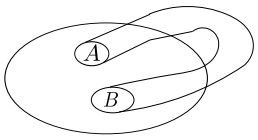
$$G*_A = \langle G, t \mid t^{-1}\alpha t = \phi(\alpha),\ \alpha \in A \rangle$$

Η ομάδα G λέγεται **βάση** της επέκτασης, το t **σταθερό γράμμα** και οι A, B **προσεταιριζόμενες** υποομάδες.

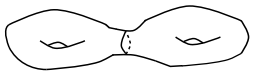
Παραδείγματα 9.6.2. (i) Έχουμε $\mathbb{Z} = 1*_1$, γιατί $1*_1 = 1 * \langle t\rangle/\langle\langle 1\rangle\rangle = \langle t\rangle \simeq \mathbb{Z}$.

(ii) Ισχύει $F_2 = \mathbb{Z}*_1$, γιατί $\mathbb{Z}*_1 = \mathbb{Z} * \langle t\rangle/\langle\langle 1\rangle\rangle \simeq \mathbb{Z} * \mathbb{Z} = F_2$.

(iii) Αν X το

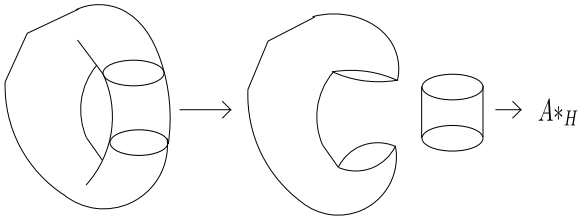


και Y το

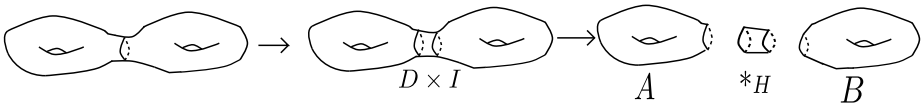


μπορεί να δειχθεί ότι $\pi_1(Y) = \pi_1(X)*_{\pi_1(A)}$.

Αν "κόψουμε" σε μια συνεκτική συνιστώσα, έχουμε HNN επέκταση



ενώ αν "κόψουμε" σε δύο έχουμε αμάλγαμα.



Έστω G ομάδα, A, $B \leq G$, $\phi : A \to B$ ισομορφισμός, και $G*_A$ η αντίστοιχη HNN επέκταση.

Παίρνουμε τον φυσικό επιμορφισμό $\pi : G * \langle t\rangle \to G*_A$. Τότε, κάθε $g \in G*_A$ γράφεται ως

$$g = \pi(g_0 t^{\varepsilon_1} \cdots t^{\varepsilon_n} g_n)$$

όπου $g_i \in G$ και $\varepsilon_i \in \{\pm 1\}$.

Μια τέτοια ακολουθία $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$ λέγεται **ανηγμένη** αν δεν περιέχει "υπολέξεις" της μορφής $t^{-1}\alpha t$ ή $t^{-1}\beta t$, όπου $\alpha \in A$, $\beta \in B$.

Προφανώς, κάθε στοιχείο της $G*_A$ μπορεί να αντικατασταθεί από μια ανηγμένη λέξη. Αρκεί να επιλέξουμε μια λέξη ελαχίστου μήκους που το αναπαριστά.

Έστω T_A σύνολο αντιπροσώπων δεξιών συμπλόκων της A στην G και T_B σύνολο αντιπροσώπων δεξιών συμπλόκων της B στην G, έτσι ώστε $1 \in T_A$, $1 \in T_B$.

Διακρίνουμε δύο περιπτώσεις:

$\varepsilon_n = 1$: Τότε, $g_n = \beta_n \cdot \hat{g}_n$, όπου $\beta_n \in B$, $\hat{g}_n \in T_B$, και

$$\pi(t^{\varepsilon_n} g_n) = \pi(t \cdot \beta_n \cdot \hat{g}_n) = \pi(\phi^{-1}(\beta_n) \cdot t \cdot \hat{g}_n)$$

$\varepsilon_n = -1$: Τότε, $g_n = \alpha_n \bar{g}_n$, όπου $\alpha_n \in A$, $\bar{g}_n \in T_A$, και

$$\pi(t^{\varepsilon_n} g_n) = \pi(t^{-1} \cdot \alpha_n \cdot \bar{g}_n) = \pi(\phi(\alpha_n) \cdot t^{-1} \cdot \bar{g}_n)$$

Συνεχίζοντας με αυτόν τον τρόπο, βρίσκουμε την λεγόμενη μορφή του $g \in G*_A$.

Ορισμός 9.6.2. Μια **κανονική μορφή** είναι μια ανηγμένη λέξη $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$, όπου:

(i) g_0 αυθαίρετο στοιχείο της G,

(ii) αν $\varepsilon_i = -1$, τότε $g_i \in T_A$, και

(iii) αν $\varepsilon_i = 1$, τότε $g_i \in T_B$.

Όπως και στα ελεύθερα γινόμενα με αμάλγαμα, αποδεικνύεται ότι:

Θεώρημα 9.6.1. *Έστω $G*_A$ μια HNN επέκταση με βάση G και προσεταιριζόμενες ομάδες A, B. Τότε, κάθε στοιχείο $x \in G*_A$ γράφεται κατά μοναδικό τρόπο ως*

$$x = \pi(g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n)$$

όπου $(g_0, \varepsilon_1, g_1, \ldots, t^{\varepsilon_n}, g_n)$ μια κανονική μορφή.

Πόρισμα 9.6.1. *Ο περιορισμός στην G του φυσικού επιμορφισμού $\pi : G * \langle t \rangle \to G*_A$ είναι μονομορφισμός.*

Συνεπώς, $G \hookrightarrow G*_A$, και όμοια $\langle t \rangle \hookrightarrow G*_A$.

Πόρισμα 9.6.2. *Αν $(g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n)$ κανονική μορφή και $n > 0$, τότε $\pi(g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n) \neq 1$.*

Τελικά, έχουμε εμφυτεύσεις G, $\langle t \rangle \hookrightarrow G*_A$ και $g = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$ σε κανονική μορφή. Έτσι, οι A, B γίνονται συζυγείς στην $G*_A$.

Ας δούμε, τώρα, δύο εφαρμογές των HNN επεκτάσεων:

Θεώρημα 9.6.2. *Κάθε αριθμήσιμη ομάδα G μπορεί να εμφυτευθεί σε μια ομάδα με δύο γεννήτορες.*

Απόδειξη. Έστω $g_0, g_1, \ldots, g_n, \ldots$ αριθμήσιμο -όχι πεπερασμένο- σύνολο γεννητόρων της G έτσι ώστε $g_0 = 1$ και ενδέχεται να υπάρχουν επαναλήψεις, για παράδειγμα αν η G είναι πεπερασμένη.

Έστω $F = F(\alpha, \beta)$ ελεύθερη στο $\{\alpha, \beta\}$ και $G * F$ το ελεύθερο γινόμενο των G και F.

Η υποομάδα της F,

$$A = \langle \beta^{-n} \alpha \beta^n : n \geq 0 \rangle$$

είναι ελεύθερη επί του $\{\beta^{-n} \alpha \beta^n : n \geq 0\}$ και η

$$\langle \alpha^{-n} \beta \alpha^n : n \geq 0 \rangle$$

ελεύθερη επί του $\{\alpha^{-n} \beta \alpha^n : n \geq 0\}$.

Έστω

$$\phi : G * F \to F, \quad g_n \alpha^{-n} \beta \alpha^n \mapsto \alpha^{-n} \beta \alpha^n$$

Εφόσον ο ϕ είναι 1-1 στο $\{g_n \alpha^{-n} \beta \alpha^n : n \geq 0\}$, έπεται ότι και η

$$B = \langle g_n n \alpha^{-n} \beta \alpha^n : n \geq 0 \rangle$$

είναι ελεύθερη υποομάδα της $G * F$ επεί του $\{g_n\alpha^{-n}\beta\alpha^n : n \geq 0\}$.

Έστω

$$\Gamma = \langle G * F, t \mid t^{-1}\beta^{-n}\alpha\beta^n t = g_n\alpha^{-n}\beta\alpha^n : n \geq 0\rangle$$

η HNN επέκταση με βάση $G * F$ και προσεταιριζόμενες υποομάδες A, B.

Τότε, $G \hookrightarrow \Gamma$ και η Γ παράγεται από δύο στοιχεία,

$$\Gamma = \langle g_n, \alpha, \beta, t : n \geq 0\rangle = \langle \alpha, \beta, t\rangle = \langle \alpha, t\rangle$$

□

Θεώρημα 9.6.3. *Για $(p, q) = 1$, η ομάδα*

$$G_{p,q} = \langle \beta, t \mid t^{-1}\beta^p t = \beta^q\rangle$$

δεν είναι Hopfian, και συνεπώς ούτε προσεγγιστικά πεπερασμένη.

Απόδειξη. Η $G_{p,q}$ είναι HNN επέκταση με βάση άπειρη κυκλική $\langle\beta\rangle$ και προσεταιριζόμενες υποομάδες $\langle\beta^p\rangle$, $\langle\beta\rangle$.

Η απεικόνιση $\psi : t \mapsto t$, $\beta \mapsto \beta^p$, επάγει ομομορφισμό $\psi : G_{p,q} \to G_{p,q}$ -για απλότητα χρησιμοποιούμε το ίδιο σύμβολο- γιατί:

$$\begin{aligned}\psi(t^{-1}\beta^p t) &= t^{-1}\psi(\beta^p)t = t^{-1}(\beta^p)^p t\\ &= (t^{-1}\beta^p t)^p = (\beta^q)^p\\ &= (\beta^p)^q = \psi(\beta^q)\end{aligned}$$

Ο ομομορφισμός ψ είναι επί: Η εικόνα του ψ περιέχει τα t, β^p και β^q. Όμως, $(p, q) = 1$, συνεπώς η εικόνα του ψ περιέχει τα t και β. Έτσι, $\operatorname{im}\psi = G_{p,q}$.

Τέλος, $\ker\psi \neq 1$. Έχουμε

$$\begin{aligned}\psi(t^{-1}\beta t\beta^{-1}) &= (t^{-1}\beta^p t\beta^{-p})^p = (\beta^{q-p})^p\\ &= (\beta^p)^{q-p} = \psi(\beta)^{q-p}\\ &= \psi(\beta^{q-p})\end{aligned}$$

άρα $(t^{-1}\beta t\beta^{-1})\beta^{p-q} \in \ker\psi$.

Επιπλέον, $(t^{-1}\beta t\beta^{-1})\beta^{p-q} \neq 1$. Για να το δούμε αυτό, αρκεί να επιλέξουμε τα β και β^{-1} στα σύνολα αντιπροσώπων, για παράδειγμα $\beta \in T_A$ και $\beta^{-1} \in T_B$. □

Κλείνοντας το κεφάλαιο, επισημαίνουμε ότι:

- Η G είναι ελεύθερη ανν δρα ελεύθερα, χωρίς αντιστροφές, σε ένα δέντρο.
- Η G είναι ελεύθερο γινόμενο ανν δρα, χωρίς αντιστροφές, σε ένα δέντρο ελεύθερα επί των ακμών, δηλαδή η σταθεροποιούσα κάθε ακμής είναι ίση με 1.
- Η G είναι ελεύθερο γινόμενο με αμάλγαμα δύο παραγόντων ανν δρα, χωρίς αντιστροφές, σε ένα δέντρο με μια τροχιά γεωμετρικών ακμών και δύο τροχιές κορυφών.

  Δηλαδή, το γράφημα πηλίκο είναι:
- Η G είναι HNN επέκταση ανν δρα, χωρίς αντιστροφές, σε ένα δέντρο με μια τροχιά κορυφών και μια τροχιά ακμών.

  Δηλαδή, το γράφημα πηλίκο είναι: 

9.7 Ασκήσεις

1. Μια αβελιανή ομάδα είναι προβολική ανν είναι ελεύθερη αβελιανή.

2. Αν η G είναι ελεύθερη αβελιανή διάστασης n, τότε η G δεν μπορεί να παραχθεί από m στοιχεία, όπου $m < n$.

3. Έστω F ελεύθερη αβελιανή ομάδα πεπερασμένης διαστάσης $n < \infty$ και $H \leq F$. Τότε, η F/H είναι πεπερασμένη ανν $\text{rank}(F) = \text{rank}(H)$.

4. Αν G ελεύθερη αβελιανή πεπερασμένης διάστασης και $\phi : G \to H$ επιμορφισμός, τότε $\text{rank}(G) = \text{rank}(H) + \text{rank}(\ker \phi)$.

5. Έστω F ελεύθερη αβελιανή διάστασης n. Αποδείξτε ότι $\text{Aut}(F) \simeq GL_n(\mathbb{Z})$.

6. Αν $G = \underset{\alpha}{*} G_\alpha$ και $G_\alpha = \underset{\beta}{*} H_{\alpha\beta}$ για κάθε α, τότε η G είναι το ελεύθερο γινόμενο όλων των $H_{\alpha\beta}$, το οποίο ελεύθερο γινόμενο ονομάζεται **επιλέπτυνση** του αρχικού.

7. Αν $G = \underset{\alpha}{*} G_\alpha$ και $1 \leq H_\alpha \leq G_\alpha$ για κάθε α, τότε η υποομάδα της G που παράγεται από τις H_α είναι το ελεύθερο γινόμενο των H_α, δηλαδή $\underset{\alpha}{*} H_\alpha = \langle H_\alpha : \alpha \rangle$.

8. (i) (Καθολική ιδιότητα του ευθέως αθροίσματος) Έστω G αβελιανή ομάδα και G_α, $\alpha \in J$, οικογένεια υποομάδων της G. Αν $G = \bigoplus_{\alpha \in J} G_\alpha$, τότε για κάθε αβελιανή ομάδα H και κάθε οικογένεια ομομορφισμών $\phi_\alpha : G_\alpha \to H$, υπάρχει μοναδικός ομομορφισμός $\phi : G \to H$ που επεκτείνει τις ϕ_α (ή $\phi \circ i_\alpha = \phi_\alpha$).

   (ii) Αν $G = \underset{\alpha}{*} G_\alpha$ και G' η παράγωγος υποομάδα της G, τότε $G/G' = \bigoplus_\alpha G_\alpha/G'_\alpha$.

   [Υπόδειξη: Η G/G' ικανοποιεί την καθολική ιδιότητα του ευθέως αθροίσματος.]

9. Αν $G_\alpha \neq 1$ για κάθε $\alpha \in J$, όπου $|J| \geq 2$, τότε $Z(\underset{\alpha}{*} G_\alpha) = 1$.

10. Αν $G = \underset{\alpha \in J}{*} G_\alpha$ με $G_\alpha \neq 1$ για κάθε α και $|J| \geq 2$, τότε η G περιέχει στοιχεία απείρου τάξης.

    Ιδιαιτέρως, η G είναι άπειρη ομάδα.

11. Κάθε στοιχείο πεπερασμένης τάξης σε ένα ελεύθερο γινόμενο $\underset{\alpha}{*} G_\alpha$, είναι συζυγές με στοιχείο ενός ελεύθερου παράγοντα.

    Ιδιαιτέρως, αν κάθε G_α είναι ελευθέρα στρέψης, τότε η $\underset{\alpha}{*} G_\alpha$ είναι ελευθέρα στρέψης.

12. Η ελεύθερη ομάδα διάστασης 2, F_2, περιέχει ελεύθερη υποομάδα διάστασης k, για κάθε φυσικό k.

13. Η F_2 περιέχει ελεύθερη υποομάδα απείρου τάξης.

14. Κάθε πεπερασμένα παραγόμενη ελεύθερη ομάδα είναι $\mathbb{Z}$-γραμμική, δηλαδή εμφυτεύεται στην $GL_n(\mathbb{Z})$.

15. Αν $N \lhd G$ και η G/N είναι ελεύθερη, τότε υπάρχει υποομάδα H της G με $G = HN$ και $H \cap N = 1$.

16. Έστω F ελεύθερη ομάδα και $H \leq F$ υποομάδα πεπερασμένου δείκτη. Αν $K \leq F$ με $K \neq 1$, τότε $K \cap H \neq 1$.

17. Κάθε πεπερασμένα παραγόμενη ελεύθερη ομάδα έχει πεπερασμένη διάσταση.

18. Έστω G_λ, $\lambda \in \Lambda$, οικογένεια ομάδων, H ομάδα, $\phi_\lambda : H \to G_\lambda$ οικογένεια ομομορφισμών και $G = \underset{H}{*} G_\lambda$ το αντίστοιχο ελεύθερο γινόμενο με αμάλγαμα. Αποδετε ότι για κάθε ομάδα K και οικογένεια ομομορφισμών $\theta_\lambda : G_\lambda \to K$ με $\theta_\lambda \circ \phi_\lambda = \theta_\mu \circ \phi_\mu$ για κάθε ζεύγος λ, $\mu \in \Lambda$, υπάρχει μοναδικός ομομορφισμός $\theta : G \to K$ με $\theta \circ \pi_\lambda = \theta_\lambda$, για κάθε λ, όπου π_λ ο περιορισμός στην G_λ του φυσικού επιμορφισμού $\pi : \underset{H}{*} G_\lambda \to G$.

19. Έστω $\phi_i : H \to G_i$, $= 1, 2$, μονομορφισμοί, $G_1 \underset{H}{*} G_2$ το αντίστοιχο ελεύθερο γινόμενο με αμάλγαμα και $\pi : G_1 * G_2 \to G_1 \underset{H}{*} G_2$ ο φυσικός επιμορφισμός.

    Για κάθε στοιχείο g της $G_1 \underset{H}{*} G_2$ που μπορεί να γραφεί ως $g = \pi(g_1)\pi(g_2)\cdots\pi(g_n)$, όπου $g_i \in G_1 \backslash H$ ή $G_2 \backslash H$ και διαδοχικά g_i δεν ανήκουν στο ίδιο $G_j \backslash H$ ισχύει ότι $g \neq 1$.

    Να δειχθεί, επίσης, ότι κάθε στοιχείο $g \in G_1 \underset{H}{*} G_2$ με $g \notin \pi(H)$, μποεί να γραφεί ως γινόμενο με τον παραπάνω τρόπο.

20. Αν $G_1 \neq H \neq G_2$, τότε η ομάδα $G_1 \underset{H}{*} G_2$ περιέχει στοιχεία απείρου τάξης,

21. Έστω G_1, G_2 υποομάδες μιας ομάδας G και $H = G_1 \cap G_2$. Υποθέτουμε ότι η G παράγεται από τις G_1 και G_2. Έστω $\phi : G_1 \underset{H}{*} G_2 \to G$ ο επιμορφισμός που επάγεται από τις ενθέσεις των G_1 και G_2 στην G.

    Αποδείξτε ότι ο ϕ είναι ισομορφισμός ανν κάθε γινόμενο $g_1 g_2 \cdots g_n$ στην G, όπου $g_k \in G_1 \backslash H$ ή $G_2 \backslash H$ και διαδοχικοίι παράγοντες δεν ανήκουν στο ίδιο σύνολο $G_i \backslash H$, είναι διάφορο του 1.

Κεφάλαιο 10

Απλές Ομάδες

Έχοντας παρατήσει, σχετικά σύντομα, την ιδέα να κατανοήσουμε κάθε ομάδα, προσπαθούμε να χειριστούμε τις πεπερασμένες απλές ομάδες, ή καλύτερα, να απαντήσουμε στο ερώτημα: για ποιές τάξεις υπάρχουν απλές ομάδες και ποιές είναι αυτές οι ομάδες όταν υπάρχουν; Η απάντηση στο ερώτημα αυτό ήταν, ίσως, το κυριότερο μέλημα για όσους ασχολούνταν με τη Θεωρία Ομάδων και τώρα δόθηκε. Η πλήρης ταξινόμηση ξεφεύγει από τους σκοπούς των παρόντων σημειώσεων, αλλά μπορεί να γίνει μια αρχή.

Αν κάποιος επικεντρωθεί στο μέρος του προβλήματος που ρωτάει για ποιες τάξεις δεν υπάρχουν απλές ομάδες, τότε μπορούμε να θεωρήσουμε ότι έχουμε κάνει μια αξιοπρεπή αρχή: θα αποκλείσουμε άπειρες πιθανές τάξεις. Αυτό, βέβαια, αφήνει άπειρες ακόμη τάξεις να ελεγχθούν, αλλά είναι πολύ καλύτερα από το να αποκλείαμε πεπερασμένες το πλήθος τάξεις.

Κάποιος μπορεί, βάσιμα, να αναρωτηθεί γιατί ταξινομούμε μόνο τις πεπερασμένες ομάδες. Αυτό γίνεται επειδή *αν* γνωρίζαμε όλες τις απλές πεπερασμένες ομάδες και *αν* μπορούσαμε να λύσουμε το πρόβλημα της επέκτασης για πεπερασμένες ομάδες, τότε θα γνωρίζαμε όλες τις πεπερασμένες ομάδες. Όσο δύσκολη κι αν φαίνεται αυτή η προσέγγιση, είναι πολύ ευκολότερη από την προσέγγιση τάξη-προς-τάξη.

10.1 Η απλότητα της A_n

Θα αποδείξουμε ότι η A_n είναι απλή για κάθε $n \geq 5$. Η A_4 δεν είναι απλή, γιατί περιέχει κανονική υποομάδα, την ομάδα Klein, V.

Λήμμα 10.1.1. *Η A_5 είναι απλή.*

Απόδειξη. Η απόδειξη γίνεται σε τρία βήματα.

(i) Όλοι οι 3-κύκλοι είναι συζυγείς στην A_5.

Αν, παραδείγματος χάριν, $\alpha = (1\ 2\ 3)$, τότε η περιττή μετάθεση $(1\ 2)$ μετατίθεται με την α. Εφόσον η A_5 είναι δείκτου 2 στην S_5, είναι μια κανονική υποομάδα πρώτου δείκτη, άρα το α έχει ίδιο πλήθος συζυγών στην A_5 και στην S_5, επειδή $\mathrm{Cl}_{A_5}(\alpha) < \mathrm{Cl}_{S_5}(\alpha)$.

(ii) Όλα τα γινόμενα ξένων αντιμεταθέσεων είναι συζυγή στην A_5.

Αν $\alpha = (1\ 2)(3\ 4)$, τότε η $(1\ 2)$ μετατίθεται με το α. Εφόσον η A_5 είναι δείκτου 2 στην S_5, το α έχει ίδιο πλήθος συζυγών στην A_5 και στην S_5.

(iii) Υπάρχουν δύο συζυγείς κλάσεις 5-κύκλων στην A_5, καθεμία από τις οποίες έχει 12 στοιχεία.

Στην S_5 η $\alpha = (1\ 2\ 3\ 4\ 5)$ έχει 24 συζυγή στοιχεία, και έτσι η $\mathrm{Cl}_{S_5}(\alpha)$ έχει 5 στοιχεία, τα οποία πρέπει να είναι δυνάμεις του α. Εφόσον $|\mathrm{Cl}_{A_5}(\alpha)| = 5$, η $\mathrm{Cl}_{A_5}(\alpha)$ είναι δείκτη 12.

Μελετήσαμε όλες τις κλάσεις συζυγίας που προκύπτουν στην A_5. Αφού κάθε κανονική υποομάδα H της A_5 είναι ένωση κλάσεων συζυγίας, η $|H|$ είναι άθροισμα των 1 και κάποιων εκ των ακεραίων: 12, 12, 15 και 20. Εύκολα, βλέπουμε ότι κανένα άθροισμα δεν είναι γνήσιος διαιρέτης του 60, άρα $|H| = 60$ και η A_5 είναι απλή. □

Λήμμα 10.1.2. *Έστω $H \lhd A_n$, όπου $n \geq 5$. Αν η H περιέχει έναν 3-κύκλο, τότε $H = A_n$.*

Απόδειξη. Δείχνουμε ότι τα $(1\ 2\ 3)$ και $(i\ j\ k)$ είναι συζυγή στην A_n, και άρα όλοι οι 3-κύκλοι είναι συζυγείς στην A_n. Αν αυτοί οι κύκλοι δεν είναι ξένοι, τότε ο καθένας σταθεροποιεί όλα τα σύμβολα εκτός των $\{1, 2, 3, i, j\}$, και οι δύο κύκλοι αυτοί ανήκουν στην A^*, την ομάδα όλων των περιττών μεταθέσεων σε αυτά τα 5 σύμβολα.

Ισχύει $A^* \simeq A_5$ και όπως πριν, στην απόδειξη του (i) του προηγούμενου λήμματος, τα $(1\ 2\ 3)$ και $(i\ j\ k)$ είναι συζυγή στην A^*, άρα και στην A_n.

Αν οι κύκλοι είναι ξένοι, έχουμε ήδη δει ότι ο $(1\ 2\ 3)$ είναι συζυγής στον $(3\ j\ k)$ και ο $(3\ j\ k)$ είναι συζυγής στον $(i\ j\ k)$.

Μια κανονική υποομάδα H που περιέχει έναν 3-κύκλο α πρέπει να περιέχει κάθε συζυγές του α. Αφού όλοι οι 3-κύκλοι είναι συζυγείς,η H περιέχει κάθε 3-κύκλο. Γνωρίζουμε, όμως, ότι η A_n παράγεται από τους 3-κύκλους, άρα $H = A_n$. □

Λήμμα 10.1.3. *Η A_6 είναι απλή.*

Απόδειξη. Έστω $H \neq 1$ απλή υποομάδα της A_6 και $\alpha \in H$ διάφορο του 1. Αν το α σταθεροποιεί κάποιο i, ορίζουμε

$$F = \{\beta \in A_6 : \beta(i) = i\}$$

Τώρα, $F \simeq A_5$ και $\alpha \in H \cap F$. Αλλά $H \cap F \lhd F$, και έτσι αν η F είναι απλή και $H \cap F \neq 1$, τότε $H \cap F = F$, δηλαδή $F \leq H$. Τελικά, η H περιέχει 3-κύκλο, $H = A_6$ και τελειώσαμε.

Μπορούμε να υποθέσουμε ότι κανένα $\alpha \in H$ με $\alpha \neq 1$ δεν σταθεροποιεί το i, για $1 \leq i \leq 6$. Μπορούμε να δούμε, τότε, ότι το α είναι $(1\ 2)(3\ 4\ 5\ 6)$ ή $(1\ 2\ 3)(4\ 5\ 6)$. Στη πρώτη περίπτωση, $\alpha^2 \in H$, $\alpha^2 \neq 1$ και το α^2 σταθεροποιεί το 1 -άτοπο. Στη δεύτερη περίπτωση, το H περιέχει το $\alpha(\beta\alpha^{-1}\beta^{-1})$, όπου $\beta = (2\ 3\ 4)$, και εύκολα ελεχεται ότι αυτό το στοιχείο δεν είναι ταυτοτικό και σταθεροποιεί το 1 -άτοπο. □

Θεώρημα 10.1.1. *Η A_n είναι απλή για κάθε $n \geq 5$.*

Απόδειξη. Έστω $n \geq 5$ και $H \neq 1$ κανονική υποομάδα της A_n. Αν $\beta \in H$ και $\beta \neq 1$, τότε υπάρχει i με $\beta(i) = j \neq i$. Αν α ένας 3-κύκλος που σταθεροποιεί το i και μεταθέτει το j, τότε τα α και β δεν μετατίθενται. Έτσι, $[\alpha, \beta] \neq 1$ και $[\alpha, \beta] \in H$. Επιπλέον, ο μεταθέτης τους είναι γινόμενο δύο 3-κύκλων $(\alpha\beta\alpha^{-1})\beta^{-1}$, οπότε μεταθέτει το πολύ έξι σύμβολα, έστω $i_1, i_2, \ldots, i_6$. Αν

$$F = \{\gamma \in A_m : \gamma(k) = k,\ \forall k \neq i_\ell,\ 1 \leq \ell \leq 6\}$$

τότε $F \simeq A_6$ και $\alpha\beta\alpha^{-1}\beta^{-1} \in H \cap F \lhd F$. Εφόσον η A_6 είναι απλή, $H \cap F = F$ και $F \leq H$.

Τελικά, η H περιέχει 3-κύκλο και $H = A_n$. □

10.2 Η απλότητα της $PSL(n,q)$

Ορισμός 10.2.1. Έστω F σώμα.

(i) Η **γενική γραμμική** ομάδα βαθμού n επί του F, $GL(n,F)$, είναι η ομάδα των $n \times n$ πινάκων, με στοιχεία από το F, που έχουν μη-μηδενική ορίζουσα.

(ii) Η **ειδική γραμμική** ομάδα βαθμού n επί του F, $SL(n,F)$, είναι η υποομάδα της $GL(n,F)$ που αποτελείται από πίνακες που έχουν ορίζουσα 1.

(iii) Η **προβολική γενική γραμμική** ομάδα βαθμού n επί του F, $PGL(n,F)$, είναι η ομάδα πηλίκο $GL(n,F)/Z(GL(n,F))$.

(iv) Η **προβολική ειδική γραμμική** ομάδα βαθμού n επί του F, $PSL(n,F)$, είναι η ομάδα πηλίκο $SL(n,F)/Z(SL(n,F))$.

Ο ορισμός της ειδικής γραμμικής ομάδας είναι αρκετά σαφής, ετσί ώστε να γνωρίζουμε ποιά είναι τα στοιχεία της. Δεν ισχύει το ίδιο, όμως, για την προβολική ειδική γραμμική ομάδα. Βρίσκουμε, λοιπόν, τις $Z(GL(n,F))$ και $Z(SL(n,F))$.

Λήμμα 10.2.1. *(i)* $Z(GL(n,F)) = \{\lambda I_n : \lambda \in F\backslash\{0\}\}$,

(ii) $Z(SL(n,F)) = Z(GL(n,F)) \cap SL(n,F) = \{\lambda I_n : \lambda \in F\backslash\{0\},\ \lambda^n = 1\}$.

Απόδειξη. Το πρώτο μέρος είναι βασικές γνώσεις γραμμικής άλγεβρας, και το δεύτερο έπεται άμεσα. □

Παρατηρήστε ότι, αν και η $SL(n,F)$ είναι υποομάδα της $GL(n,F)$, η $PSL(n,F)$ δεν είναι υποομάδα της $PGL(n,F)$. Παρ' όλα αυτά, υπάρχει ένας φυσικός ισομορφισμός της $PSL(n,F)$ με μια κανονική υποομάδα της $PGL(n,F)$.

Ιδιαίτερη σημασίας είναι η περίπτωση όπου το F είναι ένα πεπερασμένο σώμα. Υπενθυμίζουμε ότι τα πεπερασμένα σώματα έχουν τάξη μια δύναμη πρώτου αριθμού, και ότι κάθε δύο πεπερασμένα σώματα ίδιας τάξης είναι ισόμορφα. Αν $|F| = q$, θα γράφουμε $GL(n,q)$ αντί για $GL(n,F)$, και όμοια και για τις υπόλοιπες ομάδες πινάκων. Αν F ένα πεπερασμένο σώμα τάξης q, τότε η $GL(n,q)$ είναι πεπερασμένη, άρα και οι υπόλοιπες γραμμικές ομάδες, και μπορούμε να βρούμε την τάξη της.

Λήμμα 10.2.2. *Έστω F σώμα τάξης q, και έστω t το πλήθος των ριζών του πολυωνύμου $x^n - 1 \in F[x]$. Τότε, $t = (n, q-1)$, και:*

(i) $|GL(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i)$,

(ii) $|SL(n,q)| = |GL(n,q)|/(q-1)$,

(iii) $|PGL(n,q)| = |GL(n,q)|/(q-1)$ *και*

(iv) $|PSL(n,q)| = |SL(n,q)|/t = \frac{1}{(n,q-1)} q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n}(q^i - 1)$.

Αυτές οι ομάδες σας είναι αρκετά οικείες.

Παραδείγματα 10.2.1. (i) Προφανώς, $GL(1,F) \simeq F^*$, και έτσι

$$PGL(1,F) \simeq SL(1,F) \simeq PSL(1,F) \simeq 1$$

(ii) Εφόσον οι μόνες δεύτερες ρίζες της μονάδας είναι τα 1 και -1, έχουμε $Z(SL(2,\mathbb{C}) = \{I_2, -I_2\}$. Μπορεί να αποδειχθεί ότι $PSL(2,\mathbb{C}) \simeq PGL(2,\mathbb{C})$. Μάλιστα, η ομάδα αυτή είναι η ομάδα των μετασχηματισμών Mobius στη σφαίρα Riemann.

(iii) Έστω $F = \mathbb{F}_2$ το πεπερασμένο σώμα με 2 στοιχεία. Τότε, η $PSL(2,2)$ έχει 6 στοιχεία. Εύκολα, παρατηρεί κανείς ότι η ομάδα αυτή δεν είναι αβελιανή, άρα είναι ισόμορφη με την S_3.

(iv) Αν $F = \mathbb{F}_2$, τότε $q - 1 = 1$ και $(n, q-1) = 1$, άρα και οι τέσσερις ομάδες $GL(n,2)$, $SL(n,2)$, $PGL(n,2)$ και $PSL(n,2)$ έχουν ίδιες τάξεις. Έστι, $GL(n,2) = SL(n,2)$ και $PGL(n,2) = PSL(n,2)$.

(v) Αν $F = \mathbb{F}_3$, τότε $|PSL(2,3)| = 12$ και αποδεικνύεται ότι η $PSL(2,3)$ είναι ισόμορφη με την A_4.

Η ορολογία "προβολική" αναφέρεται στο γεγονός ότι αυτές οι ομάδες δρουν σε προβολικούς χώρους. Χώροι όπως ο $\mathbb{C}^n$ και ο $\mathbb{R}^n$ καλούνται αφινικοί χώροι, και οι προβολικοί χώροι είναι πηλίκα τους. Ο κύριος, γεωμετρικός, λόγος που μελετάμε προβολικούς χώρους αντί για αφινικούς είναι ότι οι προβολικοί χώροι είναι συμπαγείς τοπολογικοί χώροι. Ο γενικός ορισμός ενός προβολικού n-διάστατου χώρου είναι ο ακόλουθος:

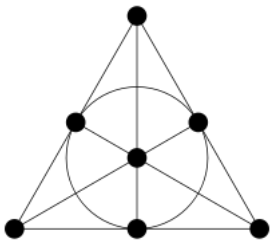
Ορισμός 10.2.2. Έστω F σώμα. Ο **προβολικός χώρος** διάστασης n επί του F, $F\mathbb{P}^n$, είναι το πηλίκο του $F^{n+1}\backslash\{0\}$ που δίνεται από τη σχέση ισοδυναμίας:

$$v \sim w \Longleftrightarrow \exists \lambda \in F^* : v = \lambda w$$

Ισοδύναμα, ο προβολικός χώρος διάστασης n είναι ο χώρος των ευθειών του F^{n+1} που περνάνε από το 0.

Έτσι, όπως η $GL(n,F)$ είναι η ομάδα των αυτομορφισμών του F^n, η $PGL(n+1,F)$ είναι η ομάδα των αυτομορφισμών του $F\mathbb{P}^n$. Ειδικότερα, η $PGL(2,\mathbb{C})$ είναι η ομάδα αυτομορφισμών του $\mathbb{CP}^1$, κάτι που είδαμε και προηγουμένως.

Το μικρότερο προβολικό επίπεδο είναι το $\mathbb{F}_2\mathbb{P}^2$. Από τα παραπάνω, η ομάδα αυτομορφισμών του είναι η $PGL(3,2)$. Το προβολικό επίπεδο $\mathbb{F}_2\mathbb{P}^2$ καλείται και επίπεδο Fano. Τα σημεία του είναι σε αντιστοιχεία με τα στοιχεία του $\mathbb{F}_2^3\backslash\{0\}$, άρα είναι 7. Οι ευθείες είναι όπως στο παρακάτω σχήμα.



Επικεντρωνόμαστε στις ειδικές προβολικές ομάδες επί πεπερασμένων σωμάτων, αφού είναι πεπερασμένες. Σημειώνουμε ότι οι ισομοφισμοί $PSL(2,2) \simeq S_3$ και $PSL(2,3) \simeq A_4$ δείχνουν ότι οι ομάδες αυτές δεν είναι απλές. Αυτό, όμως, δεν ισχύει γενικά, αφού οι $PSL(2,4) \simeq PSL(2,5) \simeq A_5$, $PSL(2,9) \simeq A_6$ και $PSL(4,2) \simeq A_8$ είναι απλές ομάδες.

Προχωράμε, τώρα, στην $PSL(2,7)$, την πρώτη $PSL(2,q)$ που δεν έχουμε ήδη συζητήσει.

Θεώρημα 10.2.1. *Η ομάδα $PSL(2,7)$, με τάξη 168, είναι απλή.*

Απόδειξη. Καταρχάς, $168 = 2^3 \cdot 3 \cdot 7$. Έστω N μεγιστική μη-τετριμμένη κανονική υποομάδα της $G = PSL(2,7)$. Έτσι, η G/N είναι απλή και έχει τάξη το πολύ $168/2 = 84$. Εφόσον η μόνη μη-αβελιανή απλή ομάδα τάξης το πολύ 84 είναι η A_5, τάξης 60, και $60 \nmid 168$, η G/N είναι αβελιανή απλή ομάδα, άρα κυκλική τάξεως 2, 3 ή 7.

Αν $M \in SL(2,7)$, έστω $[M]$ το αντίστοιχο σύμπλοκο $Z(SL(2,7))M$ στην $PSL(2,7)$. Έστω

$$x = \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right]$$

και

$$y = \left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right]$$

Τότε, τα x και y έχουν τάξη 7, και αν θέσουμε $u = xy^2x$, τότε

$$u = \left[\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}\right]$$

και έχουμε ένα στοιχείο τάξης 3. Εφόσον $|\langle x\rangle| = |\langle y\rangle| = 7$ και $y \notin \langle x\rangle$, η G έχει τουλάχιστον δύο Sylow 7-υποομάδες.

Αν $|G/N| = 2$, η N είναι κανονική υποομάδα της G τάξης 84 και δείκτη 2. Από τα Θεωρήματα Sylow, μια ομάδα τάξης 84 έχει μοναδική Sylow 7-υποομάδα. Έτσι, εφόσον αυτή θα είναι μια Sylow 7-υποομάδα της G συζυγής μόνο στον εαυτό της, η G θα έχει μοναδική Sylow 7-υποομάδα, το οποίο είναι άτοπο.

Αν $|G/N| = 3$, τότε $x, y \in N$ και $u \in N$. Άτοπο, γιατί $3 \nmid |N| = 56$. Έτσι, $|G/N| = 7$. Από τα Θεωρήματα Sylow, η N έχει 1 ή 3 Sylow 2-υποομάδες , και αυτές είναι όλες οι Sylow 2-υποομάδες της G, αφού $N \lhd G$.

Αν η G έχει μοναδική Sylow 2-υποομάδα, έστω την S, τότε $S \lhd G$ και η G/S, τάξης 21, έχει μοναδική Sylow 7-υποομάδα δείκτου 3. Μια τέτοια υποομάδα της G/S θα έδινε μια κανονική υποομάδα της G δείκτου 3 -άτοπο.

Τελικά, η G έχει 3 Sylow 2-υποομάδες και αν H η κανονικοποιούσα μιας εξ αυτών, τότε η H είναι δείκτου 3 στην G. Εφόσον απορρίψαμε την ύπαρξη κανονικών ομάδων δείκτου 3, η H δεν είναι κανονική, και η δράση της G στα σύμπλοκα της H, μας δίνει ομομορφισμό από τη G στην S_3, που έχει πυρήνα δείκτη > 3.

Άλλά η S_3 έχει υποομάδα δείκτη 2, που θα μας έδινε ομάδα δείκτη 2 στην G. Εφόσον οι υποομάδες δείκτη 2 είναι κανονικές, θα είχαμε μια κανονική υποομάδα τάξης 84 -άτοπο. □

Μάλιστα, ισχύει το ακόλουθο:

Θεώρημα 10.2.2. *Για κάθε $n \geq 2$ και p πρώτο με $p \neq 2, 3$, η ομάδα $PSL(n,q)$ είναι απλή.*

Σημειώνουμε ότι η απόδειξη δεν προχωρά όμοια με την περίπτωση της $PSL(2,7)$.

Αντίθετα, πρέπει να βρούμε κάποια "καλά" στοιχεία και να χρησιμοποιήσουμε γραμμική άλγεβρα και γεωμετρικά επιχειρήματα.

Οι προβολικές ειδικές γραμμικές ομάδες αποτελούν μέρος μιας οικογένειας ομάδων που καλούνται ομάδες τύπου Lie. Οι πεπερασμένες απλές ομάδες μέλη αυτής της οικογένειας, αποτελούν τη τρίτη και τελευταία άπειρη κλάση πεπερασμένων απλών ομάδων.

10.3 Η ταξινόμηση των πεπερασμένων απλών ομάδων

Το πλήρες θεώρημα της ταξινόμησης θα χρειαζόταν πολύ χώρο και χρόνο για να διατυπωθεί, αλλά κανείς παίρνει μια γεύση του θεωρήματος από την παρακάτω σύνοψη:

Θεώρημα 10.3.1. *Κάθε πεπερασμένη απλή ομάδα είναι ισόμορφη με:*

(i) μια κυκλική ομάδα πρώτης τάξης, ή

(ii) μια εναλλακτική ομάδα A_n για κάποιο $n \geq 5$, ή

(iii) μια απλή ομάδα τύπου Lie επί του $\mathbb{F}_q$, ή

(iv) μια εκ των 26 σποραδικών απλών ομάδων.

Τα δύο πρώτα μέρη έχουν αποδειχθεί, και το τρίτο εισήχθη στην προηγούμενη ενότητα. Ειδικότερα, οι ομάδες $PSL(n, q)$ είναι απλές ομάδες τύπου Lie. Ορισμένες άλλες ομάδες τύπου Lie μπορούν να κατασκευαστούν ως ομάδες πινάκων που διατηρούν εσωτερικά γινόμενα διαφόρων τύπων.

Υπάρχει μια άλλη προσέγγιση, που οφείλεται στον Chevalley, που εμπλέκει άλγεβρες Lie. Μια άλγεβρα Lie επί ενός σώματος F είναι ένας F-διανυσματικός χώρος L με μια απεικόνιση $L \times L \to L$, που καλείται αγκύλη Lie, τέτοια ώστε

(i) $[x, x] = 0$ και

(ii) $[[x, y], z] + [[y, z], x] + [[z, x, y] = 0$.

Τότε, μπορεί κανείς να ορίσει ένα ιδεώδες της άλγεβρας Lie L να είναι ένας υπόχωρος I τέτοιος ώστε: αν $i \in I, x \in L$, τότε $[i, x] \in I$, και λέμε ότι η L είναι απλή αν δεν έχει γνήσιο ιδεώδες. Οι άλγεβρες Lie πεπερασμένης διάστασης επί του $\mathbb{C}$ ταξινομήθηκαν από τους Cartan και Killing και είναι οι: A_n με $n \geq 1$, B_n με $n \geq 2$, C_n με $n \geq 3$, D_n με $n \geq 4$, E_6, E_7, E_8, F_4 και G_2.

Αυτές δεν δίνουν άμεσα πεπερασμένες απλές ομάδες, αλλά μπορεί κανείς να διαλέξει μια "καλή" βάση για μια απλή μιγαδική άλγεβρα Lie και μετά να θεωρήσει την άλγεβρα $L(q)$ επί του $\mathbb{F}_q$ που δίνεται από την $\mathbb{F}_q-$θήκη αυτής της βάσης. Τότε, η $\mathrm{Aut}(L(q))$ έχει έναν μη κυκλικό παράγοντα διάσπασης, μια απλή πεπερασμένη ομάδα.

Έχουμε ότι $A_n(q) \simeq PSL(n+1, q)$, $B_n(q) \simeq P\Omega_{2n+1}(q)$, $C_n(q) \simeq PSp_{2n}(q)$ και $D_n(q) \simeq P\Omega_{2n}(q)$, και ομάδες που σχετίζονται με τις E, F και G τύπου. Αυτές ονομάζονται ομάδες Chevalley.

Αυτές δεν είναι όλες οι απλές ομάδες τύπου Lie: οι υπόλοιπες κατασκευάζονται ως υποομάδες σταθερών σημείων κάτω από συγκεκριμένους αυτομορφισμούς των παραπάνω ομάδων. Αυτές λέγονται twisted ομάδες και μαζί με τις ομάδες Chevalley αποτελούν τις απλές ομάδες τύπου Lie.

Οι 26 σποραδικές ομάδες είναι:

- οι ομάδες Mathieu, M_{11}, M_{12}, M_{22}, M_{23} και M_{24},
- οι ομάδες Janko, J_1, J_2, J_3 και J_4,
- οι ομάδες Conway, Co_1, Co_2 και Co_3,
- οι ομάδες Fischer, Fi_{22}, Fi_{23} και Fi_{24},

- η ομάδα Highman-Sims, HS,
- η ομάδα McLaughlin, McL,
- η ομάδα Held, He,
- η ομάδα Rudvalis, Ru,
- η σποραδική ομάδα Suzuki, Suz,
- η ομάδα O'Nan, $O'N$,
- η ομάδα Harada-Norton, HN,
- η ομάδα Lyons, Ly,
- η ομάδα Thompson, Th,
- η ομάδα Baby Monster, B και
- η ομάδα Fischer-Griess Monster, M.

Η ομάδα M_{11} είναι η μικρότερη σποραδική ομάδα, με τάξη 7920, και η ομάδα M, η μεγαλύτερη, με τάξη

$$808017424794512875886459904961710757005754368000000000$$

Οι πεπερασμένες απλές ομάδες έχουν ακόμη πολλά να μας πουν, ειδικά όσον αφορά τη θεωρία αναπαραστάσεων τους. Η μελέτη τους, όμως, οδεύει προς ένα τέλος.

Παράρτημα Α΄

Συμμετρικές και διεδρικές ομάδες

Παράρτημα Β΄

Οι ομάδες τάξης < 16

Ταξινομούμε -ως προς ισομορφισμό- τις ομάδες που έχουν τάξη μικρότερη του 16.

Τάξη 1: Υπάρχει μια μοναδική ομάδα τάξης 1, η τετριμμένη ομάδα $\{1\}$.

Μπορούμε εύκολα να προσπεράσουμε τις ομάδες που έχουν τάξη πρώτο αριθμό.

Πρόταση Β΄.0.1. *Αν $|G| = p$, όπου p πρώτος αριθμός, τότε $G \simeq C_p$.*

Η παραπάνω πρόταση, ταξινομεί τις ομάδες με $|G| = 2$, 3, 5, 7, 11 και 13. Στη συνέχεια, ταξινομούμε τις ομάδες με τάξη τετράγωνο πρώτου αριθμού. Έχουμε δει ότι αν $|G| = p^2$, τότε η G είναι αβελιανή. Χρησιμοποιώντας τη ταξινόμηση των πεπερασμένων αβελιανών ομάδων, έχουμε:

Τάξη 4: $G \simeq C_4$ ή $C_2 \times C_2$.

Τάξη 9: $G \simeq C_9$ ή $C_3 \times C_3$.

Στη συνέχεια, μελετάμε τη περίπτωση $|G| = pq$, όπου p και q διακεκριμένοι πρώτοι. Έχουμε δείξει ότι:

Πρόταση Β΄.0.2. *Αν $|G| = 2p$, όπου p περιττός πρώτος, τότε*

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

ή

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

Τάξη 6: $G \simeq C_6$ ή D_3.

Τάξη 10: $G \simeq C_{10}$ ή D_5.

Τάξη 14: $G \simeq C_{14}$ ή D_7.

Τάξη 15: $G \simeq C_{15}$.

Έμειναν οι ομάδες τάξης 8 και 12. Ξεκινάμε με τις αβελιανές ομάδες πρώτα.

Τάξη 8: Οι αβελιανές ομάδες τάξης 8 είναι οι C_8, $C_2 \times C_4$ και $C_2 \times C_2 \times C_2$.

Έστω, τώρα, ότι η G είναι μια μη-αβελιανή ομάδα τάξης 8. Τότε, δεν υπάρχει στοιχείο τάξης 8, αλλιώς η G θα ήταν κυκλική και αβελιανή, και υπάρχει στοιχείο που δεν έχει τάξη 2, αλλιώς $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$ για κάθε $g, h \in G$. Έτσι, υπάρχει στοιχείο τάξης 4. Έστω i ένα τέτοιο στοιχείο και $A = \langle i \rangle$. Εφόσον $[G : A] = 2$, η A είναι κανονική στην G. Αν η $G\backslash A$ έχει στοιχείο j τάξης 2, τότε $j^{-1}ij = i^{-1}$. Τελικά, $G \simeq D_4$.

Υπάρχει, τουλάχιστον άλλη μια ομάδα τάξης 8. Αυτή είναι η ομάδα των quaternions, Q.

Έστω η υποομάδα της S_8 που παράγεται από τα

$$I = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$$

και

$$J = (1\ 5\ 3\ 7)(2\ 8\ 4\ 6)$$

Τότε, θεωρούμε την

$$K = IJ = (1\ 8\ 3\ 6)(2\ 7\ 4\ 5)$$

και την

$$Z = I^2 = J^2 = K^2 = (1\ 3)(2\ 4)(5\ 7)(6\ 8)$$

Έτσι, έχουμε την $Q = \langle I, J \rangle = \{\mathrm{id}, I, I^2, I^3, J, IJ, I^2J, I^3J\}$. Η άλγεβρα των quaternions, $\mathbb{H}$, είναι πραγματικός διανυσματικός χώρος διάστασης 4, παραγόμενη από την βάση $\{1, i, j, k\}$ με πολλαπλασιασμό που ικανοποιεί τις σχέσεις

$$i^2 = j^2 = k^2 = ijk = -1$$

Τα quaternions αποτελούν μια γενίκευση των μιγαδικών αριθμών, και ανακαλύφθηκαν από τον William Rowan Hamilton το 1843.

Για την ομάδα Q, έχουμε μια αναπαράσταση μέσω των πινάκων του $M_2(\mathbb{C})$,

$$1_{\mathbb{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

Τότε, $Q \simeq \{\pm 1_{\mathbb{H}}, \pm i, \pm j, \pm k\}$.

Γυρνάμε, στην άλλη περίπτωση όπου το $G\backslash A$ περιέχει μόνο στοιχεία τάξης 4. Έστω $j \in G\backslash A$ και $B = \langle j \rangle$, $|B| = 4$. Τότε, $|A \cap B| = 1$ ή 2. Αν $|A \cap B| = 1$, τότε $|AB| = |A||B|/|A \cap B| = 16$, το οποίο είναι άτοπο γιατί η AB είναι υποομάδα της G. Έτσι, $|A \cap B| = 2$ και $|AB| = 8$. Τότε, όμως, έχουμε $AB = G$ και άρα $AB = BA$. Αν z το μη-τετριμμένο στοιχείο της $A \cap B$, τότε $zA = Az$, δηλαδή η A είναι αβελιανή, και $zB = Bz$, άρα $zAB = ABz$, δηλαδή $zG = Gz$.

Τώρα, το $k = ij \notin A$, αλλιώς $j = i^3ij \in A$, έχει τάξη 4. Παρατηρήστε ότι $G = A \cup Aj$ και ότι γνωρίζουμε τη δομή της A, $A = \langle i \rangle$, άρα η δομή της G θα βρεθεί μόλις εκφράσουμε το ji σαν στοιχείο του $A \cup Aj$. Η G περιέχει στοιχείο τάξης 2, το z, και αυτό είναι το μοναδικό. Έτσι, έχουμε ότι

$$z = i^2 = j^2 = k^2$$

εφόσον τα i, j, k έχουν τάξη 4. Ειδικότερα,

$$k^2 = ijij = j^2$$

άρα

$$ji = i^{-1}j^2j^{-1} = i^3j^2j^3 = i^3j$$

Έτσι, η G είναι

$$G = \{j^m j^n : 0 \leq m \leq 4,\ 0 \leq n \leq 1\}$$

και για να πολλαπλασιάσουμε δύο στοιχεία χρησιμοποιούμε την σχέση $ji = i^3j$, λόγου χάριν,

$$(ij)(i^2j) = i(ji)(ij) = i(i^3j)(ij) = jij = (i^3j)j = i^3i^2 = i$$

Τελικά, η G είναι ισόμορφη με την Q. Το στοιχείο z είναι το $-1_{\mathbb{H}}$, που αντιστοιχεί στο Z. Όπως είδαμε και πριν, μια αναπαράσταση της Q είναι

$$Q = \langle \alpha, \beta | \alpha^4, \alpha^2 = \beta^2, \beta^{-1}\alpha\beta = \alpha^{-1} \rangle$$

Συνοψίζοντας, υπάρχουν πέντε ομάδες τάξης 8:

$$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, D_8, Q$$

Έμεινε μόνο η τάξη 12. Χρησιμοποιούμε μια διαφορετική μέθοδο, από αυτή στις ομάδες τάξης 8, που βασεται στο γεγονός ότι κάθε ομάδα τάξης 8 είναι ένα ημιευθύ γινόμενο. Βρίσκουμε τις διάφορες ομάδες αυτομορφισμών για να δούμε ποιά είναι τα πιθανά ημιευθέα γινόμενα.

Τάξη 12: Οι αβελιανές ομάδες τάξης 12 είναι οι C_{12} και $C_2 \times C_6$.

Έστω G μη-αβελιανή ομάδα τάξης 12. Από τα Θεωρήματα Sylow, $n_2 = 1$ ή 3 και $n_3 = 1$ ή 4. Δεν είναι δυνατόν να ισχύει $n_2 = 3$ και $n_3 = 4$, αφού τότε θα υπήρχαν τουλάχιστον 4 στοιχεία τάξης 2 και 8 στοιχεία τάξης 3 και η μονάδα, που είναι παραπάνω από 12 το πλήθος. Έτσι, υπάρχει ακριβώς μια Sylow 2-υποομάδα ή ακριβώς μια Sylow 3-υποομάδα.

Έστω p ο πρώτος για τον οποίο υπάρχει μοναδική Sylow p-υποομάδα και q ο άλλος πρώτος που διαιρεί το 12. Τότε, η μοναδική Sylow p-υποομάδα είναι κανονική στην G, η τομή της με μια Sylow q-υποομάδα είναι τετριμμένη, και το γινόμενο τους αποτελεί όλη την G. Έτσι, η G είναι ένα ημιευθύ γινόμενο.

Από τη προηγούμενη ταξινόμηση, μια Sylow 2-υποομάδα είναι η C_4 ή $C_2 \times C_2$, και μια Sylow 3-υποομάδα είναι η C_3. Έτσι, για να βρούμε τις ομάδες τάξης 12, πρέπει να βρούμε όλα τα πιθανά ημιευθέα γινόμενα των παραπάνω ομάδων. Προς τούτο, βρίσκουμε τις ομάδες αυτομορφισμών τους. Αυτές είναι οι

$$\mathrm{Aut}(C_3) \simeq C_2$$

$$\mathrm{Aut}(C_4) \simeq C_2$$

και

$$\mathrm{Aut}(C_2 \times C_2) \simeq S_3$$

Χρησιμοποιούμε, πάλι, το γεγονός ότι: αν ψ και ϕ μονομορφισμοί από μια ομάδα G στους αυτομορφισμούς, $\mathrm{Aut}(H)$, μιας άλλης ομάδας H, με ίδια εικόνα, τότε $H \overset{\phi}{\rtimes} G \simeq H \overset{\psi}{\rtimes} G$.

– $C_4 \rtimes C_3$: Δεν υπάρχει μη-τετριμμένος ομομορφισμός από το C_3 στο $\mathrm{Aut}(C_4) \simeq C_2$, καθώς ένας τέτοιος ομομορφισμός θα είχε μη-τετριμμένο πυρήνα, άρα θα ήταν επιμορφισμός -άτοπο. Έτσι, το μοναδικό ημιευθύ γινόμενο αυτής της μορφής είναι ευθύ, το $C_4 \times C_3 \simeq C_{12}$.

– $(C_2 \times C_2) \rtimes C_3$: Εφόσον η $\mathrm{Aut}(C_2 \times C_2) \simeq S_3$ έχει μοναδική υποομάδα τάξης 3, κάθε δύο μη-τετριμμένοι ομομορφισμοί, άρα μονομορφισμοί, από το C_3 στο S_3 έχουν την ίδια εικόνα, άρα επάγουν ίδια ημιευθέα γινόμενα. Τώρα, η A_4 έχει μοναδική Sylow 2-υποομάδα ισόμορφη με την $C_2 \times C_2$, άρα είναι κατάλληλης μορφής. Δηλαδή, $(C_2 \times C_2) \rtimes C_3 \simeq A_4$.

– $C_3 \rtimes (C_2 \times C_2)$: Εφόσον $\mathrm{Aut}(C_3) \simeq C_2$, υπάρχουν τρεις μη-τετριμμένοι ομομορφισμοί από το $C_2 \times C_2$ στο $\mathrm{Aut}(C)3) \simeq C_2$,αλλά και πάλι μας δίνουν ισόμορφα ημιευθέα γινόμενα. Αυτή τη φορά, ο υποψήφιος D_6, μπορούμε να ελεξουμε ότι έχει μοναδική Sylow 3-υποομάδα ισόμορφη με την C_3, άρα $C_3 \rtimes (C_2 \times C_2) \simeq D_6$.

– $C_3 \rtimes C_4$: Υπάρχει ακριβώς ένας μη-τετριμμένος ομομορφισμός από την C_4 στην $\mathrm{Aut}(C_3) \simeq C_2$, η φυσική προβολή στην ομάδα πηλίκο $C_4/\langle x^2 \rangle$. Αυτό το ημιευθύ γινόμενο δεν είναι ισόμορφο με την A_4 ή την D_6 και ολοκληρώνει τη λίστα των ομάδων τάξης 12. Μπορεί να υλοποιηθεί ως η υποομάδα

$$\langle (5\ 6\ 7), (1\ 2\ 3\ 4), (6\ 7) \rangle$$

της S_7.

Έτσι, οι μη-αβελιανές ομάδες τάξης 12 είναι οι A_4, D_{12} και $C_3 \rtimes C_4$.

Τελικά, η πλήρης λίστα τον ομάδων τάξης < 16 είναι:

1	$\{1\}$
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	C_6, D_3
7	C_7
8	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$, D_8, Q
9	C_9, $C_3 \times C_3$
10	C_{10}, D_5
11	C_{11}
12	C_{12}, $C_2 \times C_6$, A_4, D_6, $C_3 \rtimes C_4$
13	C_{13}
14	C_{14}, D_7
15	C_{15}

Το να συνεχίσουμε με αυτό τον τρόπο δεν είναι πρακτικό. Για ένα άνω φράγμα του πλήθους των μη-ισόμορφων ομάδων μιας δοθείσας τάξης, μπορούμε να επικαλεστούμε το γεγονός ότι μη-ισόμορφες ομάδες έχουν διαφορετικούς πίνακες πολλαπλασιασμού. Έτσι, ο αριθμός των διαφορετικών $n \times n$ πινάκων με n στοιχεία είναι ένα άνω φράγμα, παρότι λίγοι πίνακες θα περιγράφουν οντως ομάδες. Δυστυχώς για τάξη n, το φράγμα αυτό είναι n^{n^2}, το οποίο,

παρότι πεπερασμένο, είναι πολύ μεγάλο. Για $n = 8$, έχουμε $8^{64} = 6,2 \times 10^{57}$ ενώ το πλήθος των μη-ισόμορφων ομάδων τάξης οχτώ είναι 5.

Έχει δειχθεί ότι:

- Υπάρχουν 49.487.365.422 μη-ισόμορφες ομάδες τάξης $2^{10} = 1024$.
- Υπάρχουν 423.164.062 μη-ισόμορφες ομάδες τάξης το πολύ 2000, και όχι 1024. Η πλειοψηφία αυτών έχουν τάξη 1536.

Μέρος Ι

Λύσεις Ασκήσεων

Βασικές Έννοιες

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.

   Λύση. Γνωρίζουμε ότι

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

   και

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

   Συνεπώς, $[G : H \cap K] \geq$εκπ(m, n).

   Αφού $[G : K][K : H \cap K] = [G : H \cap K] = [G : H][H : H \cap K]$, έχουμε ότι

   $$[G : K] \Big| [G : H][H : H \cap K] \xrightarrow{(m,n)=1} [G : K] \Big| [H : H \cap K] \Rightarrow [G : K] \leq [H : H \cap K]$$

   Έστω

   $$\phi : H/H \cap K \to G/K, \quad h(H \cap K) \mapsto hK$$

   Η ϕ είναι καλά ορισμένη: Αν $h_1(H \cap K) = h_2(H \cap K)$, τότε $h_2^{-1}h_1 \in H \cap K \Rightarrow h_2^{-1}h_1 \in K \Rightarrow h_1K = h_2K$.

   1-1: Αν $h_1K = h_2K$, τότε $h_2^{-1}h_1 \in K$ και $h_2^{-1}h_1 \in H \Rightarrow h_2^{-1}h_1 \in H \cap K \Rightarrow h_1(H \cap K) = h_2(H \cap K)$. Συνεπώς, $[H : H \cap K] \leq [G : K]$, άρα

   $$[G : H \cap K] = [G : H][H : H \cap K] = [G : H][G : K] = mn$$

   □

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 $[G : \bigcap_{i=1}^{n} H_i] \leq \prod_{i=1}^{n} [G : H_i]$.

   Λύση. Αν $n = 2$, θα δείξουμε ότι $[G : H_1 \cap H_2] \leq [G : H_1][G : H_2]$. Εφόσον $[G : H_1 \cap H_2] = [G : H_1][H_1 : H_1 \cap H_2]$ αρκεί να δείξουμε ότι $[H_1 : H_1 \cap H_2] \leq [G : H_2]$. Όπως και στην Άσκηση 1 ο $\phi : h(H_1 \cap H_2) \mapsto hH_2$ είναι 1-1, άρα $[H_1 : H_1 \cap H_2] \leq [G : H_2]$.

   Το ζητούμενο έπεται με επαγωγή στο n. □

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

Λύση. Έστω $K = \langle k \rangle$, για κάποιο $k \in K$ και $H \leq K$. Τότε, υπάρχει $h \in \mathbb{N}$ ώστε $H = \langle k^h \rangle$. Από την υπόθεση, $K \lhd G$, άρα $gkg^{-1} \in K \Rightarrow gkg^{-1} = k^\lambda$, για κάποιο $\lambda \in \mathbb{N}$.

Έστω, τώρα, $x \in H$. Το x γράφεται $x = (k^h)^d$, για κάποιο $d \in \mathbb{N}$. Τότε,

$$gxg^{-1} = g(k^h)^d g^{-1} = (gkg^{-1})^{hd} = (k^\lambda)^{hd} = (k^h)^{\lambda d} \in H$$

Δηλαδή, $H \lhd G$. □

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 $g \in N$.

Λύση. Αφού $|G/N| = n$, έχουμε ότι $g^n N = N$ και άρα $g^n \in N$. Επιπλέον, $(m, n) = 1$, άρα υπάρχουν $x, y \in \mathbb{Z}$ με $1 = mx + ny$. Τότε,

$$g = g^1 = g^{mx+ny} = g^{mx} g^{ny} = (g^m)^x (g^n)^y \in N$$

□

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 $Z(G/K)$.

   Λύση. (i) Η $Z(G)$ είναι προφανώς αβελιανή. Έστω $a, b \in Z(G), g \in G$. Τότε,

   $$(ab)g = (ag)b = g(ab) \Rightarrow ab \in Z(G)$$

   και

   $$a^{-1}g = (g^{-1}a)^{-1} = (ag^{-1})^{-1} = ga^{-1} \Rightarrow a^{-1} \in Z(G)$$

   Δηλαδή $Z(G) \leq G$.

   Τέλος, $gag^{-1} = agg^{-1} = a \in Z(G)$, άρα $Z(G) \lhd G$.

   (ii) Έστω $H \leq Z(G)$. Τότε $H \leq G$ και αν $g \in G, h \in h$, έχουμε $ghg^{-1} = hgg^{-1} = h \in H \Rightarrow H \lhd G$.

   (iii) Έστω ότι η $G/Z(G)$ ειναι κυκλική. Τότε $G/Z(G) = \langle aZ(G) \rangle$, για κάποιο $a \in G$. Έστω $g_1, g_2 \in G$. Τότε υπάρχουν $k_1, k_2 \in \mathbb{Z} : g_1 Z(G) = a^{k_1} Z(G), g_2 Z(G) = a^{k_2} Z(G)$. Άρα, υπάρχουν $z_1, z_2 \in Z(G) : g_1 = a^{k_1} z_1, g_2 = a^{k_2} z_2$.

   Τότε

   $$g_1 g_2 = a^{k_1} z_1 a^{k_2} z_2 = a^{k_1} a^{k_2} z_1 z_2 = a^{k_2} a^{k_1} z_1 z_2 = a^{k_2} z_2 a^{k_1} z_1 = g_2 g_1$$

   Δηλαδή η G είναι αβελιανή.

(iv) Έχουμε ότι $K = \{1, k\}, k \in G$ και $K \lhd G$. Αν $g \in G$, τότε $gkg^{-1} \in K$, άρα $gkg^{-1} = k \Rightarrow gk = kg \Rightarrow K \leq Z(G)$.

(v) $1_G \in H \Rightarrow 1_{G_1} \in \phi(H) \Rightarrow \phi(H) \neq \emptyset$. Έστω $a, b \in \phi(H)$. Η ϕ είναι επί, άρα υπάρχουν $h_1, h_2 \in H$ ώστε $a = \phi(h_1)$ και $b = \phi(h_2)$. Τότε,

$$ab^{-1} = \phi(h_1)\phi(h_2^{-1}) = \phi(h_1 h_2^{-1}) \in \phi(H)$$

και

$$ab = \phi(h_1)\phi(h_2) = \phi(h_1 h_2) = \phi(h_2 h_1) = \phi(h_2)\phi(h_1) = ba$$

Τελικά, $\phi(H) \leq Z(G_1)$.

(vi) Έστω $\pi : G \to G/K$ ο φυσικός επιμορφισμός. Παίρνουμε τον περιορισμό αυτού, $\pi|_{Z(G)}$, στο $Z(G)$. Έχουμε ότι $Z(G) \leq G \Rightarrow \pi(Z(G)) = \operatorname{im} \pi|_{Z(G)} \leq Z(G/K)$ και $\ker \pi|_{Z(G)} = Z(G) \cap K$. Συνεπώς,

$$\frac{Z(G)}{\ker \pi|_{Z(G)}} = \frac{Z(G)}{Z(G) \cap K} \simeq \pi(Z(G)) \leq Z(G/K)$$

□

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.

Λύση. Παρατηρούμε αρχικά ότι $[g, h]^{-1} = (g^{-1}h^{-1}gh)^{-1} = h^{-1}g^{-1}hg = [h, g]$, δηλαδή το αντίστροφο ενός μεταθέτη είναι επίσης μεταθέτης.
Συνεπώς, κάθε στοιχείο της G' γράφεται ως γινόμενο μεταθετών.

(i) Αρκεί να δείξουμε ότι $g[x, y]g^{-1} \in G'$.
Πράγματι, $g[x.y]g^{-1} = \tau_g([x, y]) = [\tau_g(x), \tau_g(y)] = [gxg^{-1}, gyg^{-1}] \in G'$.
Γενικά, αν $h \in G'$, τότε $h = [x_1, y_1][x_2, y_2] \cdots [x_k, y_k]$ και
$ghg^{-1} = g[x_1, y_1] \cdots [x_k, y_k]g^{-1} = g[x_1, y_1]g^{-1}g[x_1, y_2]g^{-1} \cdots g[x_k, y_k]g^{-1} \in G'$.

(ii) Έστω $H \leq G$ με $H \supseteq G'$ και $h \in H, g \in G$. Τότε $ghg^{-1} = ghg^{-1}h^{-1}h = [g^{-1}, h^{-1}]h \in H$ και άρα $H \lhd G$.

(iii) Η G/H είναι αβελιανή $\Leftrightarrow g_1Hg_2H = g_2Hg_1H \quad \forall g_1, g_2 \in G \Leftrightarrow g_1g_2H = g_2g_1H$
$\forall g_1, g_2 \in G \Leftrightarrow g_1^{-1}g_2^{-1}g_1g_2 \in H \quad \forall g_1, g_2 \in G \Leftrightarrow [g_1, g_2] \in H \quad \forall g_1, g_2 \in G \Leftrightarrow G' \subseteq H$.

□

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

Λύση. (i) Έστω $a, b \in G$. Τότε,

$$a^{-1}b^{-1} = \phi(a)\phi(b) = \phi(ab) = (ab)^{-1} = b^{-1}a^{-1} \Rightarrow ab = ba$$

Άρα, η G είναι αβελιανή.
Αντίστροφα, αν η G είναι αβελιανή,

$$\phi(ab) = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1} = \phi(a)\phi(b)$$

Δηλαδή, ο ϕ είναι ομομορφισμός.

(ii) Έστω

$$K = \{a^{-1}\theta(a) : a \in G\}$$

Προφανώς $K \subseteq G$. Έστω, τώρα, $a, b \in G$ με $a^{-1}\theta(a) = b^{-1}\theta(b)$. Τότε $\theta(a)\theta(b^{-1}) = ab^{-1} \Rightarrow \theta(ab^{-1}) = ab^{-1} \Rightarrow ab^{-1} = 1 \Rightarrow a = b$, δηλαδή $|K| = |G|$.

Συνεπώς, $K = G$.

Έστω $g \in G$. Γνωρίζουμε ότι υπάρχει $a \in G$ με $g = a^{-1}\theta(a)$ και άρα $g^{-1} = \theta(a^{-1})a$. Τότε

$$\theta(g) = \theta(a^{-1})\theta^2(a) = \theta(a^{-1})a = g^{-1}$$

□

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 $|G^n| = [G : G_n]$.

Λύση. Έστω $f : G \to G, g \mapsto g^n$. Από την υπόθεση, $f(ab) = (ab)^n = a^n b^n = f(a)f(b)$, άρα ο f είναι ομομορφισμός. Προφανώς, $\ker f = G_n \lhd G$, $\operatorname{im} f = G^n \leq G$ και

$$G/G_n \simeq G^n \Rightarrow |G^n| = [G : G_n]$$

Τέλος, αν $a \in G^n, g \in G$, τότε $a = h^n$, για κάποιο $h \in G$ και

$$gag^{-1} = gh^n g^{-1} = (ghg^{-1})^n = g^n h^n (g^{-1})^n \in G^n$$

άρα $G^n \lhd G$. □

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 $|K|$.

Λύση. Έστω $H \leq G$ με $|H| = |K|$. Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/K$ και μελετάμε την εικόνα $\pi(H)$.

- $\pi(H) \leq G/K \Rightarrow |\pi(H)| \Big| |G/K| = [G : K]$

- $|\pi(H)|\Big||H| = |K|$, γιατί αν $\phi : G \to G'$ ομομορφισμός, τότε από το 1ο Θεώρημα Ισομορφισμών $G/\ker f \simeq \operatorname{im} f = \phi(G) \Rightarrow |G| = |\ker f| \cdot |\phi(G)|$.

Άρα το $|\pi(H)|$ είναι κοινός διαιρέτης των $[G : K]$ και $|K|$. Αφού $([G : K], |K|) = 1$ έπεται ότι $|\pi(H)| = 1$ και συνεπώς $\pi(H) = 1_{G/K}$. Αυτό σημαίνει ότι $H \subseteq \ker \pi = K$ και άρα $H = K$ αφού $|H| = |K|$. □

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.

Λύση. (i) d_1 Αν $g = h$, τότε $d_S(g, h) = \|g^{-1}g\|_S = \|1_G\|_S = 0$. Αντίστροφα, αν $d_S(g, h) = 0$, τότε $\|g^{-1}h\|_S = 0 \Rightarrow g^{-1}h = 1_G \Rightarrow h = g$.

d_2 Έστω $d_S(g, h) = n$. Τότε $d_S(h, g) \leq n$. Αν $d_S(h, g) = m < n$, τότε $h^{-1}g = s_{i_1}^{\varepsilon_1} \cdots s_{i_m}^{\varepsilon_m} \Rightarrow g^{-1}h = s_{i_1}^{-\varepsilon_1} \cdots s_{i_m}^{-\varepsilon_m} \Rightarrow n = d_S(g, h) < m$ -άτοπο.

d_3 Αν $\|g^{-1}k\|_S = n, \|k^{-1}h\|_S = m$, τότε $g^{-1}k = s_{i_1}^{\varepsilon_1} \cdots s_{i_n}^{\varepsilon_n}$ και $k^{-1}h = s_{j_1}^{\varepsilon_1} \cdots s_{j_m}^{\varepsilon_m}$, και άρα $g^{-1}h = g^{-1}kk^{-1}h = s_{i_1}^{\varepsilon_1} \cdots s_{i_n}^{\varepsilon_n} s_{j_1}^{\varepsilon_1} \cdots s_{j_m}^{\varepsilon_m}$. Συνεπώς, $\|g^{-1}h\|_S \geq n+m = \|g^{-1}k\|_S + \|k^{-1}h\|_S$.

(ii) Ορίζουμε $\psi : G \hookrightarrow \operatorname{Isom}(G)$, με $g \mapsto \phi_g$, όπου $\phi_g(x) = gx \quad \forall x \in G$. Η $\phi(G) \in \operatorname{Sym}(G)$ και $\|\phi_g^{-1}(x)\phi_g(y)\|_S = \|(gx)^{-1}gy\|_S = \|x^{-1}g^{-1}gy\|_S = \|x^{-1}y\|_S$ για κάθε $x, y \in G$

□

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

Λύση. Έστω $hk \in HK, mk_1 \in MK$. Τότε

$$\begin{aligned} & hkmk_1(hk)^{-1} \\ &= hkmk_1k^{-1}h^{-1} \\ &= hm\underbrace{m^{-1}km}_{\in K}\underbrace{k_1k^{-1}}_{\in K}h^{-1} \\ &= \underbrace{hmh^{-1}h}_{\in M}\underbrace{m^{-1}kmk_1k^{-1}h^{-1}}_{\in K} \in MK \end{aligned}$$

□

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

Λύση. (i) Έχουμε ότι $\phi|_H \in \mathrm{Aut}(H)$, άρα $|H| = |\phi(H)|$ και $\phi(H) \subseteq H$, δηλαδή $\phi(H) = H$.

(ii) Έστω $g \in G$. Αφού $\tau_g \in \mathrm{Aut}(G)$, $\tau_g(H) = H$, άρα $H \lhd G$.

(iii) Αν $\phi \in \mathrm{Aut}(G)$, τότε ο $\sigma \equiv \phi|_N \in \mathrm{Aut}(N)$. Άρα $\phi(H) = \phi|_N(H) = \sigma(H) = H$. Συνεπώς, $H \trianglelefteq G$.

(iv) Έχουμε $\tau_g(N) = \tau_g|_K(N) = N$, άρα $N \lhd G$.

(v) Αν $G = \langle g \rangle, K = \langle g^k \rangle \leq G$ και $\phi \in \mathrm{Aut}(G)$, τότε $\phi(K) = \langle \phi(g)^k \rangle$ και $|\phi(g)^k| \Big| |\phi(g)| \Rightarrow \phi(K) \leq K$. Τελικά, $K \trianglelefteq G$.

(vi) Έστω ϕ αυτομορφισμός. Τότε, ο ϕ είναι ειδικότερα και επιμορφισμός και $Z(G) \leq Z(G)$, άρα από την Άσκηση $5(v)$ έχουμε ότι $\phi(Z(G)) \leq Z(G)$. Δηλαδή, $Z(G) \trianglelefteq G$.

Έστω ϕ αυτομορφισμός. Τότε,

$$\phi([x,y]) = \phi(x^{-1}y^{-1}xy) = \phi(x)^{-1}\phi(y)^{-1}\phi(x)\phi(y) = [\phi(x), \phi(y)] \in G'$$

Άρα $\phi(G') \leq G' \Rightarrow G' \trianglelefteq G$.

(vii) Έστω H ομάδα με $|H| > 1$ και $G = H \times H$. Ορίζουμε $K = H \times \{1\} \lhd G$. Η K δεν είναι χαρακτηριστική στην G. Πράγματι, ο $\phi : G \to G$, με $(h_1, h_2) \mapsto (h_2, h_1)$ είναι αυτομορφισμός, αλλά $\phi(K) \cap K^c \neq \emptyset$.

□

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.]

Δράσεις Ομάδων

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.]

   Λύση. Έστω $C_n = \langle g \rangle$. Γνωρίζουμε ότι οι γεννήτορες της C_n είναι $\phi(n)$ το πλήθος, όπου ϕ η συνάρτηση Euler.

   Έστω

   $$\psi : \mathrm{Aut}(C_n) \to (\mathbb{Z}/n\mathbb{Z})^*$$

   $$\mathrm{Aut}(C_n) \ni \alpha \mapsto \alpha(g) \in (\mathbb{Z}/n\mathbb{Z})^*$$

   Έχουμε ότι $C_n = \langle \alpha(g) \rangle$, και έτσι κάθε $\alpha \in \mathrm{Aut}(C_n)$ καθορίζεται πλήρως από το $\alpha(g)$. Η ψ είναι προφανώς ομομορφισμός και έτσι

   $$\psi : \mathrm{Aut}(C_n) \xrightarrow{\simeq} (\mathbb{Z}/n\mathbb{Z})^*$$

   □

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.]

   Λύση. Έστω $\phi : G \to G$ επιμορφισμός και $H \leq G$ με $[G : H] = n < \infty$. Εφόσον η G είναι πεπερασμένα παραγόμενη, το πλήθος των υποομάδων της G δείκτη n είναι πεπερασμένο.

   Έστω $H_1, H_2, \ldots, H_\nu$ οι υποομάδες της G δείκτη n. Αν $K = \ker \phi$, τότε $G/K \simeq G$ και άρα η G/K έχει και αυτή ακριβώς ν υποομάδες δείκτη n.

   Από το θεώρημα της Αντιστοιχίας, γνωρίζουμε ότι οι παραπάνω ν υποομάδες της G/K θα είναι οι $M_1/K, M_2/K, \ldots, M_\nu/K$ για κάποιες $M_i \leq G$ με $M_i \supseteq K$ και επιπλέον

   $$[G : M_i] = [G/K : M_i/K] = \nu$$

   Άρα οι $M_1, M_2, \ldots, M_\nu$ αποτελούν μια αναδιάταξη των $H_1, H_2, \ldots, H_\nu$. Συνεπώς, $H_i \supseteq K$ για κάθε $i = 1, 2, \ldots, \nu$ και ιδαιτέρως $H \supseteq K$.

Άρα κάθε υποομάδα της G πεπερασμένου δείκτη περιέχεται στον πυρήνα της ϕ. Έτσι

$$K \subseteq \bigcap_{\substack{H \leq G \\ [G:H]<\infty}} H = \{1\}$$

Συνεπώς $K = \{1\}$ και άρα η ϕ είναι ισομορφισμός. □

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.

   Λύση. (i) Έστω $A = \{(g, x) \in G \times X : gx = x\}$ και n το πλήθος των των τροχιών της δράσης.

   Σταθεροποιούμε $g \in G$ και έχουμε ότι $gx = x \Leftrightarrow x \in \mathrm{Fix}(g)$. Άρα $|A| = \sum_{g \in G} |\,\mathrm{Fix}(g)|$.

   Τώρα σταθεροποιούμε $x \in X$ και έχουμε $gx = x \Leftrightarrow g \in G_x$. Συνεπώς $|A| = \sum_{x \in X} |G_x|$.

   Αν τα x_1, x_2 είναι στην ίδια τροχιά, τότε οι αντίστοιχες σταθεροποιούσες G_{x_1}, G_{x_2} είναι συζυγείς, άρα ισοπληθικές, $|G_{x_1}| = |G_{x_2}|$. Αν $X = \mathcal{O}(x_1) \sqcup \mathcal{O}(x_2) \sqcup \ldots \sqcup \mathcal{O}(x_n)$, τότε $|A| = \sum_{x \in X} |G_x| = \sum_{i=1}^{n} |\mathcal{O}(x_i)| \cdot |G_{x_i}| = \sum_{i=1}^{n} |G| = n|G|$. Τελικά, $n|G| = \sum_{g \in G} |\,\mathrm{Fix}(g)|$ και άρα $n = \frac{1}{|G|} \sum_{g \in G} |\,\mathrm{Fix}(g)|$.

   (ii) Αφού η δράση είναι μεταβατική $n = 1$ και $|G| = \sum_{g \in G} |\,\mathrm{Fix}(g)| = |\,\mathrm{Fix}(1_G)| + \sum_{g \neq 1_G} |\,\mathrm{Fix}(g)| = |X| + \sum_{g \neq 1_G} |\,\mathrm{Fix}(g)|$.

   Αν υποθέσουμε ότι $\mathrm{Fix}(g) \neq \emptyset$ για κάθε $g \neq 1_G$, τότε $|G| \geq |X| + |G| - 1 \Leftrightarrow 1 \geq |X|$ το οποίο είναι άτοπο. Άρα $\exists g \in G : \mathrm{Fix}(g) \neq \emptyset$.

   □

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 $\bigcap_{g \in G} \mathrm{Fix}(g) \neq \emptyset$.

   Λύση. Έστω $x \in X$. Γνωρίζουμε ότι $|\mathcal{O}(x)| \Big| |G| = p^n$, άρα $|\mathcal{O}(x)| = 1$ ή p^k για κάποιο $1 \leq k \leq n$. Έστω ότι δεν υπάρχει $x \in X$ με $|\mathcal{O}(x)| = 1$.

   Τότε $p \Big| |\mathcal{O}(x)|$ για κάθε $x \in X$ και έτσι $p \Big| \sum_{x \in X} |\mathcal{O}(x)| = |X|$ -άτοπο. Υπάρχει, λοιπόν, $x \in X$ με $|\mathcal{O}(x)| = 1$, άρα $\mathcal{O}(x) = \{x\}$, δηλαδή $g \cdot x = x$ για κάθε $g \in G$. Τελικά, $x \in \bigcap_{g \in G} \mathrm{Fix}(g)$.

   □

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

Λύση. Θεωρούμε την δράση της H στα σύμπλοκα G/H. Έχουμε ότι $|G/H| = p$ και αν $\mathcal{O}_i$ είναι μια τροχιά της δράσης, τότε $|\mathcal{O}_i| \leq |G/H| = p$. Επίσης, $|\mathcal{O}_i| \Big| |H| \Big| |G|$. Συνεπώς κάθε πρώτος διαιρέτης q του $|\mathcal{O}_i|$ είναι διαιρέτης και του $|G|$ και έτσι $q = 1$ ή $q \geq p$ από την υπόθεση. Όμως $|\mathcal{O}_i| \leq p$. Έπεται, λοιπόν, ότι κάθε τροχιά έχει 1 ή p στοιχεία. Επιπλέον, ή όλες οι τροχιές είναι μονοσύνολα ή υπάρχει μόνο μια με p στοιχεία, αφού $|G/H| = p$.

Παρατηρούμε ότι $\mathcal{O}(H) = \{H\}$, δηλαδή η τροχιά του συμπλόκου H είναι μονοσύνολο. Άρα, από τα παραπάνω, κάθε τροχιά είναι μονοσύνολο. Δηλαδή $\mathcal{O}(gH) = \{gH\}$ το οποίο σημαίνει ότι $hgH = gH$ για κάθε $g \in G, h \in H$. Ισοδύναμα $g^{-1}hg \in H$ για κάθε $g \in G, h \in H$ και έτσι $H \lhd G$. □

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.]

   Λύση. Χρησιμοποιούμε επαγωγή επί του n.

   Γνωρίζουμε ότι $Z(G) \neq 1$. Έτσι $|Z(G)| = p^k, k > 0$.

   Αν $m \leq k$, τότε η $Z(G)$ έχει υποομάδα H τάξεως p^m, η οποία είναι κανονική στην G γιατί $H \subseteq Z(G)$.

   Αν $m > k$, τότε $|G/Z(G)| = p^{n-k}$. Από την επαγωγική υπόθεση, η ομάδα $G/Z(G)$ έχει κανονική υποομάδα τάξεως p^{m-k}. Από το Θεώρημα της Αντιστοιχίας, η παραπάνω υποομάδα θα έχει τη μορφή $H/Z(G)$, όπου $Z(G) \subseteq H \lhd G$. Έτσι $H \lhd G$ και $|H| = |H/Z(G)| \cdot |Z(G)| = p^{m-k}p^k = p^m$. □

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).

   Λύση. Έστω $H \subseteq A_5$ με $[A_5 : H] = n > 1$. Θεωρούμε την δράση της A_5 στα σύμπλοκα της H και την αντίστοιχη αναπαράσταση $\rho : A_5 \to S_n$. Η A_5 είναι απλή, άρα $\ker \rho = 1$.

   Τότε $A_5 \hookrightarrow S_n$, δηλαδή η A_5 εμφυτεύεται στην S_n και $|A_5| \Big| n! \Rightarrow 3 \cdot 4 \cdot 5 | n! \Rightarrow n > 4$.

   Τώρα, αν $|H| = 15$, έχουμε ότι $[A_5 : H] = \frac{60}{15} = 4$ -άτοπο. Όμοια για $|H| = 20$ ή 30. □

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

   Λύση. Θεωρούμε την δράση της G στα αριστερά σύμπλοκα της K, G/K, και τον περιορισμό αυτής στην υποομάδα H. Έχουμε $H \rightsquigarrow G/K, h \cdot gK = hgK$.

   Έστω $\mathcal{O}(K)$ η τροχιά του K. Τότε $\mathcal{O}(K) = \{h_1K, h_2K, \ldots, h_\nu K\}$, όπου $h_i \in H, i = 1, 2, \ldots, \nu$. Γνωρίζουμε ότι $\nu = |\mathcal{O}(K)| = [H : H \cap K]$, μιας και $\mathrm{Stab}_H(K) = H \cap K$.

   Από την άλλη, $HK = \mathcal{O}(K)$ και $|HK| = \sum_{i=1}^{\nu} |h_iK| = \nu|K| = \frac{|H|}{|H \cap K|}|K|$. Τελικά,

   $|HK| \cdot |H \cap K| = |H| \cdot |K|$. □

9. 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 $\mathrm{Aut}(H)$.

Λύση. $1 \in C_G(H)$ άρα $C_G(H) \neq \emptyset$. Έστω $g_1, g_2 \in C_G(H), h \in H$. Τότε

$$g_1(g_2h) = (g_1h)g_2 = hg_1g_2$$

άρα $g_1g_2 \in C_G(H)$ και

$$g_1^{-1}h = (h^{-1}g_1)^{-1} = (g_1h^{-1})^{-1} = hg_1^{-1} \Rightarrow g_1^{-1} \in C_G(H)$$

Προφανώς, $C_G(H) \subseteq N_G(H)$, και έτσι $C_G(H) \lhd N_G(H)$.

Ορίζουμε

$$\phi : N_G(H) \to \mathrm{Aut}(H)$$

$$N_G(H) \ni g \mapsto \tau_g \in \mathrm{Aut}(H)$$

με $\tau_g(h) = ghg^{-1}$ για κάθε $h \in H$. Ο πυρήνας της ϕ είναι η $C_G(H)$. Πράγματι, $x \in \ker\phi \Leftrightarrow \tau_x(h) = 1 \quad \forall h \in H \Leftrightarrow xhx^{-1} = h \quad \forall h \in H \Leftrightarrow x \in C_G(H)$.

Συνεπώς,

$$N_G(H)/C_G(H) \simeq \phi(N_G(H)) \leq \mathrm{Aut}(H)$$

□

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

Λύση. Θεωρούμε την δράση της G στην υποομάδα $H = X$ με συζυγία, δηλαδή $g * h = ghg^{-1}$. Η δράση είναι καλά ορισμένη, γιατί $H \lhd G$. Έχουμε ότι $\mathcal{O}(h) = Cl_G(h) \subseteq H$ για κάθε $h \in H$.

Μια τροχία $\mathcal{O}(h)$ είναι μονοσύνολο ανν $ghg^{-1} = h$ για κάθε $g \in G$ ανν $hg = gh$ για κάθε $g \in G$ ανν $h \in Z(G) \cap H$. Άρα το X είναι η ξένη ένωση τροχιών που είναι μονοσύνολα και τροχιών που δεν είναι μονοσύνολα, και άρα $|H| = |H \cap Z(G)| + \sum_{h:\mathcal{O}(h)\supset\{h\}} |Cl_G(h)|$.

Αν μια τροχιά $Cl_G(h)$ δεν είναι μονοσύνολο $p \Big| |Cl_G(h)|$. Έτσι $p \Big| \sum_{h:\mathcal{O}(h)\supset\{h\}} |Cl_G(h)|, p \Big| |H|$ και άρα $p \Big| |H \cap Z(G)|$. Τελικά $|H \cap Z(G)| \geq p$ και ιδιαιτέρως $H \cap Z(G) \neq 1$. □

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

Λύση. Γνωρίζουμε ότι $[G : N_G(H)]$ είναι το πλήθος των διακεκριμένων συζυγών της H και $|gHg^{-1}| = |H|$. Τότε,

$$\Big| \bigcup_{g\in G} gHg^{-1} \Big| - 1 = \Big| \bigcup_{g\in G} (gHg^{-1} \backslash \{1\}) \Big| \leq [G : N_G(H)](|H| - 1)$$

Όμως $[G : N_G(H)] \leq [G : H]$, άρα

$$\Big| \bigcup_{g\in G} (gHg^{-1} \backslash \{1\}) \Big| \leq [G : H](|H| - 1) = |G| - [G : H]$$

και τελικά

$$\Big|\bigcup_{g\in G} gHg^{-1}\Big| \leq 1 + |G| - [G:H]$$

□

12. (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.

Λύση. (i) Έστω ότι $G = \bigcup_{g\in G} gHg^{-1}$. Τότε $|G| = \Big|\bigcup_{g\in G} gHg^{-1}\Big|$ και από την Άσκηση 11

$$[G:H] \leq 1 \Rightarrow [G:H] = 1 \Rightarrow G = H$$

-άτοπο. Άρα υπάρχει στοιχείο της G το οποίο δεν περιέχεται στην ένωση των συζυγών της H.

(ii) Έστω M μεγιστική υποομάδα της G. Από το ερώτημα (i) υπάρχει $a \in G \setminus \bigcup_{g\in G} gMg^{-1}$.

Θα δείξουμε ότι $G = \langle a\rangle$. Έστω ότι $\langle a\rangle < G$. Τότε υπάρχει μεγιστική υποομάδα K με $\langle a\rangle < K < G$. Όμως $K = gMg^{-1}$, για κάποιο $g \in G$ και $a \notin \bigcup_{g\in G} gMg^{-1}$ -άτοπο. Άρα $G = \langle a\rangle$.

□

13. 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.]

Λύση. Έστω $N = \mathrm{Core}(H) \lhd G$. Γνωρίζουμε ότι $|G/N| < \infty$. Συνεπώς, από την Άσκηση $12(i)$

$$G/N \neq \bigcup_{g\in G} g(H/N)g^{-1}$$

Άρα, υπάρχει xN τέτοιο ώστε $xN \notin g(H/N)g^{-1}$, $\forall g \in G$. Από το Θεώρημα της Αντιστοιχίας $x \notin gHg^{-1} \quad \forall g \in G$. □

14. 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]

Λύση. (i) Έστω $a \in G$. Ορίζουμε

$$\phi : \mathrm{Cl}_G(a) \to G'$$

$$g^{-1}ag \mapsto [a, g] = a^{-1}g^{-1}ag$$

Θα δείξουμε ότι η ϕ είναι 1-1 : Έστω $a^{-1}g^{-1}ag = a^{-1}g'^{-1}ag'$. Τότε $g^{-1}ag = g'^{-1}ag'$. Άρα $|G'| \geq |\,\mathrm{Cl}_G(a)| \Rightarrow \dfrac{|G|}{|\,\mathrm{Cl}_G(a)|} \geq \dfrac{|G|}{|G'|} \Rightarrow |C_G(a)| \geq |G/G'|$.

(ii) Έστω $Z(G) = 1$. Κάθε κλάση συζυγίας έχει μήκος μεγαλύτερο του p_0. Τότε, από την εξίσωση των κλάσεων,

$$1 + (r-1)p_0 \leq |G|$$

Αλλά $p_o \Big| |G| \Rightarrow rp_0 \Big| |G| \Rightarrow rp_0 \leq |G|$.

(iii) Αφού η G δεν είναι αβελιανή, έχουμε ότι $|Z(G)| \leq \frac{|G|}{2}$. Ας υποθέσουμε ότι $|Z(G)| = \frac{|G|}{2}$. Τότε η $G/Z(G)$ έχει τάξη 2, άρα είναι κυκλική. Συνεπώς η G είναι αβελιανή -άτοπο. Τότε $r - |Z(G)| \geq 1$. Αν $r - |Z(G)| = 1$, υπάρχει μοναδική κλάση συζυγίας με μήκος μεγαλύτερο του 1. Άρα η τροχιά αυτή έχει μήκος $> \frac{|G|}{2}$. Τότε, όμως, από την εξίσωση των κλάσεων παίρνουμε ότι η αντίστοιχη κανονικοποιούσα έχει τάξη ανάμεσα από το 1 και το 2.

(iv) Η $Z(G)$ είναι υποομάδα της G και $|G| = p^3$. Άρα $|Z(G)| = 1, p, p^2$ ή p^3. Αφού η G είναι p-ομάδα, το κέντρο είναι μη τετριμμένο. Επιπλέον, αν $|Z(G)| = p^2$ τότε $|G/Z(G)| = p$ και έτσι η $G/Z(G)$ είναι κυκλική, άρα η G είναι αβελιανή. Προφανώς, $|Z(G)| \neq p^3$. Έτσι $|Z(G)| = p$. Τότε $|G/Z(G)| = p^2$ και η $G/Z(G)$ είναι αβελιανή, άρα $G' \subseteq Z(G)$. Για τον αντίστροφο εγκλεισμό, γνωρίζουμε ότι $G' \neq 1$ γιατί η G δεν είναι αβελιανή, άρα $|G'| \geq p$. Τελικά $G' = Z(G)$.

Αν, τώρα, υπάρχει $g \in G$ με $|\,\mathrm{Cl}_G(g)| = p^2$, τότε $|C_G(g)| = p$ και άρα

$$|C_G(g)| = p > p^2 = |G/G'|$$

-άτοπο. Αναγκαστικά, λοιπόν, υπάρχουν $|Z(G)| = p$ κλάσεις συζυγίας τάξης 1 και έστω m το πλήθος κλάσεις συζυγίας τάξης p. Τότε, από την εξίσωση των κλάσεων

$$p^3 = p + mp$$

Τότε $m = p^2 - 1$ και $r = p^2 + p - 1$.

□

15. (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 των κεντροποιουσών 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.

Λύση. (i) Για $r = 1$ η μόνη λύση είναι η $n_1 = 1$. Έστω, τώρα, $r \in \mathbb{N}$ και $n_1 \leq n_2 \leq \ldots \leq n_r$ μια λύση της εξίσωσης.

Πρέπει $n_1 \leq r$, γιατί διαφορετικά $\frac{1}{n_i} > \frac{1}{r}$ και άρα $\sum_{i=1}^{r} \frac{1}{n_i} > 1$. Συνεπώς υπάρχουν πεπερασμένες επιλογές για το n_1. Έχουμε $1 = \sum_{i=1}^{r} \frac{1}{n_i} \Rightarrow 1 - \frac{1}{n_1} = \sum_{i=2}^{r} \frac{1}{n_i} \Rightarrow n_1 - 1 = \sum_{i=2}^{r} \frac{n_1}{n_i} \leq \sum_{i=2}^{r} \frac{n_1}{n_2} \Rightarrow n_1 - 1 \leq \frac{(r-1)n_1}{n_2} \Rightarrow n_2 \leq \frac{n_1(r-1)}{n_1 - 1}$. Συνεπώς και το n_2 έχει πεπερασμένες επιλογές. Υποθέτουμε ότι το n_i έχει πεπερασμένες επιλογές για κάθε $i < k < r$. Τότε

$$1 = \sum_{i=1}^{r} \frac{1}{n_i} \Rightarrow 1 - \sum_{j=1}^{r} \frac{1}{n_j} = \sum_{i=k+1}^{r} \frac{1}{n_i}$$

$$\Rightarrow \frac{\prod_{j=1}^{k} n_j - \sum_{l=1}^{k} \left(\prod_{\substack{s=1 \\ s \neq l}}^{k} n_s \right)}{\prod_{m=1}^{k} n_m} = \sum_{i=k+1}^{r} \frac{1}{n_i}$$

$$\Rightarrow \prod_{j=1}^{k} n_j - \sum_{l=1}^{k} \left(\prod_{\substack{s=1 \\ s \neq l}}^{k} n_s \right) = \sum_{i=k+1}^{r} \frac{\prod_{m=1}^{k} n_m}{n_i} \leq \sum_{i=k+1}^{r} \frac{\prod_{m=1}^{k} n_m}{n_{k+1}}$$

$$\Rightarrow n_{k+1} \leq \frac{\sum_{i=k+1}^{r} \left(\prod_{m=1}^{k} n_m \right)}{\prod_{j=1}^{k} n_j - \sum_{l=1}^{k} \left(\prod_{\substack{s=1 \\ s \neq l}}^{k} n_s \right)}$$

(ii) Γνωρίζουμε ότι $|G| = \sum_{i=1}^{r} |C_i|$, άρα

$$1 = \sum_{i=1}^{r} \frac{|C_i|}{|G|} = \sum_{i=1}^{r} \frac{1}{n_i}$$

(iii) Έστω G μια πεπερασμένη ομάδα με ακριβώς r κλάσεις συζυγίας, τις

$$\mathrm{Cl}_G(1_G) = C_1, C_2, \ldots, C_r$$

Τότε $|N_G(C_1)| = |G|$. Γνωρίζουμε ότι τα

$$|N_G(C_1)|, |N_G(C_2)|, \ldots, |N_G(C_r)|$$

είναι λύση της εξίσωσης $1 = \sum_{i=1}^{r} \frac{1}{n_i}$.

Οι λύσεις είναι πεπερασμένες το πλήθος. Επιλέγουμε, λοιπόν, αυτήν που εμφανίζει μέγιστο δυνατό $M \in \mathbb{N}$. Τότε $|G| = |N_G(C_1)| \leq M$.

Συνεπώς, υπάρχουν πεπερασμένες το πλήθος πεπερασμένες ομάδες με ακριβώς r κλάσεις συζυγίας.

□

16. 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.]

Λύση. Έστω H υποομάδα της G με $[G : H] = \nu$. Εφόσον η G είναι πεπερασμένα παραγόμενη υπάρχουν πεπερασμένες το πλήθος υποομάδες της G δείκτη ν, έστω $H_1, H_2, \ldots, H_k$. Ορίζουμε $K = \bigcap_{i=1}^{k} H_i$. Η υποομάδα K της G είναι πεπερασμενου δείκτη και θα δείξουμε ότι είναι χαρακτηριστική στην G.

Έστω $\phi : G \to G$ αυτομορφισμός. Γνωρίζουμε ότι

$$[G : H_i] = [\phi(G) : \phi(H_i)] = [G : \phi(H_i)] = \nu$$

Συνεπώς, οι υποομάδες $\phi(H_1), \ldots, \phi(H_k)$ αποτελούν μια αναδιάταξη των $H_1, \ldots, H_k$. Άρα

$$\phi(K) = \phi\left(\bigcap_{i=1}^{k} H_i\right) = \bigcap_{i=1}^{k} \phi(H_i) = K$$

και έτσι η K είναι χαρακτηριστική στην G. □

17. Έστω $G = O(n) = \{A \in M_{n\times n}(\mathbb{R}) : A^t A = I_n\}$ 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 $\mathbb{R}^n$.]

Λύση. Έστω $V \subseteq \mathbb{R}^n$ υπόχωρος του $\mathbb{R}^n$ με $\dim V = m$ και $\{v_1, v_2, \ldots, v_m\}$ μια ορθοκανονική βάση του V.

Επεκτείνουμε την βάση του V σε μια ορθοκανονική βάση του $\mathbb{R}^n$, έστω

$$\{v_1, v_2, \ldots, v_m, v_{m+1}, \ldots, v_n\}$$

Θεωρούμε τον πίνακα A που έχει στήλες τα v_i.

Τότε, ο A είναι ορθογώνιος και $A \cdot e_i = v_i$. Άρα $A(\mathbb{R}^n) = V$ και έτσι η δράση είναι μεταβατική. □

18. 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 $H = \langle S\rangle$.]

Θεωρήματα Sylow

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.]

Απόδειξη. (i) Έστω $o(a) = n, o(b) = m$ και $o(ab) = k$. Τότε

$$(ab)^{nm} = (a^n)^m (b^m)^n = 1$$

Άρα $k \leq mn$.

Εφόσον $o(ab) = s$, έχουμε $a^s b^s = (ab)^s = 1$. Δηλαδή, $a^s = b^{-s} \in \langle a \rangle \cap \langle b \rangle$. Συνεπώς, $o(a^s)|n$ και $o(a^s)|m$. Τότε $o(a^s) = 1 \Rightarrow a^s = 1 = b^{-s}$ και $m|s, n|s \Rightarrow mn|s \Rightarrow mn \leq s$.

Τελικά, $o(ab) = nm = o(a)o(b)$.

(ii) Σταθεροποιούμε $i \leq k$. Χρησιμοποιούμε επαγωγή στο n. Για $n_i = 1$, η P_i είναι προφανώς κυκλική.

Έστω ότι ισχύει το ζητούμενο για κάθε φυσικό μικρότερο του n_i.

Από το Θεώρημα Sylow υπάρχει $H_i \leq P_i$ με $|H_i| = p_i^{n_i - 1}$. Τότε, η H_i είναι κυκλική και τα στοιχεία της είναι οι ρίζες του $x^{p_i^{n_i-1}} - 1 \in \mathbb{F}[x]$ μιας και οι ρίζες είναι το πολύ $p_i^{n_i-1}$. Θεωρούμε το πολυώνυμο

$$x^{p^n - 1} - 1 = (x^{p_i^{n_i}} - 1)(x^{(p^n-1)p_i^{n_i} - p_i^{n_i}} + \cdots + x^{p_i^{n_i}} + 1) \in \mathbb{F}[x]$$

Το πολυώνυμο

$$x^{(p^n-1)p_i^{n_i} - p_i^{n_i}} + \cdots + x^{p_i^{n_i}} + 1 \in \mathbb{F}[x]$$

έχει το πολύ $(p^n - 1)p_i^{n_i} - p_i^{n_i}$ ρίζες, ενώ το

$$x^{p^n - 1} - 1 \in \mathbb{F}[x]$$

έχει ακριβώς $p^n - 1$ ρίζες. Έτσι, το πολυώνυμο

$$x^{p_i^{n_i}} - 1 \in \mathbb{F}[x]$$

έχει ακριβώς $p_i^{n_i}$ ρίζες.

Επιλέγουμε $\rho_i \in P_i \backslash H_i$. Τότε $o(\rho_i) = p_i^{n_i}$, αφού το ρ_i είναι ρίζα του $x^{p_i^{n_i}} - 1 \in \mathbb{F}[x]$, ενώ δεν είναι ρίζα του $x^{p_i^{n_i-1}} - 1 \in \mathbb{F}[x]$.

Τελικά,

$$\mathbb{F}^* = \langle \rho_1 \rho_2 \cdots \rho_k \rangle$$

□

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.

   Απόδειξη. (i) Έστω $|G| = p^n$ και $H \leq G$. Τότε $|H| \Big| |G|$, άρα $|H| = p^\lambda$, όπου $\lambda \leq n$.
   Επιπλέον, αν $H \lhd G$, έχουμε $|G/H| = \dfrac{|G|}{|H|} = p^{n-\lambda}$.

   (ii) Έστω $|N| = p^n$, $|G/N| = p^k$ και $g \in G$. Τότε

   $$(gN)^{p^k} = g^{p^k} N = N$$

   Έτσι, $g^{p^k} \in N$. Αφού $|N| = p^n$, έχουμε ότι $(g^{p^k})^{p^n} = 1$. Άρα $p | o(g)$, δηλαδή η G είναι p-ομάδα.

   □

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

   Λύση. Με επαγωγή επί του n.

   Γνωρίζουμε ότι $1 \neq Z(G) \lhd G$. Θεωρούμε την υποομάδα $H \cdot Z(G)$ -είναι υποομάδα γιατί η $Z(G)$ είναι κανονική. Τότε $H \subseteq H \cdot Z(G) \subseteq G$. Από την μεγιστικότητα της H έπεται ότι, $H = H \cdot Z(G)$ ή $G = H \cdot Z(G)$.

   - Αν $H = H \cdot Z(G)$, τότε $Z(G) \subseteq H$ και $Z(G) \lhd H$. Αφού η H είναι μεγιστική στην G, η $H/Z(G)$ είναι μεγιστική στην $G/Z(G)$ και από την επαγωγική υπόθεση $H/Z(G) \lhd G/Z(G)$. Από το θεώρημα της Αντιστοιχίας $H \lhd G$.
   - Αν $G = H \cdot Z(G)$, τότε για $g \in G$ και $h_1 \in H$ υπάρχουν $h \in H, x \in Z(G)$ ώστε

     $$gh_1g^{-1} = (hx)h_1(hx)^{-1} = hxh_1x^{-1}h^{-1} = hh_1h^{-1} \in H$$

     Δηλαδή, $H \lhd G$.

   Αν $|G/H| = p^\lambda$, $\lambda \geq 2$, τότε η G/H έχει υποομάδα τάξεως p της μορφής K/H για κάποιο $K \subseteq H$.

   Σε αυτήν την περίπτωση $H \subset K \subset G$ -άτοπο, από την μεγιστικότητα της H. □

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.

   Λύση. (i) Έστω $g \in G$. Τότε $gPg^{-1} \subseteq gKg^{-1} = K$.

   Άρα οι P, gPg^{-1} είναι Sylow p-υποομάδες της K. Συνεπώς, υπάρχει $x \in K$ με $xgPg^{-1}x^{-1} = P$. Αυτό σημαίνει ότι $xg \in N_G(P)$.

   Έστω $xg = g_1 \in N_G(P)$. Τότε $g = x^{-1}g_1 = g_1 g_1^{-1} x^{-1} g_1 \in N_G(P) \cdot K$.

(ii) 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 $H \lhd G$.

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 $P \lhd G$.

□

5. (i) Έστω $H \lhd G$, 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, η οποία δεν είναι Sylow p-υποομάδα της G έτσι ώστε $p|[G : H]$. Δείξτε ότι $H < N_G(H)$.

Λύση. (i) Προφανώς $P \subseteq Q \cap H$.

Για τον αντίστροφο εγκλεισμό: Εφόσον $|Q \cap H| \Big| |H|$ και $|Q \cap H| \Big| |Q|$ έχουμε ότι η $Q \cap H$ είναι p-ομάδα της H. Έτσι,

$$Q \cap H \subseteq xPx^{-1}$$

Όμως $Q \cap H \lhd G$, αφού $H \lhd G$ και άρα

$$Q \cap H = x^{-1}(Q \cap H)x \subseteq P$$

(ii)

□

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.

Λύση. (i) Από τα Θεωρήματα Sylow γνωρίζουμε ότι $n_p(G) \equiv 1 \pmod{p}$ και $n_p(H) \equiv 1 \pmod{p}$. Τότε

$$[G : N_G(P)] \equiv 1 \pmod{p}$$

και

$$[H : N_H(P)] \equiv 1 \pmod{p}$$

Όμως $N_H(P) \subseteq N_G(P) \subseteq H \subseteq G$ και έτσι

$$[G : N_G(P)] = [G : H][H : N_H(P)]$$

και έπεται το ζητούμενο.

(ii) Έστω $|G| = p^n m$, με $(m,p) = 1$, $|P| = p^n$, $|KP| = p^s k$, με $(k,p) = 1$, $|K| = p^\lambda a$, με $(a,p) = 1$, $\lambda \leq n$ και $|K \cap P| = p^\mu$, $\mu \leq \lambda$.

Τότε

$$p^\lambda a p^n = |K||P| = |KP||K \cap P| = p^s k p^\mu$$

Έτσι $\lambda = \mu$ και $n = s$. Άρα $|K \cap P| = p^\lambda$ και η $K \cap P$ είναι Sylow p-υποομάδα της K.

Αφού $K \lhd G$, έχουμε ότι $K \lhd KP$. Από το θεώρημα της Αντιστοιχίας, παίρνουμε ότι εμφανίζεται η ίδια δύναμη του p στις $|G/K|$ και $|KP/P|$, μιας και το ίδιο συμβαίνει για τις $|G|$ και $|KP|$.

Τέλος, από το 2^o Θεώρημα Ισομοφισμών

$$KP/K \simeq P/P \cap K$$

άρα η KP/P είναι p-ομάδα. Συνεπώς, η KP/P είναι Sylow p-υποομάδα της G/K.

(iii) Άμεσο από το ερώτημα (ii).

□

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.

Λύση. (i) Από τα Θεωρήματα Sylow, έχουμε ότι η gP_ig^{-1} είναι και αυτές Sylow p-υποομάδες της G.

Εφόσον

$$g(hP_ih^{-1})g^{-1} = (gh)P_i(gh)^{-1}$$

έχουμε ότι $\phi(gh) = \phi(g)\phi(h)$, δηλαδή η ϕ είναι ομομορφισμός.

Τώρα, $g \in \ker\phi \Leftrightarrow gP_ig^{-1} = P_i \quad \forall i = 1, 2, \ldots, m \Leftrightarrow g \in N_G(P_i) \quad \forall i = 1, 2, \ldots, m \Leftrightarrow g \in \bigcap_{i=1}^{m} N_G(P_i)$

Τελικά,

$$\ker\phi = \bigcap_{i=1}^{m} N_G(P_i)$$

(ii)

□

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

Λύση. Ξέρουμε ότι αν $|G| = p^n, pq$ ή pqr, όπου p, q, r είναι πρώτοι, τότε η G δεν είναι απλή. Σύμφωνα με αυτό, απομένει να κοιτάξουμε αν μια ομάδα τάξης $|G| = 24, 40, 48, 54$ ή 56 δεν είναι απλές.

- Αν $|G| = 24 = 2^3 \cdot 3$, από τα θεωρήματα Sylow έχουμε $n_3 = 3k + 1|8$, άρα $n_3 = 1$ ή 4. Αν η G είναι απλή, τότε $n_3 = 4$ και

$$G \hookrightarrow S_4$$

  Αλλά $|G| = 2^3 \cdot 3 = |S_4|$, άρα $G \simeq S_4$. Τότε, όμως, οδηγούμαστε σε άτοπο, εφόσον $A_4 \lhd S_4$.
- Έστω $|G| = 40 = 2^3 \cdot 5$. Από τα Θεωρήματα Sylow έχουμε $n_5 = 5k+1|8$, άρα $n_5 = 1$, το οποίο σημαίνει ότι υπάρχει μοναδική, άρα και κανονική, Sylow 5-υποομάδα της G.
- Έστω $|G| = 48 = 2^4 \cdot 3$. Από τα Θεωρήματα Sylow έχουμε $n_3 = 16 + 1|3$. Αν η G είναι απλή, τότε $n_3 = 16$, άρα υπάρχουν $16 \cdot 2 = 32$ στοιχεία τάξης 3. Απομένουν 16 στοιχεία τάξης $2, 2^2, 2^3, 2^4$, άρα υπάρχει μοναδική και κανονική Sylow 2-υποομάδα της G.
- Έστω $|G| = 54 = 2 \cdot 3^3$. Αν H Sylow 3-υποομάδα της G, τότε $[G : H] = 2$, άρα η H είναι κανονική στην G.
- Έστω $|G| = 56 = 2^3 \cdot 7$. Τότε $n_7 = 8k + 1|7$, και αν η G είναι απλή έχουμε $n_7 = 8$. Έχουμε, δηλαδή, $8 \cdot (7 - 1) = 48$ στοιχεία τάξης 7 και απομένουν $2^3 = 8$ στοιχεία. Άρα υπάρχει μοναδική και κανονική Sylow 2-υποομάδα της G.

□

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

Λύση. (i) Έστω ότι η G είναι απλή με $|G| = 90 = 2 \cdot 3^2 \cdot 5$. Τότε $n_5 = 5k+1|18 \Rightarrow n_5 = 6$ και $n_3 = 3k + 1|10 \Rightarrow n_3 = 10$.

Αν $P_k \cap P_\lambda = 1$ για κάθε P_k, P_λ Sylow 3-υποομάδα της G, τότε έχουμε $6 \cdot 4 = 24$ στοιχεία τάξης 5 και $8 \cdot 10$ στοιχεία τάξης 3 ή 9 -άτοπο.

Έστω P, Q Sylow 3-υποομάδες της G με $|P \cap Q| = 3$. Τότε $9 \Big| |N_G(P \cap Q)| \Big| 90$. Άρα $|N_G(P \cap Q)| = 18, 45$ ή 90.

Αν $|N_G(P \cap Q)| = 90$, τότε $P \cap Q \lhd G$.

Αν $|N_G(P \cap Q)| = 45$, τότε $[G : N_G(P \cap Q)] = 2$, άρα $N_G(P \cap Q) \lhd G$.

Τέλος, αν $|N_G(P \cap Q)| = 18$, τότε $[G : N_G(P \cap Q)] = 5$ και έτσι $G \hookrightarrow S_5$ -άτοπο, αφού $90 \not| 5!$.

(ii) Έστω ότι η G είναι απλή με $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Τότε $n_2 > 1, n_3 > 1$ και $n_{11} > 1$. Γνωρίζουμε ότι

$$n_{11} | 2^2 \cdot 3 \Rightarrow n_{11} = 2, 3, 4, 12 \quad \text{ή} \quad 6$$

$$n_{11} \equiv 1 \pmod 1 11 \Rightarrow 11 | n_{11} - 1 \Rightarrow n_{11} \geq 12$$

Άρα $n_{11} = 12$.

Επίσης $n_3 | 2 \cdot 11$ και $n_3 \equiv 1 \pmod 1 3 \Rightarrow n_3 \geq 4$

Τέλος, $n_2 | 3 \cdot 11$ και $n_2 \equiv 1 \pmod 2 \Rightarrow n_2 \geq 3$.

Οι $n_{11} = 12$ Sylow 11-υποομάδες μας δίνουν $12(11-1) = 120$ στοιχεία τάξης 11. Οι $n_3 \geq 4$ Sylow 3-υποομάδες μας δίνουν τουλάχιστον $4(3-1) = 8$ στοιχεία τάξης 3. Οι $n_2 \geq 3 > 2$ Sylow 2-υποομάδες μας δίνουν τουλάχιστον $2^2 + 2^2 - 2 = 6$ στοιχεία τάξης τάξεως 2^2 ή 2 ή 0.

Άρα $|G| \geq 120 + 8 + 6 = 134$ -άτοπο. Τελικά, $n_{11} = 1$ ή $n_3 = 1$ ή $n_2 = 1$ και η αντίστοιχη Sylow υποομάδα είναι κανονική.

Άρα, η G δεν είναι απλή.

(iii) Έστω G απλή ομάδα με $|G| = 150 = 2 \cdot 3 \cdot 5^2$. Τότε, $n_5 = 5k+1 | 6$. Συνεπώς $n_5 = 6$. Έτσι έχουμε

$$G \hookrightarrow S_6$$

και άρα $2 \cdot 3 \cdot 5^2 = |G| \Big| |S_6| = 6!$ -άτοπο.

□

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 $|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.]

Λύση. Έστω $A \in GL_n(\mathbb{F}_p)$. Για την πρώτη στήλη του A υπάρχουν $p^n - 1$ επιλογές, για την δεύτερη $p^n - p$ και για την n-οστή $p^n - p^{n-1}$ επιλογές.

Έτσι

$$|GL_n(\mathbb{F}_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1}) = p \cdot p^2 \cdots p^{n-1} \cdot m$$

με $p \not| m$.

Αν, τώρα, $B \in UT_n(\mathbb{F}_p)$, τότε για την πρώτη στήλη υπάρχει 1 επιλογή, για την δεύτερη p και για την n-οστή p^{n-1}. Άρα

$$|UT_n(\mathbb{F}_p)| = p \cdot p^2 \cdots p^{n-1}$$

Συνεπώς, η $UT_n(\mathbb{F}_p)$ είναι Sylow υποομάδα της $GL_n(\mathbb{F}_p)$. □

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.

Λύση. Έστω $|G| = p^n m$ με $p \nmid m$ και $|H| p^n$. Θεωρούμε την δράση της K στα σύμπλοκα G/H.

Έχουμε ότι $|G/H| = [G : H] = m = \sum_{i=1}^{r} |\mathcal{O}(x_i H)| = \sum_{i=1}^{r} [K : K \cap x_i H x_i^{-1}]$.

Εφόσον $p \nmid m = [G : H]$, υπάρχει $x_i \in X$ ώστε $p \not\Big| [K : K \cap x_i H x_i^{-1}]$. Αν $|K| = p^\nu \mu = [K : K \cap x_i H x_i^{-1}] |K \cap x_i H x_i^{-1}|$, τότε $p^\nu \Big| |K \cap x_i H x_i^{-1}|$ αφού $p \not\Big| [K : K \cap x_i H x_i^{-1}]$.

Επιπλέον, η $K \cap x_i H x_i^{-1}$ είναι p-υποομάδα της H και υποομάδα της K.

Άρα $|K \cap x_i H x_i^{-1}| = p^\nu$ και η $K \cap x_i H x_i^{-1}$ είναι Sylow 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 $n = |G|$.]

Λύση. Έστω $|G| = p^k m = n$, με $(p, m) = 1$. Τότε, υπάρχει

$$\phi : G \hookrightarrow GL_n(\mathbb{F}_p)$$

και

$$\psi : G \xrightarrow{\simeq} \operatorname{im} \phi = K \leq GL_n(\mathbb{F}_p)$$

Αφού η $UT_n(\mathbb{F}_p)$ είναι Sylow p-υποομάδα της $GL_n(\mathbb{F}_p)$ και $\operatorname{im} \phi \leq GL_n(\mathbb{F}_p)$, ξέρουμε ότι υπάρχει $x \in GL_n(\mathbb{F}_p)$ τέτοιο ώστε η $K \cap xUT_n(\mathbb{F}_p)x^{-1}$ να είναι Sylow p-υποομάδα της K.

Τότε η

$$L = \psi^{-1}(K \cap xUT_n(\mathbb{F}_p)x^{-1})$$

είναι Sylow p-υποομάδα της G. □

Γινόμενα Ομάδων

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 μας 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.

   Λύση. Έστω $|G| = n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου p_i διακεκριμένοι πρώτοι. Αφού η G είναι αβελιανή, για κάθε i υπάρχει μοναδική, έστω P_i, Sylow p_i-υποομάδα της G, η οποία επιπλέον θα είναι κανονική.

   Μάλιστα, η G είναι το ευθύ γινόμενο των Sylow υποομάδων της, δηλαδή

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

   Τώρα, $m|n$, άρα $m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, όπου $b_i \leq a_i$ για κάθε i. Όμως, η P_i είναι p_i-ομάδα. Άρα η P_i έχει υποομάδα τάξεως $p_i^{m_i}$ για κάθε $m_i \leq a_i$.

   Ιδιαιτέρως, η P_i έχει υποομάδα $p_i^{b_i}$, έστω Q_i. Έστω $H = Q_1 \times Q_2 \times \cdots \times Q_k$. Τότε $H \leq G$ και $|H| = |Q_1||Q_2| \cdots |Q_k| = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} = m$. □

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 $a' \equiv a \,(\mathrm{mod} m)$, δηλ. $[a']_m = [a]_m$, και $(a', n) = 1$. Για να δείξουμε ότι $(a', n) = 1$, θεωρούμε πρώτο διαιρέτη p του n και διακρίνουμε δύο περιπτώσεις: $p|a$ και $p \nmid a$.]

Σειρές Ομάδων

1. Να βρεθούν δυο μη ισόμορφες ομάδες G_1, G_2 τέτοιες ώστε να υπάρχει συνθετική σειρά 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.

Επιλύσιμες Ομάδες

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 της 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:
   (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. Αν $K \underset{\text{π.α.}}{\leq} \Lambda \underset{\text{π.α.}}{\leq} M$, τότε $K \underset{\text{π.α.}}{\leq} M$.
15. Αποδείξτε ότι $G^{(n)} \underset{\text{π.α.}}{\leq} G$ για κάθε n.
16. Αποδείξτε ότι η $Z(G)$ δεν είναι αναγκαστικά πλήρως αναλλοιώτη υποομάδα της G. [Υπόδειξη: Θεωρήστε την $G = \mathbb{Z}_2 \times S_3$.]
17. Να βρεθεί η παράγωγος σειρά της S_4.

Μηδενοδύναμες Ομάδες

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, $\gamma_i(G) \underset{\text{π.α.}}{\leq} G$.

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 πεπερασμένη ομάδα. Αποδείξτε ότι η G είναι μηδενοδύναμη ανν για κάθε α, $\beta \in G$ με $(o(\alpha), o(\beta)) = 1$, ισχύει $\alpha\beta = \beta\alpha$.

15. 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.

16. 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: $\alpha, \beta\alpha\beta^{-1} \in \langle \alpha, G' \rangle$.]

17. 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 $[x, g^{-1}]y^{-1}[g^{-1}, x]y = 1$.]

18. *(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.]

Πολυκυκλικές και Προσεγγιστικά Πεπερασμένες Ομάδες

1. Μια ομάδα G λέγεται **Hopfian** αν δεν είναι ισόμορφη με γνήσιο πηλίκο της, ή ισοδύναμα αν $\phi : G \to G$ επιμορφισμός, τότε η ϕ είναι επιμορφισμός.

   Αποδείξτε ότι κάθε πεπερασμένα παραγόμενη προσεγγιστικά πεπερασμένη ομάδα είναι Hopfian.

2. Αν G πεπερασμένα παραγόμενη και προσεγγιστικά πεπερασένη ομάδα, τότε η $\mathrm{Aut}(G)$ είναι προσεγγιστικά πεπερασμένη.

3. (i) Αν $G_1, G_2, \ldots, G_n$ προσεγγιστικά πεπερασμένες p-ομάδες, τότε η $G = G_1 \times G_2 \times \cdots \times G_n$ είναι προσεγγιστικά πεπερασμένη p-ομάδα.

   (ii) Κάυε πεπερασμένα παραγόμενη ελευθέρα στρέψης αβελιανή ομάδα είναι προσεγγιστικά πεπερασμένη p-ομάδα, για κάθε πρώτο p.

   (iii) Αν G πεπερασμένα παραγόμενη ελευθέρα στρέψης μηδενοδύναμη ομάδα, τότε η G είναι προσεγγιστικά πεπερασμένη p-ομάδα, για κάθε πρώτο p.

Ελεύθερες Ομάδες

1. Μια αβελιανή ομάδα είναι προβολική ανν είναι ελεύθερη αβελιανή.

2. Αν η G είναι ελεύθερη αβελιανή διάστασης n, τότε η G δεν μπορεί να παραχθεί από m στοιχεία, όπου $m < n$.

3. Έστω F ελεύθερη αβελιανή ομάδα πεπερασμένης διαστάσης $n < \infty$ και $H \leq F$. Τότε, η F/H είναι πεπερασμένη ανν $\text{rank}(F) = \text{rank}(H)$.

4. Αν G ελεύθερη αβελιανή πεπερασμένης διάστασης και $\phi : G \to H$ επιμορφισμός, τότε $\text{rank}(G) = \text{rank}(H) + \text{rank}(\ker \phi)$.

5. Έστω F ελεύθερη αβελιανή διάστασης n. Αποδείξτε ότι $\text{Aut}(F) \simeq GL_n(\mathbb{Z})$.

6. Αν $G = \underset{\alpha}{*} G_\alpha$ και $G_\alpha = \underset{\beta}{*} H_{\alpha\beta}$ για κάθε α, τότε η G είναι το ελεύθερο γινόμενο όλων των $H_{\alpha\beta}$, το οποίο ελεύθερο γινόμενο ονομάζεται **επιλέπτυνση** του αρχικού.

7. Αν $G = \underset{\alpha}{*} G_\alpha$ και $1 \leq H_\alpha \leq G_\alpha$ για κάθε α, τότε η υποομάδα της G που παράγεται από τις H_α είναι το ελεύθερο γινόμενο των H_α, δηλαδή $\underset{\alpha}{*} H_\alpha = \langle H_\alpha : \alpha \rangle$.

8. (i) (Καθολική ιδιότητα του ευθέως αθροίσματος) Έστω G αβελιανή ομάδα και G_α, $\alpha \in J$, οικογένεια υποομάδων της G. Αν $G = \bigoplus_{\alpha \in J} G_\alpha$, τότε για κάθε αβελιανή ομάδα H και κάθε οικογένεια ομομορφισμών $\phi_\alpha : G_\alpha \to H$, υπάρχει μοναδικός ομομορφισμός $\phi : G \to H$ που επεκτείνει τις ϕ_α (ή $\phi \circ i_\alpha = \phi_\alpha$).

   (ii) Αν $G = \underset{\alpha}{*} G_\alpha$ και G' η παράγωγος υποομάδα της G, τότε $G./G' = \bigoplus_{\alpha} G_\alpha/G'_\alpha$.

   [Υπόδειξη: Η G/G' ικανοποιεί την καθολική ιδιότητα του ευθέως αθροίσματος.]

9. Αν $G_\alpha \neq 1$ για κάθε $\alpha \in J$, όπου $|J| \geq 2$, τότε $Z(\underset{\alpha}{*} G_\alpha) = 1$.

10. Αν $G = \underset{\alpha \in J}{*} G_\alpha$ με $G_\alpha \neq 1$ για κάθε α και $|J| \geq 2$, τότε η G περιέχει στοιχεία απείρου τάξης.

    Ιδιαιτέρως, η G είναι άπειρη ομάδα.

11. Κάθε στοιχείο πεπερασμένης τάξης σε ένα ελεύθερο γινόμενο $\underset{\alpha}{*} G_\alpha$, είναι συζυγές με στοιχείο ενός ελεύθερου παράγοντα.

    Ιδιαιτέρως, αν κάθε G_α είναι ελευθέρα στρέψης, τότε η $\underset{\alpha}{*} G_\alpha$ είναι ελευθέρα στρέψης.

12. Η ελεύθερη ομάδα διάστασης 2, F_2, περιέχει ελεύθερη υποομάδα διάστασης k, για κάθε φυσικό k.

13. Η F_2 περιέχει ελεύθερη υποομάδα απεου τάξης.

14. Κάθε πεπερασμένα παραγόμενη ελεύθερη ομάδα είναι $\mathbb{Z}$-γραμμική, δηλαδή εμφυτεύεται στην $GL_n(\mathbb{Z})$.

15. Αν $N \lhd G$ και η G/N είναι ελεύθερη, τότε υπάρχει υποομάδα H της G με $G = HN$ και $H \cap N = 1$.

16. Έστω F ελεύθερη ομάδα και $H \leq F$ υποομάδα πεπερασμένου δείκτη. Αν $K \leq F$ με $K \neq 1$, τότε $K \cap H \neq 1$.

17. Κάθε πεπερασμένα παραγόμενη ελεύθερη ομάδα έχει πεπερασμένη διάσταση.