ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

ανοικτάμαθήματα
opencourses

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Οι Ομάδες τάξης pq, p, q: πρώτοι αριθμοί

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

6. **Οι Ομάδες τάξης** pq, p, q: **πρώτοι αριθμοί**

Στην παρούσα ενότητα θα ταξινομήσουμε όλες τις δυνατές ομάδες τάξης τάξης $2p$, όπου p είναι ένας πρώτος αριθμός. Με άλλα λόγια θα περιγράψουμε όλες τις ομάδες τάξης $2p$ οι οποίες είναι δομικά διαφορετικές. Αργότερα η έννοια «δομικά διαφορετικές» θα εκφρασθεί με χρήση της έννοιας του ομομορφισμού ομάδων, ως «μη-ισόμορφες».

6.1. **Ομάδες τάξης $2p$.** Υπενθυμίζουμε ότι, αν $n \geq 3$, η n-οστή διεδρική ομάδα D_n είναι η ομάδα των συμμετριών του κανονικού n-γώνου. Αν $n = 1$ η D_n είναι η κυκλική τάξης 2, και αν $n = 2$, η D_2 είναι η ομάδα του Klein. Η ομάδα D_n περιγράφεται ως:

$$D_n = \{e, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots, a^{n-1}b \mid \text{όπου } a^n = e, \quad b^2 = e, \quad \text{και} \quad bab = a^{-1}\}$$

Σημειώνουμε ότι οι σχέσεις $a^n = e, b^2 = e, bab = a^{-1}$ καθορίζουν πλώρως την ομάδα D_n. Δηλαδή κάθε ομάδα η οποία «παράγεται» από δύο στοιχεία a, b τα οποία ικανοποιούν τις παραπάνω σχέσεις, είναι «ισόμορφη» με την D_n.

Θεώρημα 6.1. *Έστω G μια ομάδα τάξης $\mathsf{o}(G) = 2p$, όπου p: πρώτος. Τότε:*

(1) *Είτε η G είναι δομικά ίδια με την κυκλική ομάδα $\mathbb{Z}_{2p}$.* *(όταν η G είναι αβελιανή)*
(2) *ή η G είναι δομικά ίδια με την διεδρική ομάδα D_p.* *(όταν η G δεν είναι αβελιανή)*

και οι ομάδες $\mathbb{Z}_{2p}$ και D_p είναι δομικά διαφορετικές.

Για την απόδειξη θα χρειασθούμε κάποιες βοηθητικές προτάσεις οι οποίες είναι ενδιαφέρουσες από μόνες τους.

Λήμμα 6.2. *Έστω G μια πεπερασμένη αβελιανή ομάδα. Αν η G περιέχει δύο στοιχεία a, b τάξης 2, όπου $a \neq b$, τότε το σύνολο $V = \{e, a, b, ab\}$ είναι μια υποομάδα της G και επομένως $4 \mid \mathsf{o}(G)$.*

Απόδειξη. Επειδή η G είναι αβελιανή έπεται ότι $ab = ba$ και η τάξη του ab είναι ίση με 2, διότι $(ab)^2 = abab = aabb = a^2b^2 = ee = e$, και $ab \neq e$ διότι αν $ab = e$, τότε $a = b^{-1} = b$ το οποίο έιναι άτοπο. Το σύνολο V είναι πεπερασμένο και κλειστό στον πολλαπλασιασμό της G. Επομένως, σύμφωνα με το Λήμμα 2.7, έπεται ότι το υποσύνολο V είναι μια υποομάδα της G. Τέλος από το Θεώρημα του Lagrange έπεται ότι $\mathsf{o}(V) = 4 \mid \mathsf{o}(G)$. $\square$

Λήμμα 6.3. *Έστω G μια ομάδα άρτιας τάξης. Τότε η G περιέχει ένα στοιχείο τάξης 2.*

Απόδειξη. Επειδή η G έχει άρτια τάξη, θα έχουμε $\mathsf{o}(G) = 2\lambda$, με $\lambda \geq 1$, και άρα το σύνολο $G \setminus \{e\}$ έχει $2\lambda - 1$ στοιχεία. Θεωρούμε το σύνολο

$$X = \{x \in G \setminus \{e\} \mid x \neq x^{-1}\}$$

Το πλήθος των στοιχείων του X είναι άρτιο, διότι αν $x \in X$ τότε και $x^{-1} \in X$. Επίσης, το X είναι γνήσιο υποσύνολο του $G \setminus \{e\}$, δηλαδή $X \subseteq G \setminus \{e\}$ και $X \neq G \setminus \{e\}$, αφού το X έχει άρτιο πλήθος στοιχείων ενώ το $G \setminus \{e\}$ έχει περιττό πλήθος στοιχείων. Άρα υπάρχει στοιχείο $a \in G \setminus \{e\}$ και $a \notin X$. Αυτό όμως σημαίνει ότι $a \neq e$ και $a = a^{-1}$, δηλαδή $a^2 = e$ και άρα η G έχει ένα τουλάχιστον στοιχείο τάξης 2. $\square$

Η παρακάτω πρόταση μας εξασφαλίζει την ύπαρξη ενός μοναδικού στοιχείου τάξης 2 σε μια ομάδα άρτιας τάξης, υπο την προϋπόθεση ότι η τάξη της ομάδας δεν διαιρείται από το 4.

Λήμμα 6.4. *Έστω G μια πεπερασμένη αβελιανή ομάδα άρτιας τάξης. Αν $4 \nmid \mathsf{o}(G)$, τότε η G περιέχει ακριβώς ένα στοιχείο τάξης* 2.

Απόδειξη. Απο το παραπάνω Λήμμα 8.3, η G περιέχει τουλάχιστον ένα στοιχείο a τάξης 2. Αν η G περιέχει δύο διαφορετικά στοιχεία a, b τάξης 2, τότε σύμφωνα με το Λήμμα 8.2, θα έπρεπε $4 \mid \mathsf{o}(G)$ κάτι το οποίο είναι άτοπο. Άρα η G περιέχει ακριβώς ένα στοιχείο τάξης 2. □

Λήμμα 6.5. *Έστω G μια ομάδα. Αν κάθε μη-ταυτοτικό στοιχείο της G έχει τάξη 2, τότε η G είναι αβελιανή.*

Απόδειξη. Επειδή $\mathsf{o}(x) = 2$, $\forall x \in G \setminus \{e\}$, έπεται ότι $x^2 = e$ και άρα

$$\forall x \in G : \quad x^{-1} = x$$

Έστω τώρα ότι $x, y \in G$. Τότε

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

και άρα η G είναι αβελιανή. □

Μπορούμε τώρα να αποδέιξουμε το Θεώρημα 6.1:

Απόδειξη. (*του Θεωρήματος* 6.1) Θα διακρίνουμε περιπτώσεις:

(1) Αν η G περιέχει ένα στοιχείο τάξης $2p$, τότε προφανώς η G είναι κυκλική και άρα δομικά ίδια με την κυκλική ομάδα $\mathbb{Z}_{2p}$.

(2) Υποθέτουμε ότι η G δεν έχει κανένα στοιχείο τάξης $2p$.

  (α΄) Αν $p = 2$, τότε $\mathsf{o}(G) = 4$, και επειδή η G δεν είναι κυκλική η G θα είναι δομικά ίδια με την ομάδα του Klein V η οποία συμπίπτει με την D_2.

  (β΄) Έστω $p > 2$. Τότε p είναι περιττός και επομένως $4 \nmid 2p = \mathsf{o}(G)$.

    (i) Αν όλα τα στοιχεία της G (εκτός του ταυτοτικού) έχουν τάξη 2, τότε από το Λήμμα 6.5 η G είναι αβελιανή και τότε Από το Λήμμα 8.2 τότε η G έχει ως υποομάδα την ομάδα του Klein η οποία έχει τάξη 4, κάτι το οποίο είναι άτοπο διότι $4 \nmid 2p = \mathsf{o}(G)$.

    (ii) Επομένως δεν έχουν όλα τα στοιχεία της G τάξη 2. Έτσι αν a είναι ένα στοιχείο της G, θα είναι: $\mathsf{o}(a) = 1, 2, p$, ή $2p$. Οι περιπτώσεις $\mathsf{o}(a) = 1, 2, 2p$, έχουν αποκλειστεί και άρα, η G περιέχει ένα στοιχείο a τάξης p.

    Θεωρούμε την κυκλική υποομάδα $H = \langle a \rangle$ της G η οποία παράγεται από το a. Προφανώς $[G : H] = 2$, και άρα η H έχει ακριβώς δύο διακεκριμμένα αριστερά σύμπλοκα στην G: H και bH, και τότε:

$$G = H \cup bH, \qquad \text{όπου} \quad b \in G \setminus H \qquad \text{και} \qquad H \cap bH = \emptyset$$

    Ισχυρισμός: $b^2 = e$.

    Πραγματικά: $b^2 \in H \cup bH$. Αν $b^2 \in bH$, τότε $b^2 = bh$, $h \in H$ και τότε $b = h \in H$ που είναι άτοπο. Άρα $b^2 \in H$ και άρα $b^2 = a^k$ για κάποιο $k \in \mathbb{Z}$. Αν $k \neq 0$, τότε η κυκλική υποομάδα $\langle b \rangle$ η οποία παράγεται από το b θα περιέχει την H αφού το στοιχείο $b^2 = a^k$ θα την παράγει, και το $b \notin H$, και άρα η $\langle b \rangle$ θα περιέχει τουλάχιστον $p + 1$ στοιχεία. Επειδή $\mathsf{o}(H) = 2p$, έπεται ότι $\langle b \rangle = G$ και άρα η G είναι κυκλική το οποίο είναι άτοπο. Άρα δείξαμε ότι κάθε στοιχείο $b \in G \setminus H$ έχει τάξη $\mathsf{o}(b) = 2$.

    Θεωρούμε το στοιχείο $bab \in G$. Τότε από την Πρόταση 3.17 θα έχουμε:

$$b^2 = e \implies b^{-1} = b \implies bab = b^{-1}ab \implies \mathsf{o}(bab) = \mathsf{o}(b^{-1}ab) = \mathsf{o}(a) = p$$

    Τότε όμως

$$b^{-1}ab = bab = a^k \qquad \text{για κάποιο} \qquad k \in \mathbb{Z}^+ \tag{†}$$

και επομένως:

$$a = bbabb = ba^k b = (bab)^k = (a^k)^k = a^{k^2} \quad \Longrightarrow \quad a^{k^2-1} = e$$

Επειδή $\mathsf{o}(a) = p$ είναι ένας πρώτος αριθμός, έπεται ότι

$$p \mid k^2 - 1 \quad \Longrightarrow \quad p \mid (k+1)(k-1) \quad \Longrightarrow \quad p \mid k+1 \quad \text{ή} \quad p \mid k-1$$

(Α') Αν $p \mid k-1$, τότε θα έχουμε $k - 1 = pr$, για κάποιο $r \geq 1$, και άρα $k = pr + 1$. Τότε από την σχέση (†) θα έχουμε:

$$bab = a^k = a^{pr+1} = (a^p)^r a^1 = e^r a = a$$

Τότε όμως θα έχουμε $bab = a$ και άρα $babb = ab \implies ba = ab$. Επειδή $\mathsf{o}(a) = p$ και $\mathsf{o}(b) = 2$ και $(2, p) = 1$, θα έχουμε ότι το στοιχείο ab έχει τάξη $\mathsf{o}(ab) = 2p$ κάτι το οποίο είναι άτοπο.

(Β') Επομένως $p \mid k+1$, και τότε θα έχουμε $k + 1 = ps$, για κάποιο $s \geq 1$, και άρα $k = ps - 1$. Τότε από την σχέση (†) θα έχουμε:

$$bab = a^k = a^{ps-1} = (a^p)^s a^{-1} = e^r a^{-1} = a^{-1}$$

Συνοψίζοντας την δεύτερη περίπτωση, θα έχουμε ότι η G περιέχει δύο στοιχεία a, b έτσι ώστε:

$$a,\, b \in G: \quad a^p = e = b^2 \quad \text{και} \quad bab = b^{-1}ab = a^{-1}$$

Τότε όμως η G είναι δομικά ίδια με την διεδρική ομάδα D_p.

Προφανώς οι ομάδες $\mathbb{Z}_{2p}$ και D_p είναι δομικά διαφορετικές, διότι, π.χ., η $\mathbb{Z}_{2p}$ είναι αβελιανή και η D_p δεν είναι αβελιανή. □

Το Θεώρημα 6.1 μας εξασφαλίζει ότι υπάρχουν μόνο δύο, δομικά διαφορετικές ομάδας τάξης $6, 10, 14, \cdots$: η κυκλική ομάδα τάξης $6, 10, 14, \cdots$, και η ομάδα συμμετριών του κανονικού τριγώνου, πενταγώνου, επταγώνου, $\cdots$.

6.2. **Ομάδες τάξης** pq**.** Γενικότερα ενδιεφερόμαστε για ομάδες G τάξης pq όπου p, q είναι πρώτοι αριθμοί. Αυτή η περίπτωση είναι περισσότερο σύνθετη. Όταν η ομάδα G είναι αβελιανή, τότε έχουμε το ακόλουθο αποτέλεσμα:

Θεώρημα 6.6. *Έστω G μια ομάδα με τάξη pq, όπου p, q είναι διακεκριμμένοι πρώτοι αριθμοί: $p \neq q$. Αν η G είναι αβελιανή, τότε η G είναι κυκλική.*

Απόδειξη. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $p > q$. Αν υπάρχει στοιχείο τάξης pq στην G, τότε προφανώς η G είναι κυκλική.

Υποθέτουμε ότι η G δεν έχει κανένα στοιχείο τάξης pq, και θα οδηγηθούμε σε άτοπο.

Έστω $e \neq a \in G$. Τότε $\mathsf{o}(a) \mid pq$ και άρα $\mathsf{o}(a) = p$ ή q ή pq. Επειδή έχουμε υποθέσει ότι η G δεν έχει στοιχείο τάξης pq, θα έχουμε:

$$\forall a \in G \setminus \{e\}: \quad \mathsf{o}(a) = p \quad \text{ή} \quad q$$

(1) Έστω ότι η G έχει ένα στοιχείο a τάξης p. Τότε θα έχουμε την υποομάδα $H = \langle a \rangle$ της G τάξης p. Από το Πόρισμα 2.24 έπεται ότι η H είναι η μοναδική υποομάδα τάξης p της G.

Επομένως για κάθε $b \in G \setminus H$, θα έχουμε ότι η υποομάδα $K = \langle b \rangle$ έχει τάξη q. Πραγματικά, αν $\mathsf{o}(K) = p$, τότε θα πρέπει $H = K$ και άρα $b \in H$ το οποίο είναι άτοπο. Άρα επειδή η G δεν έχει στοιχείο τάξης pq έπεται ότι $\mathsf{o}(K) = q$.

Για ένα τέτοιο στοιχείο $b \in G \setminus H$ τάξης q, θεωρούμε το στοιχείο ab. Τότε: $\mathsf{o}(ab) \neq 1$, διότι διαφορετικά: $ab = e$ και άρα $b = a^{-1} \in H$ το οποίο είναι άτοπο. Αν $\mathsf{o}(ab) = p$, τότε όπως και πριν $\langle a \rangle = \langle ab \rangle$ και άρα $ab = a^k$ το οποίο δίνει $b = a^{k-1} \in H$ το οποίο είναι άτοπο. Άρα $\mathsf{o}(ab) = q$, και επομένως $(ab)^q = e$. Επειδή η G είναι αβελιανή, και επειδή $\mathsf{o}(b) = q$, θα έχουμε:

$$(ab)^q = a^q b^q = e \implies a^q = e$$

το οποίο είναι άτοπο διότι $\mathsf{o}(a) = p > q$. Άρα σ' αυτή την περίπτωση καταλήξαμε σε άτοπο.

(2) Έστω ότι η G δεν έχει κανένα στοιχείο τάξης p. Τότε όλα τα στοιχεία της G εκτός του ταυτοτικού έχουν τάξη q.

Έστω $e \neq a \in G$ και έστω $H = \langle a \rangle$. Τότε $\mathsf{o}(a) = q$. Διαλέγουμε ένα στοιχείο $b \in G \setminus H$ και θέτουμε $K = \langle b \rangle$. Τότε $\mathsf{o}(H) = q = \mathsf{o}(K)$.

Επειδή η G είναι αβελιανή έπεται άμεσα ότι το υποσύνολο $HK = KH$ είναι μια υποομάδα της G, και επομένως, επειδή προφανώς $\mathsf{o}(HK) > 1$, θα έχουμε:

$$\mathsf{o}(HK) \in \{p, q, pq\}$$

Αν $\mathsf{o}(HK) = p$, τότε η HK είναι κυκλική και άρα η G έχει ένα στοιχείο τάξης p το οποίο είναι άτοπο. Άρα $\mathsf{o}(HK) = q$ ή pq. Όμως από την Πρόταση 2.22, θα έχουμε:

$$\mathsf{o}(HK) = \frac{\mathsf{o}(H)\,\mathsf{o}(K)}{\mathsf{o}(H \cap K)} = \frac{q^2}{\mathsf{o}(H \cap K)} = q \quad \text{ή} \quad pq$$

Επομένως:

$$\mathsf{o}(H \cap K)p = q \quad \text{ή} \quad \mathsf{o}(H \cap K) = q$$

Όμως η περίπτωση $\mathsf{o}(H \cap K)p = q$ οδηγεί στο άτοπο $p \leq q$. Άρα μένει η περίπτωση $\mathsf{o}(H \cap K) = q$. Όμως επειδή $K \supseteq H \cap K \subseteq H$ και $\mathsf{o}(K) = \mathsf{o}(H \cap K) = q = \mathsf{o}(H)$ έπεται ότι $H \cap K = H$ και $H \cap K = K$. Τότε όμως $H = K$ κατι το οποίο είναι άτοπο διότι $K = \langle b \rangle$, όπου $b \neq H = \langle a \rangle$. □

Με χρήση περισσότερο προχωρημένων εργαλείων αποδεικνύεται τα ακόλουθα γενικότερα αποτελέσματα τα οποία περιγράφουν πλήρως τις ομάδες τάξης pq, όπου p, q είναι διακεκριμμένοι πρώτοι αριθμοί:

Θεώρημα 6.7. *Έστω G μια ομάδα τάξης pq, όπου p, q είναι πρώτοι αριθμοί, έτσι ώστε: $p < q$.*

(1) *Η G είναι κυκλική αν:*
   (α') *είτε η G είναι αβελιανή,*
   (β') *ή $p \nmid q - 1$.*

(2) *Αν η G είναι μη-αβελιανή, και $p \mid q - 1$, τότε η G παράγεται από ένα στοιχείο a τάξης p και ένα στοιχείο b τάξης q, έτσι ώστε: $a^{-1}ba = b^r$, όπου $q \mid r^p - 1$:*

$$G = \left\langle a, b \;\mid\; a^p = e = b^q \quad \textit{και} \quad a^{-1}ba = b^r \quad \textit{όπου} \quad q \mid r^p - 1 \right\rangle$$

Τι συμβαίνει αν $p = q$;

Θεώρημα 6.8. *Έστω G μια ομάδα τάξης p^2, όπου p είναι ένας πρώτος αριθμός. Τότε:*

(1) *Η G είναι αβελιανή.*

(2) *Η G είναι δομικά ίδια (ισόμορφη) με μια από τις ακόλουθες, δομικά διαφορετικές (μη-ισόμορφες), ομάδες:*

$$\mathbb{Z}_{p^2} \qquad \textit{ή} \qquad \mathbb{Z}_p \times \mathbb{Z}_p$$

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Ιωαννίνων**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Σημειώματα

Σημείωμα Αναφοράς

Copyright Πανεπιστήμιο Ιωαννίνων, Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης «Αλγεβρικές Δομές Ι». Έκδοση: 1.0. Ιωάννινα 2014. Διαθέσιμο από τη δικτυακή διεύθυνση: http://ecourse.uoi.gr/course/view.php?id=1248.