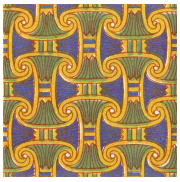
Βασική Άλγεβρα

Σημειώσεις Παραδόσεων και Ασκήσεις

Σεπτέμβριος 2021
ΜΜ



Περιεχόμενα

Οι περισσότερες ασκήσεις προέρχονται από διάφορα βιβλία αλγεβρας. Οι υπόλοιπες είναι πρωτότυπες ή προέρχονται από θέματα εξετάσεων του μαθήματος.

Τί άλλαξε από την προηγούμενη έκδοση (2020) των σημειώσεων;
Διορθώθηκαν τυπογραφικά λάθη και ασάφειες. Ευχαριστώ θερμά τους φοιτητές που τα εντόπισαν. Προστέθηκαν 3 νέες παραγράφους στα τέλη των Μερών I, II, III με Επαναληπτικές Ασκήσεις και λύσεις. Τέλος προστέθηκε το Κεφάλαιο 11 ΄Δράσεις ομάδων και θεωρήματα Sylow΄. Αυτό δεν είναι στη διδακτέα ύλη του μαθήματος, αλλά περιέχει πολύ σημαντικά αποτελέσματα της θεωρίας των πεπερασμένων ομάδων. Μπορεί να θεωρηθεί ως επιστέγασμα των Κεφαλαίων 7-10.

Η εικόνα στο εξώφυλλο των σημειώσεων αυτών αναφέρεται στο another brick in the wall των Pink Floyd ή στο εξώφυλλο των πρώτου άλμπουμ των Ramones;
Όχι. Η λύση του μυστηρίου υπάρχει στην άσκηση 9.30.

Βρήκα λάθος στις σημειώσεις, τι κάνω;
Αφού περάσει η ταραχή και αποκατασταθεί η ηρεμία, μπορείς να μου στείλεις σχετικό email στη διεύθυνση mmaliak[at]math.uoa.gr. Ο ευρών αμειφθήσεται με σοκολάτα υγείας, σοβαρά.

Συχνές Ερωτήσεις

Γιατί αυτή η σελίδα είναι ανάποδα;
Για να αυξηθούν οι πιθανότητες να τη διαβάσετε.

Ποιος ο σκοπός των σημειώσεων;
Ο σκοπός είναι
(1) όσοι παρακολουθούν, να ασχολούνται περισσότερο με την ουσία του τι γίνεται στην τάξη και να συμμετέχουν πιο ενεργά χωρίς το άγχος να κρατήσουν λεπτομερείς σημειώσεις, και
(2) όσοι δεν παρακολουθούν, να έχουν έναν αναλυτικό οδικό χάρτη του μαθήματος.
Στην τάξη σκοπεύω να ακολουθήσω τις σημειώσεις αυτές πιστά, θεωρία και ασκήσεις. Μάλιστα αυτές προέκυψαν από τη διδασκαλία του μαθήματος επί σειρά ετών στο Πανεπιστήμιο Αθηνών και αλλού.

Οι σημειώσεις αρκούν για το μάθημα ή πρέπει να διαβάσουμε κάποιο από τα προτεινόμενα συγγράμματα;
Οι σημειώσεις αρκούν για το μάθημά μου, **αλλά**: Και φυσικά πρέπει να μελετήσετε κάποιο καλό βιβλίο, όπως πχ το Algebra του M. Artin που είναι καταπληκτικό. Γιατί να περιοριστείτε σε κάποιες σημειώσεις και να μη δείτε τη σκοπιά και το εύρος που προσφέρει ένα εξαιρετικό βιβλίο; Και γιατί ένα μόνο;

Οι σημειώσεις έχουν πάνω από 330 ασκήσεις, χώρια τα παραδείγματα. Αναμένεις να τις λύσουμε όλες; Άλλη δουλειά δεν έχουμε;
Ακολουθεί μακροσκελής απάντηση. Πριν δεκαετίες, το σύνηθες στα ελληνικά ΑΕΙ (τουλάχιστον στα τμήματα Μαθηματικών) ήταν να υπάρχουν μαζικά τμήματα διδασκαλίας της θεωρίας με 3-4 ώρες την εβδομάδα μάθημα. Παράλληλα υπήρχαν μικρότερα τμήματα φροντιστηριακών ασκήσεων με 2-3 ώρες την εβδομάδα, όπου, έκπληξη-έκπληξη, λύνονταν ασκήσεις πάνω στην ύλη που καλύφθηκε στη θεωρία. Αργότερα με την εισαγωγή των εξαμήνων, το τμήμα θεωρίας και τα τμήματα ασκήσεων συγχωνεύτηκαν σε ενιαίο μάθημα και έτσι προέκυψαν τα υποχρεωτικά μαθήματα του προγράμματος σπουδών του Μαθηματικού διάρκειας 6 ωρών. Το συμπέρασμα είναι ότι στο 6ωρο αυτό, πρέπει να γίνονται και ασκήσεις. Είναι μεγάλος ο πειρασμός να ασχολούμαστε μόνο με θεωρία, αλλά ως εισαγωγικό μάθημα σε συγκεκριμένο ευρύ κλάδο των μαθηματικών, οι ασκήσεις κατά τη γνώμη μου είναι ακέραιο κομμάτι του μαθήματος. Αν προτιμάτε εξάωρο χωρίς ασκήσεις, τότε θα απογοητευθείτε στο μάθημά μου. Αν περιμένετε ασκησιολογία με υποβάθμιση της θεωρίας, πάλι θα απογοητευθείτε. Σε πολλά καλά πανεπιστήμια της Ευρώπης και Β. Αμερικής διατηρούν το δϋϊσμό θεωρία και ασκήσεις - δεν τονίζω το διαχωρισμό αλλά την ύπαρξη ασκήσεων. Για παράδειγμα στο HB γίνεται ουσιαστική δουλειά στα tutorials σχεδόν σε 1-1 βάση. Σε εμάς, αυτές οι ώρες έχουν ενσωματωθεί στο εξάωρο. Είμαι της γνώμης ότι χωρίς σοβαρή ενασχόληση με ασκήσεις, η κατανόηση στα προπτυχιακά μαθηματικά καθίσταται σαφώς πιο δύσκολη για την πλειονότητα των φοιτητών.
Για τις συγκεκριμένες ασκήσεις των σημειώσεων: Προέκυψαν προσθέτοντας ασκήσεις σε αυτές που συνήθως κάνω στην τάξη. Άρα συμπεριλαμβάνονται περισσότερες ασκήσεις από όσες μπορούν σε λογικά πλαίσια να λυθούν στο μάθημα. Είναι για δική σας εξάσκηση και ευχαρίστηση, ή αγνόηση. Η συμβουλή μου είναι (αν ακόμα διαβάζετε μέχρι εδώ) να δοκιμάζετε μόνοι σας πολλές ασκήσεις. Πιάστε χαρτί και μολύβι. Να καταφεύγετε στις λύσεις ή υποδείξεις, μόνο μετά από σοβαρή προσπάθεια. Πολλές ασκήσεις λύνονται με διάφορους τρόπους, βρείτε δικό σας.
Ασκήσεις που φέρουν το σημάδι $\star$ χρησιμοποιούνται παρακάτω (στο κυρίως κείμενο ή σε άλλες ασκήσεις). Έχει γίνει ομαδοποίηση των ασκήσεων με βάση τη δυσκολία τους κατά την υποκειμενική κρίση μου. Η Ομάδα m περιλαμβάνει πιο εύκολες από την Ομάδαn αν $m < n$. Οι ασκήσεις από την Ομάδα3 υπερβαίνουν σε δυσκολία τα ερωτήματα των τελικών εξετάσεων. Οι δυσκολότερες από όλες φέρουν το σημάδι $\wr$.

Μέρος 1

Ακέραιοι

Διαιρετότητα

Στο Μέρος 1 (Κεφάλαια 1 και 2) μελετάμε ιδιότητες των ακεραίων που θα χρησιμοποιήσουμε συχνά παρακάτω. Επίσης θα εισάγουμε στην ειδική περίπτωση των ακεραίων μερικές σημαντικές έννοιες που θα μελετήσουμε πιο γενικά στα επόμενα κεφάλαια.

Ο σκοπός μας στο Κεφάλαιο 1 είναι να αναπτύξουμε τα πλέον βασικά στοιχεία από τη διαιρετότητα στους ακέραιους, με έμφαση στην έννοια του μέγιστου κοινού διαιρέτη, το θεμελιώδες θεώρημα της αριθμητικής και τον Ευκλείδειο αλγόριθμο.

Βασικά σημεία

- διαιρετότητα
- Ευκλείδεια διαίρεση
- μέγιστος κοινός διαιρέτης, λήμμα του Ευκλείδη
- θεμελιώδες θεώρημα της Αριθμητικής

1.1. Διαιρετότητα, Ευκλείδεια διαίρεση, πρώτοι

Θα συμβολίζουμε με

$$\mathbb{N} = \{0, 1, 2, \cdots\}$$

$$\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\},$$

$$\mathbb{Z}_{>0} = \{m \in \mathbb{Z} : m > 0\},$$

$$\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\},$$

$$\mathbb{R}$$

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

τα σύνολα των φυσικών αριθμών, ακέραιων αριθμών, θετικών ακέραιων αριθμών, ρητών αριθμών, πραγματικών αριθμών και μιγαδικών αριθμών αντίστοιχα. Θεωρούμε γνωστές τις βασικές ιδιότητες των συνήθων αριθμητικών πράξεων στα σύνολα αυτά όπως και της διάταξης στο $\mathbb{R}$.

Αξίωμα *(Αξίωμα Ελαχίστου) Κάθε μη-κενό υποσύνολο του* $\mathbb{N}$ *έχει ελάχιστο στοιχείο.*

Δηλαδή αν $A \subseteq \mathbb{N}$ και $A \neq \emptyset$, τότε υπάρχει $a \in A$ τέτοιο ώστε $a \leq x$ για κάθε $x \in A$. Αντίστοιχη ιδιότητα στο $\mathbb{Q}$ δεν ισχύει καθώς το υποσύνολο

$$\{1, \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, ...\}$$

του $\mathbb{Q}$ δεν έχει ελάχιστο στοιχείο.

Ορισμός 1.1. *Έστω $a, b \in \mathbb{Z}$. Αν υπάρχει $c \in \mathbb{Z}$ με $b = ac$, θα λέμε ότι το a **διαιρεί** το b (ή ότι το a είναι **διαιρέτης** του b) και θα γράφουμε $a|b$.*

Παρατηρούμε ότι $a|0$, για κάθε $a \in \mathbb{Z}$. Ειδικά $0|0$.

Λήμμα 1.2. *Έστω $a, b, c \in \mathbb{Z}$.*
(1) *Αν $a|b$ και $b|c$, τότε $a|c$.*
(2) *Αν $a|b$ και $a|c$, τότε $a|xb + yc$ για κάθε $x, y \in \mathbb{Z}$.*
(3) *Αν $a|b$ και $b|a$, τότε $a = \pm b$.*

Απόδειξη. Ας αποδείξουμε ενδεικτικά το (3) Αφού $a|b$ και $b|a$ υπάρχουν $x, y \in \mathbb{Z}$ ώστε $b = ax$ και $a = by$. Επομένως

$$b = byx.$$

Αν $b = 0$, τότε από $b|a$, έπεται ότι $a = 0$. Αν $b \neq 0$, τότε $1 = yx$, δηλαδή $y = \pm 1$ καθώς οι x, y είναι ακέραιοι. Επομένως $a = \pm b$. □

Ορισμός 1.3. *Ένας ακέραιος $p > 1$ λέγεται **πρώτος** αν οι μόνοι διαιρέτες του είναι οι ± 1 και $\pm p$.*

Για παράδειγμα, οι πρώτοι μικρότεροι του 20 είναι οι $2, 3, 5, 7, 11, 13, 17, 19$.

Πρόταση 1.4. *Κάθε ακέραιος $a > 1$ είναι πρώτος ή γινόμενο πρώτων.*

Απόδειξη. Υποθέτουμε ότι η πρόταση δεν ισχύει. Έστω M το σύνολο των ακεραίων $a > 1$ που δεν είναι πρώτοι και ούτε γράφονται ως γινόμενο πρώτων. Τότε $M \neq \emptyset$. Από το Αξίωμα Ελαχίστου υπάρχει ελάχιστο στοιχείο στο M, έστω m . Αφού ο m δεν είναι πρώτος, υπάρχουν $b, c \in \mathbb{Z}$ με

$$m = bc, 1 < b, c < m.$$

Από τον ορισμό του m έπεται ότι οι b, c δεν ανήκουν στο M. Όμως $b, c > 1$. Άρα καθένας από τους b, c είναι γινόμενο πρώτων. Τότε και ο $m = bc$ είναι γινόμενο πρώτων. Αυτό είναι άτοπο αφού $m \in M$. □

Θεώρημα 1.5 (Ευκλείδης)**.** *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Έστω ότι το σύνολο των πρώτων είναι πεπερασμένο και ότι είναι το $\{p_1, \cdots, p_k\}$. Θέτουμε

$$N = p_1 p_2 \cdots p_k + 1.$$

Τότε $N > 1$ και από την Πρόταση 1.4 έπεται ότι $p_i|N$ για κάποιο $i \in \{1, 2, \cdots, k\}$. Επειδή $p_i|p_1 p_2 \cdots p_k$, από το Λήμμα 1.2 παίρνουμε

$$p_i|N - p_1 p_2 \cdots p_k.$$

Επομένως $p_i|1$, άτοπο. □

Θεώρημα 1.6 (Ευκλείδεια διαίρεση)**.** *Έστω $a, b \in \mathbb{Z}$ με $a \neq 0$. Τότε υπάρχουν μοναδικοί $q, r \in \mathbb{Z}$ ώστε $b = qa + r$ και $0 \leq r < |a|$.*

Ορισμός 1.7. *Το r (αντίστοιχα q) στο παραπάνω θεώρημα λέγεται το* **υπόλοιπο** *(αντίστοιχα* **πηλίκο***) της διαίρεσης του b με το a.*

Για παράδειγμα, έχουμε

$$44 = 7 \cdot 6 + 2,$$

το υπόλοιπο της διαίρεσης του 44 με το 6 είναι 2 και το πηλίκο 7. Επίσης το υπόλοιπο της διαίρεσης του 44 με το 7 είναι 2 και το πηλίκο 6.

Απόδειξη του Θεωρήματος 1.6.
Ύπαρξη. Έστω

$$M = \{b - t|a| \geq 0 : t \in \mathbb{Z}\}.$$

Το M είναι μη κενό υποσύνολο του $\mathbb{N}$ (γιατί;) και επομένως από το Αξίωμα Ελαχίστου έχει ελάχιστο στοιχείο, έστω r. Επειδή $r \in M$, έχουμε $r \geq 0$ και υπάρχουν $a, b, q \in \mathbb{Z}$ με $r = b - q|a|$.

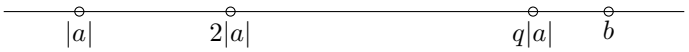
Έστω ότι $r \geq |a|$. Τότε

$$b - q|a| \geq |a| \implies b - (q+1)|a| \geq 0 \implies b - (q+1)|a| \in M.$$

Από τον ορισμό του r έχουμε ότι

$$b - (q+1)|a| \geq r \implies r - |a| \geq r \implies -|a| \geq 0,$$

που είναι αδύνατο. Άρα $r < |a|$.



Σχήμα 1. Ο ακέραιος q έχει την ιδιότητα ότι ο ακέραιος $b - q|a|$ είναι μη αρνητικός και ελάχιστος.

Μοναδικότητα. Έστω ότι υπάρχουν $q, r, q_1, r_1 \in \mathbb{Z}$ με

$$b = qa + r, \quad 0 \leq r < |a|,$$
$$b = q_1 a + r_1, \quad 0 \leq r_1 < |a|.$$

Αφαιρώντας παίρνουμε $(q - q_1)a = r_1 - r$ και $-|a| < r_1 - r < |a|$. Επομένως

$$-|a| < (q - q_1)a < |a|.$$

Άρα $-1 < q_1 - q < 1$ και επειδή $q_1 - q \in \mathbb{Z}$, έπεται ότι $q = q_1$. Συνεπώς $r = r_1$.

□

1.2. Μέγιστος κοινός διαιρέτης

Ορισμός 1.8. *Έστω $a, b \in \mathbb{Z}$ όχι και οι δύο 0. Ένας* **μέγιστος κοινός διαιρέτης** *των a, b είναι ένας θετικός ακέραιος d που έχει τις εξής ιδιότητες.*

(1) *$d|a$ και $d|b$.*
(2) *Αν $c \in \mathbb{Z}$ με $c|a$ και $c|b$, τότε $c|d$.*

Θεώρημα 1.9. *Έστω $a, b \in \mathbb{Z}$ όχι και οι δύο μηδέν. Τότε υπάρχει μοναδικός μκδ των a και b (συμβολίζουμε $d = \text{μκδ}(a, b)$). Επίσης υπάρχουν $x, y \in \mathbb{Z}$ ώστε*

$$d = ax + by$$

Απόδειξη. Έστω

$$M = \{ax + by > 0 : x, y \in \mathbb{Z}\}.$$

Επειδή το M είναι μη κενό υποσύνολο του $\mathbb{N}$, από το Αξίωμα Ελαχίστου το M έχει ελάχιστο στοιχείο, έστω d. Τότε υπάρχουν $x, y \in \mathbb{Z}$ με

$$d = ax + by.$$

Ισχυρισμός 1. $d|a$ και $d|b$.

Πράγματι, από Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ ώστε

$$a = qd + r, \quad 0 \leq r < d.$$

Έχουμε

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Έστω ότι $r \neq 0$, οπότε $r \in M$. Από τον ορισμό του d έπεται ότι $r \geq d$. Αυτό είναι αδύνατο αφού $r < d$. Επομένως $r = 0$, άρα $a = qd$, δηλαδή $d|a$. Ομοίως αποδεικνύεται ότι $d|b$.

Ισχυρισμός 2. Αν $c|a$ και $c|b$, τότε $c|d$.

Πράγματι αφού $c|a$ και $c|b$, έπεται ότι $c|ax + by = d$.

Από τους δύο παραπάνω ισχυρισμούς παίρνουμε ότι το d είναι μκδ των a και b.

Θα δείξουμε τώρα τη μοναδικότητα. Έστω d, d_1 δύο μκδ των a και b. Τότε $d|a$, $d|b$. Αφού d_1 είναι μκδ των a και b, έπεται ότι $d|d_1$. Ομοίως έχουμε $d_1|d$. Επειδή οι d, d_1 είναι θετικοί ακέραιοι, έχουμε $d = d_1$. □

Ορισμός 1.10. *Δύο ακέραιοι a, b λέγονται* ***σχετικά πρώτοι*** *αν $\mu\kappa\delta(a, b) = 1$.*

Μια σημαντική εφαρμογή της παράστασης $\mu\kappa\delta(a, b) = ax + by$ του προηγούμενου θεωρήματος είναι το Λήμμα του Ευκλείδη.

Λήμμα 1.11 (Ευκλείδης). *Έστω p πρώτος και $a, b \in \mathbb{Z}$. Αν $p|ab$, τότε $p|a$ ή $p|b$.*

Απόδειξη. Έστω ότι ο p δεν διαιρεί τον a. Τότε επειδή ο p είναι πρώτος, έχουμε $1 = \mu\kappa\delta(p, a)$. Από το Θεώρημα 1.9 υπάρχουν $x, y \in \mathbb{Z}$ ώστε $1 = px + ay$. Επομένως

$$b = bpx + aby.$$

Επειδή $p|bpx$ και $p|aby$, έπεται ότι και p διαιρεί το δεξιό σκέλος και άρα το αριστερό, δηλαδή p διαιρεί το b. □

Θεώρημα 1.12 (Θεμελιώδες θεώρημα της Αριθμητικής). *Έστω $a \in \mathbb{Z}, a > 1$. Τότε υπάρχουν μοναδικοί πρώτοι $p_1, \cdots p_m$ ώστε*

$$a = p_1 p_2 \cdots p_m$$

(χωρίς να λαμβάνεται υπόψη η σειρά των p_i).

Απόδειξη. Η ύπαρξη έχει αποδειχθεί στην Πρόταση 1.4. Για τη μοναδικότητα, έστω πρώτοι $p_1, \ldots, p_m$, $q_1, \ldots q_n$ με

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n.$$

Υποθέτουμε χωρίς περιορισμό της γενικότητας ότι $m \leq n$ και εφαρμόζουμε επαγωγή στο m.

Για $m = 1$ έχουμε $p_1 = q_1 q_2 \cdots q_n$, οπότε σύμφωνα με τον ορισμό του πρώτου, έχουμε $n = 1$.

Έστω $m > 1$. Από την ισότητα $p_1 \cdots p_m = q_1 \cdots q_n$, παίρνουμε από το Λήμμα του Ευκλείδη ότι ο p_1 διαιρεί κάποιον από τους q_j, έστω τον q_1 (μετά ενδεχομένως από αναδιάταξη των q_j). Επειδή ο q_1 είναι πρώτος και $p_1 > 1$, παίρνουμε $p_1 = q_1$.Άρα

$$p_2 \cdots p_m = q_2 \cdots q_n.$$

Από την επαγωγική υπόθεση έπεται ότι $m - 1 = n - 1$ και τα $q_2, \ldots, q_n$ είναι αναδιάταξη των $p_2, \ldots p_n$. Τελικά έχουμε ότι $m = n$ και τα $q_1, \ldots, q_n$ είναι αναδιάταξη των $p_1, \ldots p_n$. □

Παρατηρήσεις.

(1) Το θεμελιώδες θεώρημα της Αριθμητικής λέει ότι κάθε $a \in \mathbb{Z}, a \neq 0, \pm 1$ γράφεται μοναδικά στην μορφή $a = \pm p_1^{a_1} \cdots p_m^{a_m}$, όπου οι p_i είναι ανά δύο διαφορετικοί πρώτοι αριθμοί και οι a_i είναι θετικοί αριθμοί. Την παράσταση αυτή θα ονομάζουμε **την ανάλυση του a σε γινόμενο πρώτων**.

(2) Αν $a, b \in \mathbb{Z}$ είναι μη μηδενικοί, τότε μπορούμε να γράψουμε

$$a = \pm p_1^{a_1} \cdots p_m^{a_m}, \quad b = \pm p_1^{b_1} \cdots p_m^{b_m},$$

όπου οι p_i είναι ανά δύο διαφορετικοί πρώτοι αριθμοί και οι a_i, b_i είναι **θετικοί ή 0**.

(3) Με τον προηγούμενο συμβολισμό έχουμε $a|b \Leftrightarrow a_i \leq b_i \ \forall i$.
Πράγματι, έστω ότι $a|b$. Τότε υπάρχει $c \in \mathbb{Z}$ ώστε $b = ac$. Έστω

$$c = p_1^{c_1} \cdots p_k^{c_k}, \quad c_i \in \mathbb{N}.$$

Τότε $p_1^{b_1} \cdots p_k^{b_k} = p_1^{a_1+c_1} \cdots p_k^{a_k+c_k}$. Από την μοναδικότητα στο θεμελιώδες θεώρημα της Αριθμητικής έπεται ότι $b_i = a_i + c_i$ για κάθε i, άρα $a_i \leq b_i$.

Αντίστροφα, έστω $a_i \leq b_i$ για κάθε i. Θέτουμε $c = p_1^{c_1} \cdots p_k^{c_k}$, όπου $c_i = b_i - a_i \in \mathbb{N}$. Τότε $b = ac$ και $a|b$.

Πρόταση 1.13. *Έστω*

$$a = \pm p_1^{a_1} \cdots p_m^{a_m}, \ b = \pm p_1^{b_1} \cdots p_m^{b_m},$$

όπου οι p_i είναι ανά δύο διαφορετικοί πρώτοι αριθμοί και $a_i, b_i \geq 0$. Θέτοντας $d_i = min\{a_i, b_i\}$ έχουμε ότι

$$\mu\kappa\delta(a, b) = p_1^{d_1} ... p_m^{d_m}.$$

Απόδειξη. Άσκηση. □

Για παράδειγμα,

$$\mu\kappa\delta(45, 735) = \mu\kappa\delta(3^2 \cdot 5^1 \cdot 7^0, 3^1 \cdot 5^1 \cdot 7^2) = 3^1 \cdot 5^1 \cdot 7^0 = 15.$$

Ελάχιστο κοινό πολλαπλάσιο

Με το συμβολισμό της προηγούμενης πρότασης, έστω $e_i = max\{a_i, b_i\}$. Ο ακέραιος $p_1^{e_1} ... p_m^{e_m}$ ονομάζεται το **ελάχιστο κοινό πολλαπλάσιο** των a, b και συμβολίζεται με $\varepsilon\kappa\pi(a, b)$.

Για παράδειγμα,

$$\varepsilon\kappa\pi(45, 735) = \varepsilon\kappa\pi(3^2 \cdot 5^1 \cdot 7^0, 3^1 \cdot 5^1 \cdot 7^2) = 3^2 \cdot 5^1 \cdot 7^2 = 2205.$$

Σημειώνουμε ότι το $\varepsilon\kappa\pi(a, b)$ έχει τις εξής ιδιότητες, οι αποδείξεις των οποίων αφήνονται ως άσκηση:

- το $\varepsilon\kappa\pi(a, b)$ είναι θετικός ακέραιος,
- $a|\varepsilon\kappa\pi(a, b)$ και $b|\varepsilon\kappa\pi(a, b)$,
- Αν $a|c$ και $b|c$, τότε $\varepsilon\kappa\pi(a, b)|c$.

Πρόταση 1.14. *Αν a, b είναι θετικοί ακέραιοι, τότε*

$$\mu\kappa\delta(a, b) \cdot \varepsilon\kappa\pi(a, b) = ab.$$

Απόδειξη. Έπεται άμεσα από τη σχέση

$$min\{a_i, b_i\} + max\{a_i, b_i\} = a_i + b_i,$$

την Πρόταση 1.13 και τον ορισμό του εκπ. □

1.3. Ευκλείδειος Αλγόριθμος

Με τον Ευκλείδειο αλγόριθμο, που θα εξηγήσουμε στη συνέχεια, μπορούμε να υπολογίσουμε, μεταξύ των άλλων, το $\mu\kappa\delta(a,b)$ όπως και μια επιλογή ακεραίων x, y με $\mu\kappa\delta(a,b) = ax + by$.

Παρατηρούμε τα εξής.

(1) Αν $b = aq + r$, τότε $\mu\kappa\delta(a,b) = \mu\kappa\delta(r,a)$.

Πράγματι, αφού $\mu\kappa\delta(a,b)|a$ και $\mu\kappa\delta(a,b)|b$, παίρνουμε $\mu\kappa\delta(a,b)|r$. Δηλαδή $\mu\kappa\delta(a,b)|a$ και $\mu\kappa\delta(a,b)|r$, άρα

$$\mu\kappa\delta(a,b)|\mu\kappa\delta(r,a).$$

Ομοίως έχουμε $\mu\kappa\delta(r,a)|\mu\kappa\delta(a,b)$. Επομένως $\mu\kappa\delta(a,b) = \mu\kappa\delta(r,a)$.

(2) **Ευκλείδειος Αλγόριθμος** Έστω $a > 0$. Εφαρμόζουμε Ευκλείδεια διαίρεση διαδοχικά μέχρι να βρούμε υπόλοιπο 0,

$$\begin{aligned} b &= aq + r, \quad 0 < r < a \\ a &= rq_1 + r_1, \quad 0 < r_1 < r \\ r &= r_1q_2 + r_2, \quad 0 < r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_nq_{n+1} + 0. \end{aligned}$$

Εφαρμόζοντας το (1) διαδοχικά έχουμε ότι

$$\mu\kappa\delta(a,b) = \mu\kappa\delta(r,a) = \mu\kappa\delta(r,r_1) = \cdots = \mu\kappa\delta(r_n,0) = r_n,$$

το οποίο είναι το τελευταίο μη μηδενικό υπόλοιπο.

(3) Στη διαδικασία του (2) θα βρούμε πράγματι $r_{n+1} = 0$ μετά κάποιο πεπερασμένο πλήθος Ευκλείδειων διαιρέσεων γιατί έχουμε μια γνησίως φθίνουσα ακολουθία φυσικών αριθμών $a > r > r_1 > r_2 > \cdots$ με αρχικό όρο το a.

Παράδειγμα 1.15. Έστω $a = 165$ και $b = 418$. Από τον Ευκλείδειο αλγόριθμο έχουμε

$$\begin{aligned} 418 &= 2 \cdot 165 + 88 \\ 165 &= 1 \cdot 88 + 77 \\ 88 &= 1 \cdot 77 + 11 \\ 77 &= 7 \cdot 11 + 0. \end{aligned}$$

Άρα μκδ(165, 418)=11. Τώρα θα βρούμε $x, y \in \mathbb{Z}$ ώστε $11 = 165x + 418y$. Με διαδοχικές αντικαταστάσεις των *υπολοίπων* από κάτω προς τα πάνω έχουμε,

$$\begin{aligned} 11 &= 88 - 1 \cdot 77 = 88 - 1(165 - 1 \cdot 88) \\ &= 2 \cdot 88 - 1 \cdot 165 = 2(418 - 2 \cdot 165) - 1 \cdot 165 \\ &= 165(-5) + 418 \cdot 2. \end{aligned}$$

Άρα ένα ζεύγος (x, y) είναι το $(-5, 2)$.

Παρατήρηση. Τα x, y στην παράσταση $\mu\kappa\delta(a,b) = ax + by$ δεν είναι μοναδικά καθώς για κάθε $t \in \mathbb{Z}$ έχουμε

$$ax + by = a(x - tb) + b(y + ta).$$

Ασκήσεις Κεφαλαίου 1

Ομάδα1: 1-9, 17.
Ομάδα2: 10-16.
Ομάδα3:- .

1. Αποδείξτε την Πρόταση 1.13.
2. ⋆ Δείξε ότι $\sqrt{2} \notin \mathbb{Q}$. Γενικά αν ο θετικός ακέραιος a δεν είναι το τετράγωνο ακεραίου, τότε $\sqrt{a} \notin \mathbb{Q}$.
3. ⋆ Έστω $a, b, c \in \mathbb{Z}$ με $\mu\kappa\delta(a, b) = 1$. Δείξτε ότι ισχύουν τα ακόλουθα.
   i) Αν $a|bc$, τότε $a|c$.
   ii) Αν $a|c$ και $b|c$, τότε $ab|c$.
   iii) $\mu\kappa\delta(a, bc) = \mu\kappa\delta(a, c)$
4. Έστω $a, b \in \mathbb{Z}_{>0}$ με $a^3|b^7$. Δείξτε ότι $a|b^3$.
5. Ποιο είναι το ελάχιστο στοιχείο του συνόλου $\{165x + 418y > 0 : x, y \in \mathbb{Z}\}$ και ποιο το μέγιστο στοιχείο του $\{21x + 77y < 0 : x, y \in \mathbb{Z}\}$;
6. Δείξτε ότι αν $\mu\kappa\delta(m, n) = 1$, τότε $\mu\kappa\delta(m + n, mn) = 1$. Αληθεύει το αντίστροφο;
7. Δείξτε ότι αν $\mu\kappa\delta(m, n) = 1$, τότε $\mu\kappa\delta(a, mn) = \mu\kappa\delta(a, m)\mu\kappa\delta(a, n)$ για κάθε $a \in \mathbb{Z}_{>0}$.
8. Δείξτε ότι υπάρχει μοναδική τριάδα της μορφής $(p, p + 2, p + 4)$, όπου οι $p, p + 2, p + 4$ είναι πρώτοι.
9. Βρείτε το $\mu\kappa\delta(3n+1, 10n+3)$, για κάθε $n \in \mathbb{N}$. Στη συνέχεια δείξτε ότι για κάθε $m, n \in \mathbb{Z}$ υπάρχουν $x, y \in \mathbb{Z}$ με $(3n + 1)x + (10n + 3)y = m$.
10. Έστω a, m, n θετικοί ακέραιοι με $m > n$.
    i) Δείξτε ότι $a^{2^n} + 1 | a^{2^m} - 1$.
    ii) Βρείτε το $\mu\kappa\delta(a^{2^n} + 1, a^{2^m} + 1)$.
11. Να βρεθούν όλοι οι πρώτοι p, q τέτοιοι ώστε $49p + 72q = pq^2$.
12. Έστω $a, b, n \in \mathbb{Z}_{>0}$, με $n > 1$, και $d = \mu\kappa\delta(a, b)$. Τότε $\mu\kappa\delta(n^a - 1, n^b - 1) = n^d - 1$.
13. Δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $6k + 5$, $k \in \mathbb{N}$.
    Σημείωση. Το φημισμένο θεώρημα του Dirichlet λέει ότι σε κάθε αριθμητική πρόοδο $ak + b, k \in \mathbb{N}$, όπου a, b σχετικά πρώτοι, περιέχονται άπειροι πρώτοι.
14. (Δυαδική παράσταση) Έστω $n \in \mathbb{N}$. Δείξτε ότι υπάρχουν $t \in \mathbb{N}$ και $a_0, ..., a_t \in \{0, 1\}$ με $n = a_t 2^t + ... + a_1 2 + a_0$. Επιπλέον δείξτε ότι οι $t, a_0, ...a_t$ είναι μοναδικά καθορισμένοι από το n. Βρείτε τη δυαδική παράσταση του 100.
    Αν $b > 1$ είναι ακέραιος, δείξτε ότι υπάρχουν μοναδικοί $t \in \mathbb{N}$ και $a_0, ..., a_t \in \{0, 1, ..., b-1\}$ με $n = a_t b^t + ... + a_1 b + a_0$. (Όταν $b = p$ πρώτος, η προηγούμενη παράσταση λέγεται η p-αδική παράσταση του n.)
15. (Αρχή της μαθηματικής επαγωγής) Χρησιμοποιώντας το αξίωμα ελαχίστου, δείξτε το εξής. Έστω $A \subseteq \mathbb{N}$ τέτοιο ώστε (1) $0 \in A$ και (2) αν $m - 1 \in A$, τότε $m \in A$. Τότε $A = \mathbb{N}$.
16. Έστω $n > 1$ ακέραιος. Δείξτε ότι ο n είναι πρώτος αν και μόνο αν για κάθε ακέραιο a ισχύει ότι $n|a$ ή $\mu\kappa\delta(n, a) = 1$.
17. Έστω a, b, c ακέραιοι. Είναι δυνατό το πλήθος των πρώτων αριθμών που ανήκουν στο σύνολο $\{ax + by + cz : x, y, z \in \mathbb{Z}\}$ να ισούται με 2021;

Υποδείξεις Κεφαλαίου 1

1. *Υπόδειξη.* Δείξτε ότι ο ακέραιος $p_1^{d_1}...p_m^{d_m}$ ικανοποιεί τις ιδιότητες στον ορισμό του μκδ των a και b.

2. *Λύση.* Υποθέτουμε ότι $\sqrt{2} \in \mathbb{Q}$ και έστω $\sqrt{2} = \frac{m}{n}$, με $m, n \in \mathbb{Z}, n \neq 0$. Μπορούμε να υποθέσουμε ότι $\mu\kappa\delta(m,n) = 1$ (αν όχι απλοποιούμε το κλάσμα). Έστω ότι υπάρχει p πρώτος με $p|n$. Επειδή $m^2 = 2n^2$ και $p|n$, έχουμε $p|m^2$. Αφού ο p είναι πρώτος, το Λήμμα του Ευκλείδη δίνει ότι $p|m$. Δηλαδή $p|m$ και $p|n$, άρα $p|\mu\kappa\delta(m,n)$. Επομένως $p|1$, το οποίο είναι άτοπο. Άρα $n = \pm 1$. Τότε $\sqrt{2} = \pm m \in \mathbb{Z}$, που είναι άτοπο.
Ο δεύτερος ισχυρισμός της εκφώνησης αποδεικνύεται με παρόμοιο τρόπο.

3. *Λύση.* Αφού $\mu\kappa\delta(a,b) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ ώστε $1 = ax + by$, άρα

$$c = acx + bcy.$$

(i) Παρατηρούμε ότι $a|a$ και $a|bc$. Επομένως $a|acx + bcy = c$.
(ii) Αφού $a|c$ και $b|c$, έχουμε $ab|acx$ και $ab|bcy$. Επομένως $ab|acx + bcy = c$.
(iii) Έχουμε $\mu k\delta(a,bc)|a$ και $\mu k\delta(a,bc)|bc$. Επειδή οι a, b είναι σχετικά πρώτοι, οι $\mu k\delta(a,bc), b$ είναι σχετικά πρώτοι. Το (i) δίνει $\mu k\delta(a,bc)|c$. Συνεπώς $\mu k\delta(a,bc)|\mu k\delta(a,c)$. Στην άλλη κατεύθυνση έχουμε ότι ο $\mu k\delta(a,c)$ διαιρεί τους a, c, άρα και τους a, bc. Συνεπώς $\mu k\delta(a,c)|\mu k\delta(a,bc)$. Άρα $\mu k\delta(a,bc) = \mu k\delta(a,c)$ καθώς είναι θετικοί.

4. *Λύση.* Έστω $a = p_1^{a_1} \cdots p_k^{a_k}$ και $b = p_1^{b_1} \cdots p_k^{b_k}$, όπου p_i πρώτοι με $p_i \neq p_j$ για κάθε $i \neq j$ και $a_i, b_i \in \mathbb{N}$. Άρα

$$a^3 = p_1^{3a_1} \cdots p_k^{3a_k} \text{ και } b^7 = p_1^{7b_1} \cdots p_k^{7b_k}.$$

Αφού $a^3|b^7$, από την Πρόταση 1.13 (που είναι βέβαιο ότι την αποδείξτε στην άσκηση 1.1), έπεται ότι $3a_i \leq 7b_i$. Επομένως $a_i \leq \frac{7}{3}b_i \leq 3b_i$, για κάθε i. Πάλι από την Πρόταση 1.13 παίρνουμε ότι $a|b^3$.

5. Υπόδειξη: Βλ. Θεώρημα 1.9 και την απόδειξή του.

6. *Λύση.* Υποθέτουμε ότι υπάρχει p πρώτος με $p|\mu\kappa\delta(m+n, mn)$. Τότε $p|m+n$ και $p|mn$. Επειδή ο p είναι πρώτος και $p|mn$ έπεται ότι $p|m$ ή $p|n$.
Έστω ότι $p|m$. Επειδή $p|m+n$, έχουμε $p|n$. Επομένως $p|m$ και $p|n$, οπότε έχουμε $p|\mu\kappa\delta(m,n) = 1$, άτοπο. Ομοίως, αν $p|n$ καταλήγουμε σε άτοπο, οπότε $\mu\kappa\delta(m+n, mn) = 1$.

7. *Λύση.* Έστω $d = \mu\kappa\delta(a, mn), d_1 = \mu\kappa\delta(a,m), d_2 = \mu\kappa\delta(a,n)$. Θα δείξουμε ότι $d = d_1d_2$.
Επειδή το d_1 είναι κοινός διαιρέτης των a, mn, έχουμε $d_1|d$. Όμοια $d_2|d$. Σύμφωνα με την άσκηση 1.3 ii), οι σχέσεις αυτές δίνουν $d_1d_2|d$ γιατί οι d_1, d_2 είναι σχετικά πρώτοι καθώς $d_1|m$, $d_2|n$ και οι m, n είναι σχετικά πρώτοι. Εφαρμόζοντας το Θεώρημα 1.9 δύο φορές, υπάρχουν ακέραιοι x_i, y_i με $d_1 = x_1a + y_1m$, $d_2 = x_2a + y_2n$. Πολλαπλασιάζοντας κατά μέλη λαμβάνουμε παράσταση της μορφής

$$d_1d_2 = za + z'(mn),\ z, z' \in \mathbb{Z}.$$

Από αυτή έπεται ότι $d|d_1d_2$.
Επειδή οι ακέραιοι d, d_1d_2 είναι θετικοί, παίρνουμε $d = d_1d_2$.

8. *Λύση.* Παρατηρούμε ότι για $p = 3$ έχουμε την τριάδα $(3,5,7)$. Έστω $p > 3$, p πρώτος. Από την Ευκλείδεια διαίρεση έχουμε $p = 3q$ ή $p = 3q+1$ ή $p = 3q+2$, με $q \in \mathbb{N}$. Όμως $p \neq 3q$, αφού $p \neq 3$.
Έστω $p = 3q+1$. Τότε $p+2 = 3q+1+2 = 3(q+1)$, ο οποίος δεν είναι πρώτος.
Έστω $p = 3q+2$. Τότε $p+4 = 3q+2+4 = 3(q+2)$, ο οποίος δεν είναι πρώτος.

9. *Λύση.* Έχουμε

$$\begin{aligned} 10n+3 &= 3(3n+1)+n \\ 3n+1 &= 3n+1 \\ n &= 1n+0. \end{aligned}$$

Επομένως $\mu\kappa\delta(3n+1, 10n+3) = 1$.

10. *Λύση.*
    i) Ένας τρόπος είναι με επαγωγή στο m (θεωρώντας το n σταθερό). Πράγματι, για $m = n+1$ έχουμε

$$a^{2^{n+1}} - 1 = (a^{2^n})^2 - 1 = (a^{2^n} - 1)(a^{2^n} + 1)$$

    που είναι πολλαπλάσιο του $a^{2^n} + 1$. Έστω ότι $m > n+1$ και το $a^{2^m} - 1$ είναι πολλαπλάσιο του $a^{2^n} + 1$. Τότε

$$a^{2^{m+1}} - 1 = (a^{2^m})^2 - 1 = (a^{2^m} - 1)(a^{2^m} + 1)$$

    που από την επαγωγική υπόθεση είναι πολλαπλάσιο του $a^{2^n} + 1$.
    ii) Έστω d ο ζητούμενος μκδ. Από το πρώτο υποερώτημα παίρνουμε ότι $d | a^{2^m} - 1$. Επειδή $d | a^{2^m} + 1$, συμπεραίνουμε ότι $d|2$, δηλαδή $d = 1, 2$.
    Όταν ο a είναι άρτιος, τότε από τον ορισμό του d έχουμε ότι ο d είναι περιττός, οπότε $d = 1$. Όταν ο a είναι άρτιος, τότε από τον ορισμό του d έχουμε ότι ο d είναι άρτιος, οπότε $d = 2$.

11. *Απάντηση:* $p = q = 11$.

12. *Λύση.* Από τον Ευκλείδειο αλγόριθμο έχουμε

$$\begin{aligned} b &= aq + r, \quad 0 \le r < a \\ a &= rq_1 + r_1, \quad 0 \le r_1 < r \\ r &= r_1 q_2 + r_2, \quad 0 \le r_2 < r_1 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \le r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + 0. \end{aligned}$$

    Έστω $b = aq + r$ και

$$Q = n^r \frac{n^{qa} - 1}{n^a - 1} = n^r (n^{a(q-1)} + \cdots n^a + 1) \in \mathbb{Z}.$$

    Τότε $n^b - 1 = Q(n^a - 1) + (n^r - 1)$. Άρα έχουμε

$$\begin{aligned} n^{b-1} &= Q(n^a - 1) + n^r - 1 \\ n^a - 1 &= Q_1(n^r - 1) + n^{r_1} - 1 \\ n^r - 1 &= Q_2(n^{r_1} - 1) + n^{r_2} - 1 \\ &\vdots \\ n^{r_{m-2}} &= Q_m(n^{r_{m-1}} - 1) + n^{r_m} - 1 \\ n^{r_{m-1}} &= Q_{m+1}(n^{r_m} - 1) + 0. \end{aligned}$$

    Επομένως $\mu\kappa\delta(n^a - 1, n^b - 1) = n^{r_m} - 1$, όπου $r_m = \mu\kappa\delta(a, b)$.

13. *Υπόδειξη.* Αρχικά παρατηρήστε ότι από την Ευκλείδεια διαίρεση έπεται ότι κάθε πρώτος μεγαλύτερος ή ίσος του 5 είναι της μορφής $6k+1$ ή $6k+5$, $k \in \mathbb{Z}$. Στη συνέχεια τροποποιήστε την απόδειξη του λήμματος του Ευκλείδη ως εξής. Έστω ότι το σύνολο των πρώτων της μορφής $6k+5$ είναι πεπερασμένο και είναι το $\{p_1 ..., p_m\}$. Δείξτε ότι ο $N = 6p_1 ... p_m + 5$ διαιρείται από κάποιο p_i.

14. *Υπόδειξη.* Για την ύπαρξη θεωρείστε διαδοχικές Ευκλείδειες διαιρέσεις με το 2 της μορφής

$$n = 2q_0 + r_0$$
$$q_0 = 2q_1 + r_1$$
$$\ldots$$

και θέστε $a_i = r_i$. Η δυαδική παράσταση του 100 είναι $100 = (1100100)_2 = 2^6 + 2^5 + 2^2$.

15. *Λύση.* Αν A είναι γνήσιο υποσύνολο του $\mathbb{N}$, τότε το σύνολο $B = \mathbb{N} - A$ είναι μη κενό υποσύνολο των φυσικών αριθμών. Από το αξίωμα ελαχίστου, το B διαθέτει ελάχιστο στοιχείο, έστω b. Επειδή $0 \in A$, έχουμε $b > 0$. Από τον ορισμό του b έχουμε $b - 1 \in A$. Άρα από την υπόθεση έπεται ότι $b \in A$, άτοπο.

16.

17. *Απάντηση.* Όχι.

Ισοτιμίες και οι ακέραιοι modulo n

Εδώ εισάγουμε το σύνολο των ακεραίων modulo n και μελετάμε την αριθμητική σε αυτό. Δίνουμε έμφαση στα αντιστρέψιμα στοιχεία και τη συνάρτηση του Euler.

Βασικά σημεία

- ισοτιμίες
- σχέσεις ισοδυναμίας
- το σύνολο $\mathbb{Z}_n$ των ακεραίων modulo n
- αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$
- συνάρτηση του Euler

2.1. Ισοτιμίες

Ορισμός 2.1. *Έστω $a, b, n \in \mathbb{Z}$. Θα λέμε ότι οι a, b είναι* **ισότιμοι** *modulo n (ή ισοϋπόλοιποι modulo n), αν $n|a-b$. Στην περίπτωση αυτή γράφουμε $a \equiv b \mod n$.*

Για παράδειγμα, $13 \equiv 3 \mod 5$, αφού $5|13-3$. Επίσης $13 \equiv -2 \mod 5$, αφού $5|13-(-2)$. Έστω $a, b, n \in \mathbb{Z}$. Σημειώνουμε τα εξής.

(1) $a \equiv b \mod n \Leftrightarrow a \equiv b \mod (-n)$.

(2) Αν $n = 0$, τότε $a \equiv b \mod 0 \Leftrightarrow a = b$.

Με βάση την πρώτη ιδιότητα, όταν εργαζόμαστε $\mod n$ μπορούμε να υποθέσουμε ότι $n \geq 0$.

Πρόταση 2.2. *Έστω $a, b, c, n \in \mathbb{Z}$. Τότε ισχύουν τα ακόλουθα.*

(1) $a \equiv a \mod n$.

(2) *Αν* $a \equiv b \mod n$ *τότε* $b \equiv a \mod n$.

(3) *Αν* $a \equiv b \mod n$ *και* $b \equiv c \mod n$, *τότε* $a \equiv c \mod n$.

Απόδειξη. Οι (1) και (2) έπονται άμεσα τον ορισμό. Για τη (3) παρατηρούμε ότι αν $n|a-b$ και $n|b-c$, τότε από το Λήμμα 1.2 έχουμε ότι $n|(a-b)+(b-c)$, δηλαδή $n|a-c$. □

Η επόμενη πρόταση δικαιολογεί την ορολογία 'ισοϋπόλοιποι' στον Ορισμό 2.1.

Πρόταση 2.3. *Έστω $a, b, n \in \mathbb{Z}, n \neq 0$. Τότε $a \equiv b \mod n$ αν και μόνο αν οι a και b αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n.*

Απόδειξη. Από την Ευκλείδεια διαίρεση υπάρχουν $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, ώστε

$$a = q_1 n + r_1, \quad 0 \leq r_1 < |n|, \text{ και}$$

$$b = q_2 n + r_2, \quad 0 \leq r_2 < |n|$$

Επομένως $a - b = (q_1 - q_2)n + r_1 - r_2$, με $0 \leq |r_1 - r_2| < |n|$. Άρα

$$a \equiv b \mod n \Leftrightarrow n|a-b \Leftrightarrow n|r_1 - r_2 \Leftrightarrow r_1 - r_2 = 0 \quad (\text{αφού } |r_1 - r_2| < |n|.)$$

Δηλαδή $a \equiv b \mod n \Leftrightarrow r_1 = r_2$. □

Στην επόμενη πρόταση βλέπουμε ότι οι ισοτιμίες είναι συμβατές με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού ακεραίων.

Πρόταση 2.4. *Έστω $a, b, c, d, n \in \mathbb{Z}$. Τότε ισχύουν τα ακόλουθα.*
(1) *Αν $a \equiv b \mod n$ και $c \equiv d \mod n$, τότε $a + c \equiv b + d \mod n$.*
(2) *Αν $a \equiv b \mod n$ και $c \equiv d \mod n$, τότε $a \cdot c \equiv bd \mod n$.*
(3) *Αν $a \equiv b \mod n$, τότε $a^k \equiv b^k \mod n$, για κάθε $k \in \mathbb{Z}_{>0}$.*

Απόδειξη. (1) Έχουμε $a \equiv b \mod n \Leftrightarrow n|a-b$ και $c \equiv d \mod n \Leftrightarrow n|c-d$. Επομένως

$$n|a-b+c-d \Rightarrow n|a+c-(b+d) \Rightarrow a+c \equiv b+d \mod n.$$

(2) Έχουμε $n|a-b$ και $n|c-d$. Παρατηρούμε ότι

$$ac - bd = ac - bc + bc - bd = (a-b)c + b(c-d).$$

Επειδή $n|(a-b)c + b(c-d)$ έπεται ότι $n|ac-bd$. Επομένως $ac \equiv bd \mod n$.
(3) Έπεται άμεσα από το (2). □

Παρατηρήσεις.

(1) Σε σχέση με την ιδιότητα (2) της προηγούμενης πρότασης, τονίζουμε ότι γενικά **δεν** ισχύει ότι από $ac \equiv bd \mod n, c \neq 0$, έπεται ότι $a \equiv b \mod n$. Για παράδειγμα, $5 \cdot 2 \equiv 2 \cdot 2 \mod 6$ αλλά δεν ισχύει ότι $5 \equiv 2 \mod 6$. Αν όμως μκδ$(c, n) = 1$, τότε από $ac \equiv bc \mod m$ έπεται ότι $a \equiv b \mod m$, βλ. άσκηση 2.2.

(2) Η Πρόταση 2.4 μας δίνει ένα αλγεβρικό λογισμό με ισοτιμίες. Μιλώντας με μεγάλο βαθμό ελευθερίας, μπορούμε στις ισοτιμίες $\mod n$ (για το ίδιο n) να προσθέτουμε κατά μέλη, να πολλαπλασιάζουμε κατά μέλη και να υψώνουμε σε θετικές ακέραιες δυνάμεις.

Παραδείγματα 2.5.

(1) Αποδείξτε ότι για κάθε $n \in \mathbb{N}$ ο ακέραιος $5^{1821} + 6^{1821}$ είναι πολλαπλάσιο του 11.
Πράγματι, από $5 \equiv -6 \mod 11$ έπεται ότι για κάθε περιττό θετικό ακέραιο a,

$$5^a + 6^a \equiv (-6)^a + 6^a \equiv (-1)^a 6^a + 6^a \equiv -6^a + 6^a \equiv 0 \mod 11.$$

Άρα $11|5^{1821} + 6^{1821}$.

(2) Αποδείξτε ότι για κάθε $a \in \mathbb{Z}$ ισχύει $a^2 \equiv 0, 1$ ή $4 \mod 8$. Κατά συνέπεια ο αριθμός 202040067085 δεν είναι τετράγωνο ακεραίου.
Από $a \equiv 0, 1, .., 7 \mod 8$ έπεται ότι $a^2 \equiv 0^2, 1^2, .., 7^2 \mod 8$. Εύκολα επαληθεύουμε ότι $0^2 \equiv 0 \mod 8$, $1^2 \equiv 1 \mod 8$, $2^2 \equiv 4 \mod 8$, $3^2 \equiv 1 \mod 8$, $4^2 \equiv 0 \mod 8$, $5^2 \equiv 1 \mod 8$, $6^2 \equiv 4 \mod 8$, $7^2 \equiv 1 \mod 8$. Συνεπώς $a^2 \equiv 0, 1$ ή $4 \mod 8$. Επειδή $202040067085 \equiv 5 \mod 8$, έχουμε ότι ο 202040067085 δεν είναι τετράγωνο ακεραίου.

(3) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 9 αν και μόνο αν το άθροισμα των ψηφίων του, $\sum_i a_i$, διαιρείται με το 9.

Πράγματι, στη δεκαδική γραφή έχουμε $a_k \cdots a_1 a_0 = a_k 10^k + ... + a_1 10^1 + a_0$. Επειδή $10^m \equiv 1^m \equiv 1 \mod 9$ για κάθε $m \in \mathbb{N}$, έχουμε $a_k \cdots a_1 a_0 \equiv a_k + ... + a_1 + a_0 \mod 9$. Άρα $a_k \cdots a_1 a_0 \equiv 0 \mod 9$ αν και μόνο αν $a_k + ... + a_1 + a_0 \equiv 0 \mod 9$.

(4) Ένας ακέραιος αριθμός $a_k \cdots a_1 a_0$ (σε δεκαδική γραφή) διαιρείται με το 11 αν και μόνο αν το εναλλασσόμενο άθροισμα των ψηφίων του, $\sum_i (-1)^i a_i$, διαιρείται με το 11.

Η απόδειξη είναι παρόμοια με την προηγούμενη ξεκινώντας από $10^m \equiv (-1)^m \mod 11$.

(5) Να βρεθούν όλοι οι πρώτοι p ώστε οι $p + 10$ και $p + 14$ να είναι πρώτοι.
Δοκιμάζοντας μερικούς μικρούς πρώτους, βλέπουμε ότι για $p = 3$ οι 13 και 17 είναι πρώτοι. Θα δείξουμε τώρα ότι δεν υπάρχει άλλος p. Έστω p πρώτος με $p > 3$. Τότε $p \equiv 1$ ή $2 \mod 3$. Αν $p \equiv 1 \mod 3$, τότε $p + 14 \equiv 15 \equiv 0 \mod 3$, και επομένως ο $p + 14$ δεν είναι πρώτος αφού είναι πολλαπλάσιο του 3 και μεγαλύτερος του 3. Αν $p \equiv 2 \mod 3$, τότε $p + 10 \equiv 12 \equiv 0 \mod 3$ και κατά συνέπεια ο $p + 10$ δεν είναι πρώτος.

(6) Δείξτε ότι δεν υπάρχουν ακέραιοι x, y με $7x^2 - 150y^2 = 1$.
Έστω ότι υπάρχουν ακέραιοι x, y με $7x^2 - 150y^2 = 1$. Τότε

$$7x^2 - 150y^2 \equiv 1 \mod 5 \Rightarrow 2x^2 \equiv 1 \mod 5.$$

Επειδή $x \equiv 0, 1, 2, 3, 4 \mod 5$, παίρνουμε $x^2 \equiv 0^2, 1^2, 2^2, 3^2, 4^2 \mod 5$, δηλαδή $x^2 \equiv 0, 1, 4 \mod 5$. Άρα $2x^2 \equiv 0, 2, 3 \mod 5$. Σε κάθε περίπτωση βλέπουμε ότι $2x^2 \not\equiv 1 \mod 5$.

2.2. Σχέσεις ισοδυναμίας

Υπενθυμίζουμε ότι αν A είναι σύνολο, με $A \times A$ συμβολίζουμε το σύνολο των διατεταγμένων ζευγών (a, a'), όπου $a, a' \in A$.

Ορισμός 2.6. *Μια **σχέση** του συνόλου A είναι ένα υποσύνολο του $A \times A$.*

Αν $X \subseteq A \times A$, τότε αντί του συμβολισμού $(a, a') \in X$ θα γράφουμε $a \sim_X a'$ ή $a \sim a'$ (αν είναι σαφές ποιο είναι το X).

Ορισμός 2.7. *Έστω $A \neq \emptyset$ και $X \subseteq A \times A$. Το X λέγεται **σχέση ισοδυναμίας** στο A, αν ισχύουν οι ακόλουθες ιδιότητες.*

(1) *$a \sim a$ για κάθε $a \in A$ (ανακλαστική).*
(2) *Αν $a \sim b$, όπου $a, b \in A$, τότε $b \sim a$ (συμμετρική).*
(3) *Αν $a \sim b$ και $b \sim c$, όπου $a, b, c \in A$, τότε $a \sim c$ (μεταβατική).*

Για παράδειγμα, αν $A = \{1, 2, 3\}$, το $X = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$ είναι σχέση ισοδυναμίας στο A. Η σχέση $Y = \{(1, 1), (2, 2), (3, 3), (2, 3)\}$ δεν είναι σχέση ισοδυναμίας στο A αφού $(2, 3) \in Y$ και $(3, 2) \notin Y$, δηλαδή δεν ισχύει η συμμετρική ιδιότητα για το ζεύγος $(2, 3)$.

Ορισμός 2.8. *Έστω X μια σχέση ισοδυναμίας στο A και $a \in A$. Η **κλάση ισοδυναμίας** του a είναι το σύνολο $[a] = \{x \in A : x \sim a\}$.*

Σημειώνουμε ότι στον παραπάνω ορισμό έχουμε $a \in [a]$ λόγω της ανακλαστικής ιδιότητας. Συνεπώς κάθε κλάση ισοδυναμίας είναι μη κενό σύνολο.

Παραδείγματα 2.9.

(1) Στο παράδειγμα X που είδαμε αμέσως μετά τον Ορισμό 2.7, για $a = 1$ ισχύει $[a] = \{1\}$, για $b = 2$ ισχύει $[b] = \{2, 3\}$ και για $c = 3$ ισχύει $[c] = \{2, 3\}$.

(2) Έστω $A \neq \emptyset$. Ορίζουμε μια σχέση στο A ως εξής.

$$a \sim b \Leftrightarrow a = b.$$

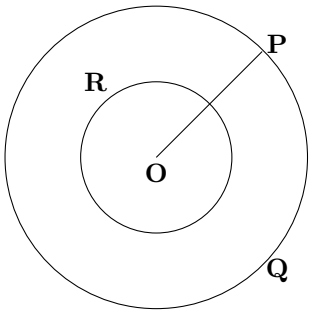
Αυτή είναι μια σχέση ισοδυναμίας. Παρατηρούμε ότι $[a] = \{a\}$ για κάθε $a \in A$.

(3) Η σχέση στο $\mathbb{R}$ που ορίζεται από $a \sim b \Leftrightarrow a \leq b$ δεν είναι σχέση ισοδυναμίας καθώς δεν ισχύει η συμμετρική ιδιότητα. Η ανακλαστική ιδιότητα και η μεταβατική ισχύουν.

(4) Έστω A το σύνολο των σημείων του επιπέδου $\mathbb{R}^2$. Ορίζουμε την σχέση

$$P \sim Q \Leftrightarrow |OP| = |OQ|,$$

όπου P, Q σημεία του επιπέδου και O η αρχή των αξόνων. Εύκολα επαληθεύεται ότι η $\sim$ είναι σχέση ισοδυναμίας. Παρατηρούμε ότι $[P] =$ το σύνολο των σημείων του κύκλου με ακτίνα $|OP|$ και κέντρο το O.

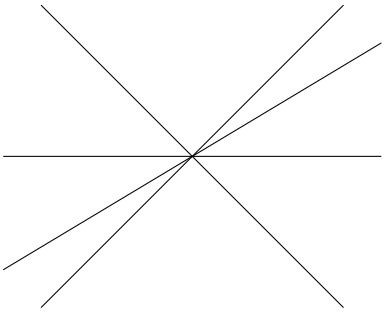


Οι κλάσεις ισοδυναμίας είναι ομόκεντροι κύκλοι.

(5) **Προβολική ευθεία** $\mathbb{P}^1(\mathbb{R})$. Στο σύνολο $A = \mathbb{R}^2 - \{(0, 0)\}$ ορίζουμε την εξής σχέση

$$(x, y) \sim (x', y') \Leftrightarrow \exists \lambda \in \mathbb{R}, (x, y) = \lambda(x', y').$$

Εύκολα επαληθεύεται ότι είναι σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του $(x, y) \in A$ είναι η "ευθεία" που διέρχεται από το (x, y) και $(0, 0)$ (χωρίς να περιέχει το $(0, 0)$). Το σύνολο των κλάσεων ισοδυναμίας στο παράδειγμα αυτό λέγεται η πραγματική προβολική ευθεία.



Οι κλάσεις ισοδυναμίας είναι ευθείες που διέρχονται από το (0,0).

(6) Έστω $A, B \in M_n(\mathbb{R})$. Από τη Γραμμική Άλγεβρα ξέρουμε ότι η σχέση που ορίζεται από

$$A \sim B \Leftrightarrow \text{υπάρχει αντιστρέψιμος } P \in M_n(\mathbb{R}) \text{ με } B = P^{-1}AP$$

είναι σχέση ισοδυναμίας.

(7) **Σημαντικό παράδειγμα** Έστω $n \in \mathbb{Z}_{>0}$. Ορίζουμε την εξής σχέση στο $\mathbb{Z}$,

$$a \sim b \Leftrightarrow n|a - b.$$

Δηλαδή $a \sim b \Leftrightarrow a \equiv b \mod n$. Από την Πρόταση 2.2 έπεται ότι η παραπάνω σχέση είναι σχέση ισοδυναμίας. Για την κλάση ισοδυναμίας του a, την οποία συμβολίζουμε με $[a]_n$ ή $[a]$ όταν είναι σαφές ποιο είναι το n, έχουμε

$$[a]_n = \{x \in \mathbb{Z} : x = a \mod n\} = \{a + kn,\ k \in \mathbb{Z}\}$$

$$= \{..., a-2n, a-n, a, a+n, a+2n, ...\}.$$

(a) Έστω $n = 2$. Έχουμε

$$[0]_2 = \{x \in \mathbb{Z} : x \sim 0\}.$$

Αλλά $x \sim 0 \Leftrightarrow x \equiv 0 \mod 2 \Leftrightarrow x = 2k,\ k \in \mathbb{Z}$. Επομένως

$$[0]_2 = \{2k : k \in \mathbb{Z}\} = \{..., -4, -2, 0, 2, 4, ...\}.$$

που είναι το σύνολο των άρτιων ακεραίων. Ομοίως βλέπουμε ότι

$$[1]_2 = \{2k+1 : k \in \mathbb{Z}\} = \{..., -3, -1, 1, 3, 5, ...\}$$

που είναι το σύνολο των περιττών ακεραίων. Επίσης έχουμε $[5]_2 = [3]_2 = [1]_2 = [-1]_2$. Γενικά, για $n = 2$ έχουμε $[m] = [0]$ αν m άρτιος και $[m] = [1]$ αν m περιττός. Παρατηρούμε ότι

$$\mathbb{Z} = [0]_2 \cup [1]_2 \quad \kappa\alpha\iota \quad [0]_2 \cap [1]_2 = \emptyset.$$

(b) Έστω $n = 3$. Τότε

$$[0]_3 = \{3k : k \in \mathbb{Z}\} = \{..., -6, -3, 0, 3, 6...\}$$
$$[1]_3 = \{3k+1 : k \in \mathbb{Z}\} = \{..., -5, -2, 1, 4, 7, ...\}$$
$$[2]_3 = \{3k+2 : k \in \mathbb{Z}\} = \{... -4, -1, 2, 5, 8, ...\}.$$

Εδώ $[5]_3 = [2]_3 = [-1]_3 = [-4]_3 = \{..., -1, 2, 5, 8, ...\}$. Παρατηρούμε ότι

$$\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3 \quad \kappa\alpha\iota \quad [i]_3 \cap [j]_3 = \emptyset\ \forall i, j \in \{0, 1, 2\}, i \neq j.$$

Θα δούμε τώρα ότι δύο κλάσεις ισοδυναμίας μιας σχέσης ισοδυναμίας ή ταυτίζονται ή είναι ξένα σύνολα.

Πρόταση 2.10. *Αν X είναι σχέση ισοδυναμίας στο A και $a, b \in A$, τότε:*
(1) $[a] = [b] \Leftrightarrow a \sim b$,
(2) $[a] \cap [b] = \emptyset \Leftrightarrow a \nsim b$.

Απόδειξη. (1) Έστω $[a] = [b]$. Τότε $a \in [a] = [b]$, οπότε από τον ορισμό της κλάσης παίρνουμε $a \sim b$.

Αντίστροφα έστω $a \sim b$ και έστω $x \in [a]$. Τότε $x \sim a$ και αφού $a \sim b$, από την μεταβατική ιδιότητα παίρνουμε ότι $x \sim b$. Επομένως $x \in [b]$ και συνεπώς $[a] \subseteq [b]$. Ομοίως αποδεικνύεται ότι $[b] \subseteq [a]$. Άρα $[a] = [b]$.
(2) Έστω $[a] \cap [b] = \emptyset$ και $a \sim b$. Τότε $a \in [a]$ και $a \in [b]$. Άρα $a \in [a] \cap [b]$, άτοπο.

Αντίστροφα έστω $a \nsim b$ και $x \in [a] \cap [b]$. Τότε $x \in [a]$ και $x \in [b]$, δηλαδή $x \sim a$ και $x \sim b$. Από τη συμμετρική ιδιότητα έχουμε $a \sim x$ και $x \sim b$, και από τη μεταβατική ιδιότητα $a \sim b$, άτοπο. □

Η προηγούμενη πρόταση λέει ότι το X μπορεί να παρασταθεί ως ξένη ένωση κλάσεων ισοδυναμίας. Για παράδειγμα, όταν $n = 3$ είδαμε στο Παράδειγμα 2.9(7) ότι $\mathbb{Z} = [0]_3 \cup [1]_3 \cup [2]_3$ και οι κλάσεις $[0]_3, [1]_3, [2]_3$ είναι ανά δύο ξένες.

Μια **διαμέριση** ενός μη κενού συνόλου A είναι μια οικογένεια $(A_i)_{i \in I}$ μη κενών υποσυνόλων του A τέτοιων ώστε $A_i \cap A_j = \emptyset$ για κάθε $i \neq j$ και $\cup_{i \in I} A_i = A$. Για παράδειγμα, αν $A = \{1, 2, 3\}$, τότε όλες οι διαμερίσεις του A είναι οι εξής χωρίς να λαμβάνεται υπόψη η σειρά των A_i:

- {1,2,3}
- {1},{2,3}
- {2},{1,3}
- {3},{1,2}
- {1},{2},{3}.

Είδαμε πριν ότι κάθε σχέση ισοδυναμίας στο A παρέχει μια διαμέριση του A μέσω των κλάσεων ισοδυναμίας. Ισχύει και το αντίστροφο.

Πρόταση 2.11. *Αν $(A_i)_{i\in I}$ είναι διαμέριση του συνόλου A, τότε υπάρχει σχέση ισοδυναμίας στο A της οποίας οι κλάσεις ισοδυναμίας είναι τα $A_i, i \in I$.*

Απόδειξη. Ορίζουμε την εξής σχέση στο A,

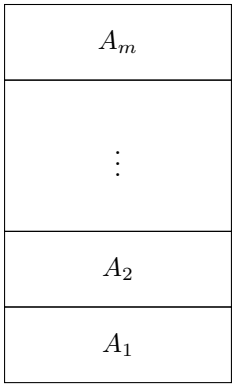
$$a \sim b \Leftrightarrow \exists i \in I \text{ με } a, b \in A_i.$$

Εύκολα επαληθεύεται ότι αυτή είναι σχέση ισοδυναμίας.

- Ανακλαστική ιδιότητα: Αν $a \in A$, τότε επειδή $\cup_{i\in I} A_i = A$, υπάρχει $i \in I$ με $a \in A_i$.
- Συμμετρική ιδιότητα: Άμεσο καθώς αν $a, b \in A_i$, τότε $b, a \in A_i$.
- Μεταβατική ιδιότητα: Έστω ότι $a \sim b$ και $b \sim c$. Τότε υπάρχουν $i, j \in I$ με $a, b \in A_i$ και $b, c \in A_j$. Επειδή $b \in A_i \cap A_j$, ο ορισμός της διαμέρισης δίνει $i = j$. Άρα $a, c \in A_i$.

Έστω $a \in A$ οπότε $a \in A_i$ για κάποιο $i \in I$. Για την κλάση ισοδυναμίας $[a] = \{x \in A : x \sim a\}$ του a είναι σαφές ότι $A_i \subseteq [a]$. Έστω $x \in [a]$, δηλαδή $x, a \in A_j$ για κάποιο j. Επειδή $a \in A_i$, ο ορισμός της διαμέρισης δίνει $i = j$. Άρα $[a] \subseteq A_i$ οπότε $[a] = A_i$. □

Παρατήρηση. Μιλώντας με μεγάλο βαθμό ελευθερίας, οι σχέσεις ισοδυναμίες σε ένα σύνολο A και οι διαμερίσεις του A αποτελούν δύο τρόποι να βλέπουμε το ίδιο πράγμα. Στην πρώτη περίπτωση, ομαδοποιούμε στοιχεία του A σύμφωνα με ιδιότητα τους, ενώ στη δεύτερη καταγράφουμε τα στοιχεία κάθε ομαδοποίησης.



Το σύνολο A έχει διαμερισθεί σε m κλάσεις ισοδυναμίας.

2.3. Το σύνολο $\mathbb{Z}_n$

Θωρούμε τη σχέση ισοδυναμίας στο $\mathbb{Z}$ που ορίζεται από

$$a \sim b \Leftrightarrow a \equiv b \mod n.$$

Το σύνολο των κλάσεων ισοδυναμίας αυτής συμβολίζεται με $\mathbb{Z}_n$, δηλαδή

$$\mathbb{Z}_n = \{[a]_n : a \in \mathbb{Z}\}$$

και ονομάζεται το **σύνολο των ακεραίων modulo** n. Η Πρόταση 2.10(1) μας λέει πότε δύο στοιχεία του $\mathbb{Z}_n$ είναι ίσα, δηλαδή

$$[a]_n = [b]_n \Leftrightarrow a \equiv b \mod n \Leftrightarrow n|a-b.$$

Για παράδειγμα στο $\mathbb{Z}_3$ έχουμε $[2020]_3 = [1]_3$ αφού $3|2020-1$ και $[-10]_3 = [2]_3$ αφού $3|-10-2$.

Πρόταση 2.12. *Αν $n > 0$, τότε $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$.*

Απόδειξη. Προφανώς $[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n \in \mathbb{Z}_n$.

Έστω $[a] \in \mathbb{Z}_n$. Από την Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ με

$$a = qn + r, \quad 0 \leq r \leq n-1.$$

Τότε $a \equiv r \mod n$ και άρα $[a]_n = [r]_n$.

Μένει να δειχθεί ότι τα στοιχεία $[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n$ είναι διακεκριμένα. Αυτό έπεται άμεσα από την Πρόταση 2.3. □

Η προηγούμενη πρόταση λέει ότι για $n > 0$, το σύνολο $\mathbb{Z}_n$ είναι πεπερασμένο και έχει n στοιχεία.

Για $n = 0$, έχουμε $a \equiv b \mod 0 \Leftrightarrow a = b$, πράγμα που σημαίνει ότι η κλάση ισοδυναμίας κάθε $a \in \mathbb{Z}$ είναι μονοσύνολο, $[a]_0 = \{a\}$. Στην περίπτωση αυτή, $\mathbb{Z}_0 = \{[a] : a \in \mathbb{Z}\}$ και η αντιστοιχία $\mathbb{Z}_0 \to \mathbb{Z}$, $[a]_0 \longmapsto a$ είναι 1-1 και επί. Μπορούμε να σκεφτόμαστε το $\mathbb{Z}_0$ ως το $\mathbb{Z}$.

Παράδειγμα 2.13. Έχουμε

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\},$$

όπου $[0]_2 = \{2k : k \in \mathbb{Z}\}$ και $[1]_2 = \{2k+1 : k \in \mathbb{Z}\}$. Επίσης

$$\mathbb{Z}_2 = \{[1]_2, [2]_2\} = \{[2020]_2, [1821]_2\}, \text{ και}$$

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} = \{[1]_3, [1821]_3, [8]_3\}.$$

Παρατήρηση. Έστω $n > 0$ και $a_0, a_1, \cdots, a_{n-1} \in \mathbb{Z}$ με $a_i \equiv i \mod n$ για κάθε i. Τότε $\mathbb{Z}_n = \{[a_0]_n, [a_1]_n, \cdots, [a_{n-1}]_n\}$.

Οι επαΐοντες στη θεωρία αριθμών θα θυμούνται ότι ένα σύνολο ακεραίων $a_0, \cdots, a_{n-1}$, όπως στην παραπάνω παρατήρηση λέγεται πλήρες σύστημα αντιπροσώπων των κλάσεων υπολοίπων modulo n.

Στη συνέχεια θα ορίσουμε με φυσιολογικό τρόπο δύο πράξεις στο σύνολο $\mathbb{Z}_n$ και θα μελετήσουμε ιδιότητές τους.

Μια **πράξη** σε μη κενό σύνολο A είναι μια απεικόνιση της μορφής $A \times A \to A$. Για παράδειγμα, η συνήθης πρόσθεση ακεραίων ορίζει πράξη $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, όπου η εικόνα του διατεταγμένου ζεύγους $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ είναι το άθροισμα $a + b$. Απεναντίας, η συνήθης διαίρεση πραγματικών αριθμών δεν ορίζει πράξη στο $\mathbb{R}$, καθώς η εικόνα του (a, b), δηλαδή το πηλίκο $\frac{a}{b}$, δεν ορίζεται όταν $b = 0$.

Ορίζουμε τις ακόλουθες πράξεις στο $\mathbb{Z}_n$,

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a], [b]) \to [a + b],$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n([a], [b]) \to [a \cdot b].$$

που τις ονομάζουμε **πρόσθεση** και **πολλαπλασιασμό** αντίστοιχα. Θα χρησιμοποιούμε τους συμβολισμούς $[a] + [b] = [a + b]$ και $[a][b] = [ab]$ αντίστοιχα, και θα γράφουμε $[a]$ στη θέση του $[a]_n$.

Οι ορισμοί των παραπάνω πράξεων *εξαρτώνται από επιλογή αντιπροσώπων* a, b των κλάσεων $[a], [b]$. Το ακόλουθο λήμμα λέει ότι δεδομένων των κλάσεων $[a], [b]$, οι κλάσεις $[a + b], [ab]$ τελικά **δεν** εξαρτώνται από επιλογές των a, b, ισοδύναμα ότι έχουμε ορίσει πράγματι απεικονίσεις
.

Λήμμα 2.14. *Οι απεικονίσεις του προηγούμενου ορισμού είναι καλά ορισμένες.*

Απόδειξη. Έστω $a, a', b, b' \in \mathbb{Z}$ με $[a] = [a']$ και $[b] = [b']$. Θα δείξουμε ότι $[a+b] = [a'+b']$ και $[ab] = [a'b']$.

Από $[a] = [a']$ έχουμε $a \equiv a' \mod n$ και από $[b] = [b']$ έχουμε $b \equiv b' \mod n$. Σύμφωνα με την Πρόταση 2.4,

$$a + b \equiv a' + b' \mod n, \quad ab \equiv a'b' \mod n,$$

δηλαδή $[a + b] = [a' + b']$ και $[ab] = [a'b']$. □

Παράδειγμα 2.15. Στο $\mathbb{Z}_6$ έχουμε, $[8] + [4] = [12] = [0]$, $[8][4] = [32] = [2]$ και $[2][-5] + [-7] = [2\dot{(}-5) - 7] = [-17] = [1]$. Στον παρακάτω πίνακα πρόσθεσης (αντίστοιχα, πολλαπλασιασμού) του $\mathbb{Z}_6$, στη θέση που αντιστοιχεί στη γραμμή $[i]$ και στήλη $[j]$ υπάρχει το στοιχείο $[i] + [j]$ (αντίστοιχα, το $[i][j]$).

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Πίνακας πρόσθεσης του $\mathbb{Z}_6$.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Πίνακας πολλαπλασιασμού του $\mathbb{Z}_6$.

Ακολουθούν μερικές ιδιότητες των παραπάνω πράξεων.

Πρόταση 2.16. *Έστω $a, b, c \in \mathbb{Z}$. Στο $\mathbb{Z}_n$ ισχύουν οι ακόλουθες ισότητες.*

(1) $([a] + [b]) + [c] = [a] + ([b] + [c])$.
(2) $[a] + [0] = [0] + [a] = [a]$.
(3) $[a] + [-a] = [-a] + [a] = [0]$.
(4) $[a] + [b] = [b] + [a]$.
(5) $[a]([b][c]) = ([a][b])[c]$.
(6) $[a]([b] + [c]) = [a][b] + [a][c]$.
(7) $([a] + [b])[c] = [a][c] + ([b][c])$.
(8) $[1][a] = [a][1] = [a]$.
(9) $[a][b] = [b][a]$.

Απόδειξη. Αποδεικνύουμε ενδεικτικά την (7). Έχουμε διαδοχικά

$$\begin{aligned}([a] + [b])[c] &= [a + b][c] \\ &= [(a + b)c] \\ &= [ac + bc] \\ &= [ac] + [bc] \\ &= [a][c] + [b][c].\end{aligned}$$

Οι άλλες αποδείξεις είναι επίσης άμεσες. □

Παρατήρηση. Τονίζουμε ότι αν και η πρόσθεση και ο πολλαπλασιασμός στοιχείων του $\mathbb{Z}_n$ έχουν ιδιότητες που θυμίζουν την πρόσθεση και τον πολλαπλασιασμό ακεραίων, υπάρχουν **σημαντικές διαφορές**. Για παράδειγμα, στο $\mathbb{Z}$ το γινόμενο δύο μη μηδενικών στοιχείων είναι μη μηδενικό. Στο $\mathbb{Z}_6$ όμως, έχουμε $[2][3] = [0]$. Επίσης, αν οι ακέραιοι a, b, c ικανοποιούν $ac = bc$ και $c \neq 0$, τότε $a = b$. Στο $\mathbb{Z}_6$ όμως, έχουμε $[1][3] = [5][3]$ με $[3] \neq [0]$ και $[1] \neq [5]$.

Ένα στοιχείο $[a] \in \mathbb{Z}_n$ λέγεται **μηδενοδιαιρέτης** αν υπάρχει $[b] \in \mathbb{Z}_n$, $[b] \neq [0]$, έτσι ώστε $[a][b] = [0]$. Είδαμε πριν ότι το $[2] \in \mathbb{Z}_6$ είναι μηδενοδιαιρέτης.

Παραδείγματα 2.17.

(1) Λύστε στο $\mathbb{Z}_{121}$ την εξίσωση $[a]^2 = [1]$.
Έχουμε

$$[a]^2 = [1] \Leftrightarrow [a^2 - 1] = [0] \Leftrightarrow$$
$$[(a-1)(a+1)] = [0] \Leftrightarrow 11^2 | (a-1)(a+1) \Leftrightarrow$$
$$\begin{cases} 11^2 | a-1 \\ \text{ή} \\ 11^2 | a+1 \\ \text{ή} \\ 11 | a-1 \text{ και } 11 | a+1. \end{cases}$$

Στην πρώτη περίπτωση έχουμε $[a-1] = [0]$, δηλαδή $[a] = [1]$. Στη δεύτερη έχουμε $[a+1] = [0]$, δηλαδή $[a] = [-1] = [120]$. Η τρίτη περίπτωση είναι αδύνατη καθώς από $11|a-1$ και $11|a+1$ έπεται ότι $11|2$. Τελικά οι ζητούμενες λύσεις είναι οι $[1], [120]$.

(2) Λύστε στο $\mathbb{Z}_{240}$ την εξίσωση $[a]^2 = [0]$.
Έχουμε

$$[a]^2 = [0] \Leftrightarrow [a^2] = [0] \Leftrightarrow 2^4 \cdot 3 \cdot 5 | a^2 \Leftrightarrow \begin{cases} 2^4 | a^2 \\ 3 | a^2 \\ 5 | a^2 \end{cases}$$

όπου στην τελευταία ισοδυναμία χρησιμοποιήσαμε την άσκηση 1.3(ii). Χρησιμοποιώντας το λήμμα του Ευκλείδη και την άσκηση 1.3(ii),

$$\begin{cases} 2^4 | a^2 \\ 3 | a^2 \\ 5 | a^2 \end{cases} \Leftrightarrow \begin{cases} 2^2 | a \\ 3 | a \\ 5 | a \end{cases} \Leftrightarrow 2^2 \cdot 3 \cdot 5 | a.$$

(Στην ισοδυναμία $2^4 | a^2 \Leftrightarrow 2^2 | a$ χρησιμοποιήσαμε την Παρατήρηση (3) μετά το Θεώρημα 1.12.) Οι φυσικοί αριθμοί που είναι πολλαπλάσιοι του $2^2 \cdot 3 \cdot 5 = 60$ και μικρότεροι του 240 είναι οι 0, 60, 120, 180 και συνεπώς οι ζητούμενες λύσεις είναι οι $[0], [60], [120], [180]$.

2.4. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$

Ορισμός 2.18. *Ένα στοιχείο $[a] \in \mathbb{Z}_n$ λέγεται **αντιστρέψιμο** αν υπάρχει $[a'] \in \mathbb{Z}_n$ με*

$$[a][a'] = [a'][a] = [1].$$

*Στην περίπτωση αυτή θα λέμε ότι το στοιχείο $[a']$ είναι ένα **αντίστροφο** του $[a]$ στο $\mathbb{Z}_n$.*

Για παράδειγμα, στο $\mathbb{Z}_{10}$ έχουμε $[3][7] = [7][3] = [21] = [1]$. Επομένως το $[3]$ και το $[7]$ είναι αντιστρέψιμα στοιχεία.

Στο $\mathbb{Z}_{10}$ το $[2]$ δεν είναι αντιστρέψιμο στοιχείο. Πράγματι, έστω ότι υπάρχει $[a'] \in \mathbb{Z}_{10}$ ώστε $[2][a'] = [1]$. Τότε $[2a'] = [1]$, δηλαδή $2a' \equiv 1 \mod 10$. Έπεται ότι $2a' = 1 + 10k$, $k \in \mathbb{Z}$ που είναι άτοπο.

Επειδή στο $\mathbb{Z}_n$ ισχύει $[a][b] = [b][a]$ για κάθε $[a], [b] \in \mathbb{Z}_n$, η ύπαρξη $[a'] \in \mathbb{Z}_n$ τέτοιου ώστε $[a][a'] = [a'][a] = [1]$ στον Ορισμό 2.17, ισοδυναμεί με την ύπαρξη $[a'] \in \mathbb{Z}_n$ τέτοιου ώστε $[a][a'] = [1]$ (ή $[a'][a] = [1]$).

Θα δούμε τώρα ποια στοιχεία του $\mathbb{Z}_n$ αντιστρέψιμα.

Πρόταση 2.19. *Το $[a] \in \mathbb{Z}_n$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(a, n) = 1$.*

Απόδειξη. Έστω $[a]$ αντιστρέψιμο στο $\mathbb{Z}_n$. Τότε υπάρχει $[a'] \in \mathbb{Z}_n$ με $[a][a'] = 1$. Τότε $[aa'] = 1 \Rightarrow aa' = 1 \mod n$. Επομένως $aa' = 1 + kn$, $(k \in \mathbb{Z})$. Έπεται ότι $\mu\kappa\delta(a, n)|1$ άρα $\mu\kappa\delta(a, n) = 1$.

Αντίστροφα, έστω ότι $\mu\kappa\delta(a, n) = 1$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ ώστε $1 = ax + ny$ σύμφωνα με το Θεώρημα 1.9. Επομένως

$$[1] = [ax + ny] = [a][x] + [n][y] = [a][x] + [0][y] = [a][x].$$

Άρα έχουμε $[1] = [a][x]$ δηλαδή το $[a]$ είναι αντιστρέψιμο. □

Πρόταση 2.20. (1) *Αν το $[a] \in \mathbb{Z}_n$ είναι αντιστρέψιμο, τότε υπάρχει μοναδικό αντίστροφό του.*
(2) *Αν $[a_1], ..., [a_m] \in U(\mathbb{Z}_n)$, τότε $[a_1...a_m] \in U(\mathbb{Z}_n)$*

Απόδειξη. (1) Έστω $[a], [b], [c] \in \mathbb{Z}_n$ ώστε $[a][b] = [1], \text{και} [a][c] = [1]$. Τότε

$$[c] = [c][1] = [c]([a][b]) = ([c][a])[b] = ([a][c])[b] = [1][b] = [b].$$

(2) Αν υπάρχουν $[a'_1], ..., [a'_m] \in \mathbb{Z}_n$ με $[a_1][a'_1] = ... = [a_m][a'_m] = 1$, τότε $[a_1...a_m][a'_1...a'_m] = [a_1...a_m a'_1...a'_m] = [(a_1a'_1)...(a_ma'_m)] = [1 \cdot ... \cdot 1] = [1]$. □

Αν το $[a] \in \mathbb{Z}_n$ είναι αντιστρέψιμο, θα συμβολίζουμε το αντίστροφό του με $[a]^{-1}$.

Παραδείγματα 2.21.

(1) Σύμφωνα με την Πρόταση 2.18, τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{12}$ είναι τα $[1], [5], [7], [11]$. Παρατηρούμε ότι $[7][7] = [49] = [1]$, οπότε το αντίστροφο του $[7]$ στο $\mathbb{Z}_{12}$ είναι το $[7]$, δηλαδή $[7]^{-1} = [7]$.

(2) Βρείτε το αντίστροφο του $[5]$ στο $\mathbb{Z}_{72}$.
Εφαρμόζουμε τη γενική μέθοδο που παρέχει η απόδειξη της Πρότασης 2.18. Από τον Ευκλείδειο αλγόριθμο έχουμε

$$\begin{aligned} 72 &= 14 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Άρα $\mu\kappa\delta(72, 5) = 1$ και το $[5]$ είναι πράγματι αντιστρέψιμο σύμφωνα με την Πρόταση 2.18. Αντικαθιστώντας παίρνουμε

$$1 = 5 - 2 \cdot 2 = 5 - 2(72 - 14 \cdot 5) = 29 \cdot 5 - 2 \cdot 72$$

Αυτό σημαίνει ότι στο $\mathbb{Z}_{72}$ έχουμε $[1] = [29][5]$, δηλαδή $[5]^{-1} = [29]$.

2.5. Η συνάρτηση του Euler

Ορισμός 2.22. *Η συνάρτηση $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ με*

$$\varphi(n) = \text{πλήθος } \{a \in \mathbb{Z} : 1 \leq a \leq n, \mu\kappa\delta(a, n) = 1\}$$

λέγεται ***συνάρτηση του Euler****.*

Για παράδειγμα έχουμε $\varphi(12) = 4$,

$$1,\ \not{2},\ \not{3},\ \not{4},\ 5,\ \not{6},\ 7,\ \not{8},\ \not{9},\ \not{10},\ 11,\ \not{12}.$$

Ας συμβολίσουμε με $U(\mathbb{Z}_n)$ το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$,

$$U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n : [a] \text{ αντιστρέψιμο}\},$$

Για παράδειγμα, $U(\mathbb{Z}_{12}) = \{[1], [5], [7], [11]\}$. Από την Πρόταση 2.18 έπεται άμεσα ότι η συνάρτηση του Euler μετράει το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$.

Πόρισμα 2.23. *Για κάθε θετικό ακέραιο n ισχύει ότι $\varphi(n) = |U(\mathbb{Z}_n)|$.*

Στο επόμενο αποτέλεσμα περιέχονται μερικές σημαντικές αριθμητικές ιδιότητες της συνάρτησης του Euler.

Θεώρημα 2.24. *Η συνάρτηση φ του Euler ικανοποιεί τις ακόλουθες ιδιότητες.*

(1) *Αν p πρώτος και $k \in \mathbb{Z}_{>0}$, τότε $\varphi(p^k) = p^k - p^{k-1}$.*
(2) *Αν $m, n \in \mathbb{Z}_{>0}$ και $\mu\kappa\delta(m, n) = 1$, τότε $\varphi(mn) = \varphi(m)\varphi(n)$.*
(3) *Αν $a \in \mathbb{Z}_{>0}$ και $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου p_i πρώτοι με $p_i \neq p_j$ για κάθε $i \neq j$, τότε*

$$\varphi(a) = (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) = a\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Για παράδειγμα, $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3)\varphi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$.

Στην απόδειξη του Θεωρήματος 2.22 θα χρειαστούμε το εξής λήμμα.

Λήμμα 2.25. *Έστω $a, m, n \in \mathbb{Z}$. Τότε $\mu\kappa\delta(a, m) = \mu\kappa\delta(a, n) = 1 \Leftrightarrow \mu\kappa\delta(a, mn) = 1$.*

Απόδειξη. Έστω ότι $\mu\kappa\delta(a, m) = \mu\kappa\delta(a, n) = 1$ και ότι υπάρχει p πρώτος με $p|\mu\kappa\delta(a, mn)$. Τότε $p|mn$ και επειδή ο p είναι πρώτος, έπεται ότι $p|m$ ή $p|n$. Δηλαδή,

$$p|a \text{ και } p|m \quad \text{ή} \quad p|a \text{ και } p|n.$$

Άρα $p|\mu\kappa\delta(a, m)$ ή $p|\mu\kappa\delta(a, n)$. Επομένως $p|1$, το οποίο είναι άτοπο.

Αντίστροφα, έστω ότι $\mu\kappa\delta(a, mn) = 1$. Επειδή κάθε κοινός διαιρέτης των a, m είναι κοινός διαιρέτης των a, mn, έπεται ότι $\mu\kappa\delta(a, m)|\mu\kappa\delta(a, mn)$. Άρα $\mu\kappa\delta(a, m) = 1$. Όμοια έπεται ότι $\mu\kappa\delta(a, n) = 1$. □

Απόδειξη του Θεωρήματος 2.24.
(1) Οι ακέραιοι που ικανοποιούν τις συνθήκες $1 \leq a \leq p^k$ και $\mu\kappa\delta(a, p^k) \neq 1$ είναι ακριβώς τα πολλαπλάσια του p της μορφής $a = pq$,όπου $q = 1, 2, \ldots p^{k-1}$. Από τον Ορισμό 2.20 έπεται ότι $\varphi(p^k) = p^k - p^{k-1}$.
(2) Υπάρχουν διάφορες αποδείξεις της σχέσης αυτής. Θα δώσουμε μια απόδειξη που οι ιδέες της θα φανούν χρήσιμες σε παρακάτω παραγράφους.

Αρκεί να δείξουμε ότι αν $\mu\kappa\delta(m, n) = 1$, τότε $|U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m)| \times |U(\mathbb{Z}_n)|$. Για το σκοπό αυτό θεωρούμε τη συνάρτηση $\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, με

$$\psi([a]_{mn}) = ([a]_m, [a]_n).$$

Η ψ είναι καλά ορισμένη. Πράγματι, έστω $[a]_{mn} = [b]_{mn}$. Τότε $mn|a - b$, οπότε $m|a - b$ και $n|a - b$. Επομένως $[a]_m = [b]_m$ και $[a]_n = [b]_n$.

Ισχυρισμός: Η ψ είναι $1 - 1$ και επί.

Πράγματι, έστω $\psi([a]_{mn}) = \psi([b]_{mn})$, οπότε $[a]_m = [b]_m$ και $[a]_n = [b]_n$. Άρα

$$m|a - b \quad \text{και} \quad n|a - b.$$

Αφού $\mu\kappa\delta(m,n)=1$, παίρνουμε ότι $mn|a-b$ σύμφωνα με την άσκηση 1.3. Άρα $[a]_{mn}=[b]_{mn}$, δηλαδή η ψ είναι $1-1$.

Επειδή η $\psi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ είναι $1-1$ και $|\mathbb{Z}_{mn}|=|\mathbb{Z}_m\times\mathbb{Z}_n|(=mn<\infty)$, έπεται ότι η ψ είναι επί.

Θεωρούμε τώρα τον περιορισμό $\bar{\psi}$ της ψ στο υποσύνολο $U(\mathbb{Z}_{mn})$ του Z_{mn}. Παρατηρούμε ότι

$$\bar{\psi}(U(\mathbb{Z}_{mn}))\subseteq U(\mathbb{Z}_m)\times U(\mathbb{Z}_n).$$

Πράγματι, έστω $[a]_{mn}\in U(\mathbb{Z}_{mn})$, οπότε $\mu\kappa\delta(a,mn)=1$ σύμφωνα με την Πρόταση 2.18. Από το Λήμμα 2.23 έπεται ότι $\mu\kappa\delta(a,m)=1$. Δηλαδή $[a]_m\in U(\mathbb{Z}_m)$. Ομοίως έχουμε $[a]_n\in U(\mathbb{Z}_n)$. Θα δείξουμε τώρα ότι η $\bar{\psi}$ είναι $1-1$ και επί.

Η $\bar{\psi}$ είναι 1-1 αφού είναι περιορισμός απεικόνισης που είναι 1-1.

Η $\bar{\psi}$ είναι επί. Πράγματι, έστω $([x]_m,[y]_n)\in U(\mathbb{Z}_m)\times U(\mathbb{Z}_n)$. Τότε $\mu\kappa\delta(x,m)=\mu\kappa\delta(y,n)=1$. Επειδή η ψ είναι επί, υπάρχει στοιχείο $[a]_{mn}\in\mathbb{Z}_{mn}$ ώστε $([a]_m,[a]_n)=([x]_m,[y]_n)$, δηλαδή

$$[a]_m=[x]_m\quad\text{και}\quad[a]_n=[y]_n.$$

Τότε $a\equiv x \mod m$ και αφού $\mu\kappa\delta(x,m)=1$, έπεται $\mu\kappa\delta(a,m)=1$. Ομοίως παίρνουμε $\mu\kappa\delta(a,n)=1$. Από το Λήμμα 2.23 έπεται ότι $\mu\kappa\delta(a,mn)=1$, δηλαδή $[a]_{mn}\in U(\mathbb{Z}_{mn})$.
(3) Από τα (2) και (1) έχουμε διαδοχικά,

$$\begin{aligned}\varphi(p_1^{a_1}p_2^{a_2}\cdots p_k^{a_a}) &= \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_k^{a_k})\\ &= (p_1^{a_1}-p_1^{a-1})(p_2^{a_2}-p_2^{a-1})\cdots(p_k^{a_k}-p_k^{a_{k-1}})\\ &= a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

□

Στο επόμενο αποτέλεσμα έχουμε μια σπουδαία ισοτιμία που ικανοποιεί η συνάρτηση του Euler.

Θεώρημα 2.26 (Euler). *Έστω $a\in\mathbb{Z}$ και $n\in\mathbb{Z}_{>0}$ με $\mu\kappa\delta(a,n)=1$. Τότε*

$$a^{\varphi(n)}\equiv 1 \mod n.$$

Παράδειγμα 2.27. Έστω πρώτος $p\neq 2,5$. Αφού $\varphi(1000)=400$ και $\mu\kappa\delta(p,1000)=1$, έχουμε $p^{400}\equiv 1 \mod 1000$. Δηλαδή τα τρία τελευταία ψηφία του p^{400} στο δεκαδικό σύστημα είναι 0,0,1.

Απόδειξη του Θεωρήματος Euler.
Έστω $U(\mathbb{Z}_n)=\{[a_1],[a_2],\cdots,[a_k]\}$, όπου $k=\varphi(n)$, και έστω $[a]\in U(\mathbb{Z}_n)$. Θεωρούμε το σύνολο $A=\{[aa_i]:i=1,2,\ldots,k\}$. Θα δείξουμε ότι $A=U(\mathbb{Z}_n)$. Δείχνουμε πρώτα ότι $A\subseteq U(\mathbb{Z}_n)$.

Από την Πρόταση 2.19, αν $[a],[b]\in U(\mathbb{Z}_n)$, τότε και $[ab]\in U(\mathbb{Z}_n)$.

Επειδή τα σύνολα A και $U(\mathbb{Z}_n)$ είναι πεπερασμένα και ισχύει $A\subseteq U(\mathbb{Z}_n)$, για να δείξουμε ότι $A=U(\mathbb{Z}_n)$, αρκεί να δείξουμε ότι έχουν το ίδιο πλήθος στοιχείων, δηλαδή ότι $|A|=k$. Ισοδύναμα, αρκεί να δείξουμε ότι αν $[a_i]\neq[a_j]$, τότε $[aa_i]\neq[aa_j]$. Έστω ότι $[aa_i]=[aa_j]$. Τότε $n|aa_i-aa_j\Rightarrow n|a(a_i-a_j)$.Επειδή $\mu\kappa\delta(a,n)=1$, έπεται ότι $n|a_i-a_j$. Επομένως $[a_i]=[a_j]$. Άρα $A=U(\mathbb{Z}_n)$.

Θεωρούμε τώρα το γινόμενο όλων των στοιχείων του συνόλου $A=U(\mathbb{Z}_n)$,

$$[aa_1][aa_2]\cdots[aa_k]=[a_1][a_2]\cdots[a_k].$$

Επομένως $[a^k][a_1a_2\cdots a_k]=[a_1a_2\cdots a_k]$. Πολλαπλασιάζοντας με τον αντίστροφο του $[a_1a_2\cdots a_k]$, προκύπτει ότι $[a]^k=[1]$, δηλαδή $a^k\equiv 1 \mod n$. □

Παρατήρηση. Από το θεώρημα Euler έχουμε ότι αν $\mu\kappa\delta(a,n)=1$, τότε το αντίστροφο του $[a]$ στο $\mathbb{Z}_n$ είναι το $[a^{\varphi(n)-1}]$.

Πόρισμα 2.28 (Μικρό θεώρημα του Fermat)**.** *Έστω $a \in \mathbb{Z}$ και p πρώτος.*
(1) *Ισχύει $a^p \equiv a \mod p$.*
(2) *Αν $p \nmid a$, τότε $a^{p-1} \equiv 1 \mod p$.*

Απόδειξη. Το (2) έπεται άμεσα από το θεώρημα του Euler. Το (1) είναι άμεσο αν $p|a$. Αν $p \nmid a$, το (1) έπεται άμεσα από το (2) πολλαπλασιάζοντας κατά μέλη με a. □

Επισημαίνουμε ότι θα δούμε μια άλλη απόδειξη του Θεωρήματος του Euler στην Παράγραφο 8.2, ως πόρισμα του Θεωρήματος του Lagrange. Επίσης, η πρώτη ισοτιμία στο Πόρισμα 2.26 μπορεί να αποδειχθεί ανεξάρτητα με επαγωγή στο a, βλέπε άσκηση 2.17.

Ασκήσεις Κεφαλαίου 2

Ομάδα1: 1-4, 6-11, 26.
Ομάδα2: 12-24.
Ομάδα3: 5, 25.

1. Βρείτε όλους τους $x \in \mathbb{Z}$, ώστε $8x \equiv 11 \mod 15$.
2. Δείξτε τα εξής.
   i) Η εξίσωση $[a][x] = [b]$ έχει λύση στο $\mathbb{Z}_n$ αν και μόνο αν $\mu\kappa\delta(a, n)|b$.
   ii) Αν $ac \equiv bc \mod n$ και οι c, n είναι σχετικά πρώτοι, τότε $a \equiv b \mod n$.
3. Δείξτε ότι δεν υπάρχει ακέραιος της μορφής $4n + 3, n \in \mathbb{Z}$, που να είναι άθροισμα δύο τετραγώνων ακεραίων.
4. Δείξτε ότι δεν υπάρχουν $x, y \in \mathbb{Z}$ ώστε $x^2 - 5y^2 = 13$.
5. Δείξτε ότι κανένας ακέραιος της μορφής $3^m + 3^n + 1$ $(m, n \in \mathbb{N})$ είναι τετράγωνο ακεραίου.
6. Βρείτε το υπόλοιπο της διαίρεσης του 19^{1000} με το 14.
7. Δείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $n^{49} \equiv n \mod 1547$. Σημ.$1547 = 7 \cdot 13 \cdot 17$.
8. Δείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $(n + 1)^9 + 4n^5 \equiv 1 \mod 5$.
9. Δείξτε ότι για κάθε θετικό περιττό ακέραιο n, ο $1^n + 2^n + ... + (n-1)^n$ είναι πολλαπλάσιος του n.
10. Έστω $n \in \mathbb{N}$. Δείξτε ότι $n^{12} + 12^n \equiv 5 \mod 11 \Leftrightarrow n \equiv 2, 9 \mod 11$.
11. Δείξτε ότι $7^n \equiv 1 \mod 20 \Leftrightarrow n = 0 \mod 4$.
12. $\star$ Έστω p πρώτος με $p = 3 \mod 4$. Δείξτε ότι $\nexists a \in \mathbb{Z}$ με $a^2 \equiv -1 \mod p$.
13. Έστω $a \in \mathbb{Z}$ με $\mu\kappa\delta(a, 72) = 1$. Δείξτε ότι $a^{12} \equiv 1 \mod 72$.
14. Έστω $n \in \mathbb{Z}_{>0}$. Δείξτε ότι $\varphi(2n) = 2\varphi(n) \Leftrightarrow n$ άρτιος.
15. Δώστε άλλη λύση της άσκησης 1.12. Αν $a, b, n \in \mathbb{Z}_{>0}$, $n > 1$, τότε $\mu\kappa\delta(n^a - 1, n^b - 1) = n^d - 1$, όπου $d = \mu\kappa\delta(a, b)$.
16. Πόσα στοιχεία έχει καθένα από τα παρακάτω σύνολα;
    - $A = \{x \in \mathbb{Z}_{77} : [5]x[6] = [7]\}$,
    - $B = \{x \in \mathbb{Z}_{77} : [5]x[7] = [6]\}$,
    - $C = \{x \in \mathbb{Z}_{77} : x^2 = [0]\}$,
    - $D = \{x \in \mathbb{Z}_{77} : x^{120} = [1]\}$.
    - $E = \{x \in \mathbb{Z}_{77} : \exists y \in \mathbb{Z}_{77} - \{[0]\}, xy = [0]\}$.
17. Δείξτε ότι για κάθε πρώτο p ισχύει $p|\binom{p}{i}, i = 1, .., p-1$. Στη συνέχεια δείξτε το μικρό θεώρημα του Fermat, χρησιμοποιώντας επαγωγή στο a.
18. Έστω a, n θετικοί ακέραιοι με $\mu\kappa\delta(a, n) = \mu\kappa\delta(a - 1, n) = 1$. Δείξτε ότι $1 + a + a^2 + \cdots + a^{\varphi(n)-1} \equiv 0 \mod n$.
19. Έστω πρώτος $p > 2$. Δείξτε ότι για κάθε $a \in \mathbb{Z}_p$ υπάρχει $x \in \mathbb{Z}_p$ με $x^{p-2} = a$
20. Αν p, q είναι διαφορετικοί πρώτοι, τότε $p^{q-1} + q^{p-1} \equiv 1 \mod pq$.
21. Έστω m, n θετικοί ακέραιοι και $d = \mu\kappa\delta(m, n)$. Δείξτε ότι $\varphi(mn)\varphi(d) = d\varphi(m)\varphi(n)$.
22. $\star$ Έστω d, n θετικοί ακέραιοι με $d|n$. Θέτουμε
$$A_d = \{m \in \{1, \ldots, n\} | \mu\kappa\delta(m, n) = d\}.$$
    i) Δείξτε ότι $|A_d| = \varphi(n/d)$.
    ii) Συμπεράνατε ότι $n = \sum_{d|n} \varphi(n/d)$ από την ξένη ένωση $\{1, \ldots, n\} = \bigcup_{d|n} A_d$.
    iii) Άρα $n = \sum_{d|n} \varphi(d)$.
23. Έστω $n > 1$ και $a \in \mathbb{Z}_n$. Θεωρούμε την απεικόνιση $f_a : \mathbb{Z}_n \to \mathbb{Z}_n, f_a(x) = ax$.

i) Δείξτε ότι : f_a είναι 1-1 $\Leftrightarrow$ f_a είναι επί $\Leftrightarrow$ $a \in U(\mathbb{Z}_n)$.
ii) Συμπληρώστε και αποδείξτε την πρόταση: f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\} \Leftrightarrow$ ο n είναι ....

24. Έστω n θετικός ακέραιος. Δείξτε ότι κάθε $x \in U(\mathbb{Z}_{2^{n+2}})$ ικανοποιεί $x^{2^n} = [1]$.

25. Αριθμοί του Bell Έστω $B(n)$ το πλήθος των σχέσεων ισοδυναμίας ενός συνόλου n στοιχείων, όπου n θετικός ακέραιος. Δείξτε ότι $B(1) = 1, B(2) = 2, B(3) = 5$ και γενικά $B(n+1) = \sum_{i=0}^{n} \binom{n}{i} B(i)$.

26. Έστω p πρώτος. Δείξτε ότι για κάθε θετικό ακέραιο n ισχύει

$$n^n \equiv n^{s_p(n)} \mod p,$$

όπου $s_p(n)$ είναι το άθροισμα των ψηφίων στην p-αδική παράσταση του n (βλ. άσκηση 1.14).

Υποδείξεις Ασκήσεων Κεφαλαίου 2

1. *Λύση.* Επειδή $\mu\kappa\delta(8,15)=1$, το $[8]$ έχει αντίστροφο στο $\mathbb{Z}_{15}$. Από τον Ευκλείδειο αλγόριθμο έχουμε,

$$\begin{aligned} 15 &= 1\cdot 8+7\\ 8 &= 1\cdot 7+1\\ 7 &= 7\cdot 1+0. \end{aligned}$$

Επομένως

$$1=8-1\cdot 7=8-1(15-1\cdot 8)=8(2)+15(-1).$$

Συνεπώς στο $\mathbb{Z}_{15}$ ισχύει ότι $[1]=[8][2]$. Αυτό σημαίνει ότι το αντίστροφο του $[8]$ στο $\mathbb{Z}_{15}$ είναι το $[2]$. Παρατηρούμε ότι $8x\equiv 11 \mod 15 \Leftrightarrow [8][x]=[11]$. Πολλαπλασιάζοντας με το αντίστροφο του $[8]$ έχουμε

$$[2]([8][x])=[2][11]\Rightarrow [x]=[22]=[7].$$

Επομένως $x=7+15t, t\in\mathbb{Z}$

2. *Λύση.* i) Έστω ότι υπάρχει $x\in\mathbb{Z}$ ώστε $[a][x]=[b]$. Τότε

$$[ax]=[b]\Rightarrow ax=b+kn \quad (k\in\mathbb{Z}).$$

Επειδή $\mu\kappa\delta(a,n)|a$ και $\mu\kappa\delta(a,n)|n$, έχουμε $\mu\kappa\delta(a,n)|b$.

Αντίστροφα, έστω ότι $\mu\kappa\delta(a,n)|b$. Τότε υπάρχουν $y,z\in\mathbb{Z}$ ώστε

$$\mu\kappa\delta(a,n)=ay+nz.$$

Πολλαπλασιάζοντας με το $\frac{b}{\mu\kappa\delta(a,n)}\in\mathbb{Z}$, παίρνουμε $b=ax+nz_1$, για κάποια $x,z_1\in\mathbb{Z}$. Επομένως $[b]=[ax]=[a][x]$.

ii) Έχουμε $ac\equiv bc \mod n \Rightarrow [ac]=[bc]\Rightarrow [a][c]=[b][c]$. Επειδή οι c,n είναι σχετικά πρώτοι, το $[c]$ είναι αντιστρέψιμο στο $\mathbb{Z}_n$. Πολλαπλασιάζοντας την παραπάνω ισότητα με το αντίστροφο του $[c]$ προκύπτει $[a]=[b]$, δηλαδή $a\equiv b \mod n$.

3. *Λύση.* Υποθέτουμε ότι υπάρχουν $a,n,b\in\mathbb{N}$ ώστε $4n+3=a^2+b^2$. Τότε

$$a^2+b^2\equiv 3 \mod 4.$$

Παρατηρούμε ότι $a=0,1,2,3 \mod 4$, άρα $a^2=0^2,1^2,2^2,3^2 \mod 4$. Δηλαδή $a^2\equiv 0,1 \mod 4$ και $b^2\equiv 0,1 \mod 4$. Επομένως

$$a^2+b^2\equiv 0,1,2 \mod 4.$$

Δηλαδή σε κάθε περίπτωση δεν ισχύει ότι $a^2+b^2\equiv 3 \mod 4$, άτοπο.

4. *Λύση.* Δουλεύουμε $\mod 5$. Έστω ότι υπάρχουν $x,y\in\mathbb{Z}$ με $x^2-5y^2=13$. Τότε $x^2\equiv 13 \mod 5\Rightarrow x^2\equiv 3 \mod 5$. Παρατηρούμε ότι

$$x=0,1,2,3,4 \mod 5\Rightarrow x^2=0^2,1^2,2^2,3^2,4^2 \mod 5\Rightarrow$$

$$x^2=0,1,4 \mod 5.$$

δηλαδή σε κάθε περίπτωση δεν ισχύει ότι $x^2\equiv 3 \mod 5$, άτοπο.

5. *Λύση.* Υποθέτουμε ότι υπάρχουν $m,n,x\in\mathbb{N}$ με $3^m+3^n+1=x^2$ και δουλεύουμε $\mod 8$. Εξετάζοντας τις περιπτώσεις $x\equiv 0,1,...,7 \mod 8$ εύκολα επαληθεύεται ότι $x^2=0,1,4 \mod 8$.

Θα δείξουμε τώρα με επαγωγή στο m ότι

$$3^m\equiv 1,3 \mod 8.$$

Για $m=1$ το ζητούμενο είναι σαφές. Έχουμε $3^{m+1}=3\cdot 3^m\equiv 3,9 \mod 8$. Επομένως $3^{m+1}\equiv 1,3 \mod 8$.

Συνεπώς έχουμε $3^m+3^n+1\equiv 3,5,7 \mod 8$, δηλαδή $x^2\equiv 3,5,7 \mod 8$, άτοπο.

6. *Λύση.* Παρατηρούμε ότι

$$19 \equiv 5 \mod 14 \Rightarrow 19^{1000} \equiv 5^{1000} \mod 14. \tag{2.1}$$

Έχουμε $\varphi(14) = \varphi(2 \cdot 7) = \varphi(2)\varphi(7) = 6$.Επειδή $1000 = 166 \cdot 6 + 4$, παίρνουμε

$$5^{1000} = (5^6)^{166}5^4 \equiv 1^{166}5^4 \mod 14,$$

όπου η δεύτερη ισότητα έπεται από το θεώρημα του Euler. Τότε από την (2.1) παίρνουμε,

$$19^{1000} \equiv 5^4 \mod 14.$$

Όμως $5^4 = (5^2)^2 \equiv 11^2 \equiv (-3)^2 \equiv 9 \mod 14$. Επομένως το υπόλοιπο της διαίρεσης του 19^{1000} με το 14 είναι το 9.

7. *Λύση.* Επειδή $1547 = 7 \cdot 13 \cdot 17$ αρκεί να δείξουμε τις ισοτιμίες

$$n^{49} \equiv n \mod 7,$$

$$n^{49} \equiv n \mod 13,$$

$$n^{49} \equiv n \mod 17.$$

Πράγματι από το μικρό θεώρημα του Fermat για $p = 7$, έχουμε $n^7 = n \mod 7$, άρα

$$n^{49} \equiv (n^7)^7 \equiv n \mod 7.$$

Ομοίως, από το μικρό θεώρημα του Fermat για $p = 13$, έχουμε $n^{13} = n \mod 13$. Επειδή $49 = 3 \cdot 13 + 10$, παίρνουμε

$$n^{49} \equiv (n^{13})^3 n^{10} \equiv n^3 n^{10} \equiv n^{13} \equiv n \mod 13.$$

Ομοίως με πριν αποδεικνύεται ότι $n^{49} \equiv n \mod 17$.

8. *Λύση.* Από το μικρό θεώρημα του Fermat, έχουμε

$$n^5 \equiv n \mod 5 \quad \text{και} \quad (n+1)^5 \equiv n+1 \mod 5.$$

Επομένως

$$(n+1)^9 = (n+1)^5(n+1)^4 \equiv (n+1)(n+1)^4 \equiv (n+1)^5 \equiv n+1 \mod 5.$$

Άρα $(n+1)^9 + 4n^5 \equiv n + 1 + 4n \equiv 1 \mod 5$.

9. *Λύση.* Ας το κάνουμε όπως ο επτάχρονος Gauss: Έστω $n = 2q + 1$. Παρατηρούμε ότι

$$1^n + 2^n + ... + q^n + (q+1)^n + ... + (n-2)^n + (n-1)^n =$$

$$(1^n + (n-1)^n) + (2^n + (n-2)^n) + \cdots (q^n + (n-q)^n).$$

Επειδή για κάθε i ισχύει $n - i \equiv -i \mod n$, έχουμε $i^n + (n-i)^n \equiv i^n + (-i)^n \equiv i^n + (-1)^n i^n \mod n$. Επειδή ο n είναι περιττός, ισχύει $(-1)^n = -1$ και επομένως

$$i^n + (n-i)^n \equiv i^n - i^n \equiv 0 \mod n.$$

Προσθέτοντας κατά μέλη τις ισοτιμίες αυτές για $i = 1, ..., q$ προκύπτει ότι

$$(1^n + (n-1)^n) + (2^n + (n-2)^n) + \cdots (q^n + (n-q)^n) \equiv 0 \mod n.$$

10. *Λύση.* Παρατηρούμε ότι $12^n \equiv 1 \mod 11$. Από το μικρό θεώρημα του Fermat για $p = 11$, παίρνουμε $n^{12} \equiv n^2 \mod 11$. Άρα $n^{12} + 12^n \equiv (n^2 + 1) \mod 11$ και συνεπώς

$$\begin{aligned} n^{12} + 12^n \equiv 5 \mod 11 &\Leftrightarrow n^2 + 1 \equiv 5 \mod 11 \\ &\Leftrightarrow n^2 - 4 \equiv 0 \mod 11 \\ &\Leftrightarrow 11 | n^2 - 4 \\ &\Leftrightarrow 11 | (n-2)(n+2), \end{aligned}$$

Επειδή ο 11 είναι πρώτος παίρνουμε ισοδύναμα $11|n-2$ ή $11|n+2$, δηλαδή $n \equiv 2 \mod 11$ ή $n \equiv 9 \mod 11$.

11. *Λύση.* Από την Ευκλείδεια διαίρεση έχουμε $n = 4m + r,\ 0 \leq r < 4$. Επειδή $7^4 = 2401$, έχουμε $7^4 = 1 \mod 20$ και $7^n = (7^4)^m \cdot 7^r \equiv 7^r \mod 20$. Επομένως

$$7^n \equiv 1 \mod 20 \Leftrightarrow 7^r \equiv 1 \mod 20.$$

Για $r = 0$ η παραπάνω ισοτιμία προφανώς ισχύει. Για $r = 1, 2, 3$ κάνοντας πράξεις βλέπουμε ότι η παραπάνω ισοτιμία δεν ισχύει.

Παρατήρηση. Έχουμε $\varphi(20) = \varphi(4\cdot 5) = \varphi(4)\varphi(5) = 2\cdot 4 = 8$. Επίσης $\mu\kappa\delta(7, 20) = 1$. Άρα από το θεώρημα του Euler έχουμε $7^8 \equiv 1 \mod 20$. Στην προηγούμενη άσκηση είδαμε ότι $7^4 \equiv 1 \mod 20$. Άρα γενικά μιλώντας, αν $\mu\kappa\delta(a, n) = 1$, τότε ο ακέραιος $\varphi(n)$ *δεν* είναι αναγκαστικά ο μικρότερος θετικός ακέραιος k ώστε $a^k \equiv 1 \mod n$.

12. *Λύση.* Υποθέτουμε ότι υπάρχει $a \in \mathbb{Z}$ ώστε $a^2 \equiv -1 \mod p$. Διακρίνουμε τις ακόλουθες περιπτώσεις.
    1. Αν $p|a$, τότε από την παραπάνω ισοτιμία έπεται ότι $p| - 1$, άτοπο.
    2. Έστω ότι $p \nmid a$. Επειδή $p = 3 \mod 4$, υπάρχει $k \in \mathbb{Z}$ με $p = 4k + 3$. Έστω $N = \frac{p-1}{2} = 2k + 1$ (περιττός ακέραιος). Από την παραπάνω ισοτιμία έπεται ότι $a^{2N} \equiv (-1)^N \mod p$, δηλαδή

$$a^{p-1} \equiv -1 \mod p.$$

Αφού ο $p \nmid a$, από το μικρό θεώρημα του Fermat παίρνουμε

$$a^{p-1} \equiv 1 \mod p.$$

Άρα $1 \equiv -1 \mod p \Rightarrow p = 2$, το οποίο είναι άτοπο αφού $p = 3 \mod 4$.

13. *Λύση.* Παρατηρούμε ότι $72 = 2^3 \cdot 3^2$. Επειδή $\mu\kappa\delta(2^3, 3^2) = 1$, αρκεί να δείξουμε ότι

$$a^{12} \equiv 1 \mod 8 \quad \text{και} \quad a^{12} \equiv 1 \mod 9.$$

Πράγματι αφού $\mu\kappa\delta(a, 72) = 1$, έπεται $\mu\kappa\delta(a, 8) = 1$. Από το θεώρημα του Euler και αφού $\varphi(8) = 2^3 - 2^2 = 4$, έχουμε $a^4 \equiv 1 \mod 8$. Επομένως $a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \mod 8$. Ομοίως επειδή $\mu\kappa\delta(a, 9) = 1$ και $\varphi(9) = 3^2 - 3 = 6$, από το θεώρημα του Euler παίρνουμε $a^{\varphi(9)}a^6 = 1 \mod 9$. Επομένως $a^{12} = 1 \mod 9$.

14. *Λύση.* Έστω $\varphi(2n) = 2\varphi(n)$ και ας υποθέσουμε ότι ο n είναι περιττός. Τότε $\mu\kappa\delta(2, n) = 1$ και $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$. Επομένως $\varphi(n) = 2\varphi(n) \Rightarrow \varphi(n) = 0$, αδύνατο.

Αντίστροφα, έστω n άρτιος. Τότε $n = 2^a m$, όπου $a \in \mathbb{Z}_{>0}$ και m περιττός. Τότε

$$\varphi(2n) = \varphi(2^{a+1}m) = \varphi(2^{a+1})\varphi(m) = (2^{a+1} - 2^a)\varphi(m) = 2^a\varphi(m),$$

όπου στην δεύτερη ισότητα χρησιμοποιήσαμε το γεγονός ότι $\mu\kappa\delta(2^{a+1}, m) = 1$.

Επίσης έχουμε,

$$2\varphi(n) = 2\varphi(2^a m) = 2\varphi(2^a)\varphi(m) = 2(2^a - 2^{a-1})\varphi(m) = 2^a\varphi(m)$$

Επομένως $\varphi(2n) = 2\varphi(n)$.

15. *Λύση.* Αρχικά παρατηρούμε ότι αφού $d\,|a$ έχουμε $n^d - 1\,|n^a - 1$ λόγω της ταυτότητας

$$n^{dt} - 1 = (n^d - 1)(n^{d(t-1)} + n^{d(t-2)} + ... + n^d + 1).$$

Όμοια $n^d - 1\,\big|n^b - 1$ και άρα $n^d - 1\,\big|\mu\mathrm{k}\delta(n^a - 1, n^b - 1)$. Έστω $c = \mu\mathrm{k}\delta(n^a - 1, n^b - 1)$. Τότε $n^a \equiv 1 \bmod c$ και $n^b \equiv 1 \bmod c$. Από το Θεώρημα 1.9 υπάρχουν ακέραιοι x, y με $d = ax + by$. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $x > 0$ και $y \leq 0$. Έχουμε $n^{ax} \equiv 1 \bmod c$ $n^{b(-y)} \equiv 1 \bmod c$. Άρα $n^d \equiv n^d 1 \equiv n^d n^{b(-y)} \equiv n^{d+b(-y)} \equiv n^{ax} \equiv 1 \bmod c$. Δηλαδή $c\,\big|n^d - 1$. Επειδή $n^d - 1\,|c$, $c\,\big|n^d - 1$ και $c > 0$ έχουμε $c = n^d - 1$.

16. *Λύση.* Για το A παρατηρούμε ότι τα στοιχεία $[5], [6] \in \mathbb{Z}_{77}$ είναι αντιστρέψιμα καθώς $\mu\kappa\delta(5, 77) = \mu\kappa\delta(6, 77) = 1$. Πολλαπλασιάζοντας με τα αντίστροφα έχουμε $[5]x[6] = [7] \Leftrightarrow x = [5]^{-1}[7][6]^{-1}$. Συνεπώς $|A| = 1$.

Πολλαπλασιάζοντας τη $[5]x[7] = [6]$ από δεξιά με το $[11]$ προκύπτει $[5]x[77] = [66]$, δηλαδή $[0] = [66]$, ισοδύναμα $77|66$. Επειδή αυτό είναι αδύνατο έχουμε $B = \emptyset$.

Με επιχείρημα όπως στο Παράδειγμα 2.16(2), προκύπτει ότι $C = \{[0]\}$, οπότε $|C|$=1.

Αν $x^{120} = [1]$, τότε $xx^{119} = [1]$ που σημαίνει ότι το x είναι αντιστρέψιμο. Άρα $D \subseteq U(\mathbb{Z}_{77})$. Από την άλλη μεριά, το θεώρημα του Euler δίνει $a^{60} \equiv 1 \mod 77$ για κάθε $a \in U(\mathbb{Z}_{77})$ αφού $\varphi(77) = \varphi(7 \cdot 11) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$. Άρα

$$a^{120} \equiv (a^{60})^2 \equiv 1^2 \equiv 1 \mod 77$$

για κάθε $a \in U(\mathbb{Z}_{77})$. Αυτό σημαίνει ότι $U(\mathbb{Z}_{77}) \subseteq D$. Άρα $D = U(\mathbb{Z}_{77})$ και $|D| = |U(\mathbb{Z}_{77})| = \varphi(77) = 60$.

Για το E σημειώνουμε μια γενική ενδιαφέρουσα παρατήρηση:
Κάθε $x \in \mathbb{Z}_n$, $n > 1$, είναι ή μηδενοδιαιρέτης ή αντιστρέψιμο στοιχείο αλλά όχι και τα δύο. Πράγματι, αν το $x = [a]$ δεν είναι αντιστρέψιμο, τότε $d > 1$, όπου $d = \mu\kappa\delta(a, n)$. Για τον ακέραιο $m = \frac{n}{d}$ έχουμε $1 \leq m < n$ και άρα στο $\mathbb{Z}_n$ είναι $[m] \neq [0]$. Επειδή $[a][m] = [\frac{a}{d}][n] = [0]$, x είναι μηδενοδιαιρέτης. Μένει να δείξουμε ότι κάθε μηδενοδιαιρέτης $[b] \in \mathbb{Z}_n$ είναι μη αντιστρέψιμο στοιχείο. Για το σκοπό αυτό, έστω $[c] \in \mathbb{Z}_n - [0]$ με $[b][c] = [0]$. Αν το $[b]$ ήταν αντιστρέψιμο, τότε πολλαπλασιάζοντας με το αντίστροφό του θα είχαμε $[c] = [0]$, αδύνατο.

Από την προηγούμενη παρατήρηση έπεται ότι για το σύνολο E, που είναι το σύνολο των μηδενοδιαιρετών του $\mathbb{Z}_{77}$ ισχύει ότι $E = \mathbb{Z}_{77} - U(\mathbb{Z}_{77})$ και επομένως $|E| = |\mathbb{Z}_{77}| - |U(\mathbb{Z}_{77})| = 77 - \varphi(77) = 77 - 60 = 17$.

17. *Υπόδειξη.* Το διωνυμικό ανάπτυγμα δίνει $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + ... + \binom{p}{p-1}a + 1$.

18. *Λύση.* Παρατηρούμε ότι $(a-1)b = 1 - a^{\varphi(n)}$, όπου $b = 1 + a + a^2 + \cdots + a^{\varphi(n)-1}$. Επειδή $\mu\kappa\delta(a, n) = 1$, εφαρμόζει το θεώρημα του Euler και παίρνουμε ότι $(a-1)b \equiv 0 \mod n$. Δηλαδή στο $\mathbb{Z}_n$ έχουμε $[a-1][b] = [0]$. Επειδή $\mu\kappa\delta(a-1, n) = 1$, το $[a-1]$ είναι αντιστρέψιμο (Πρόταση 2.18). Πολλαπλασιάζοντας την ισότητα $[a-1][b] = [0]$ με $[a-1]^{-1}$ προκύπτει $[b] = [0]$, δηλαδή $b \equiv 0 \mod \nu$.

19. *Υπόδειξη:* Δείξτε ότι η απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p, x \mapsto x^{p-2}$, είναι 1-1 χρησιμοποιώντας το μικρό θεώρημα του Fermat. Δικαιολογήστε ότι είναι επί.

20. *Υπόδειξη:* Από το μικρό θεώρημα του Fermat έχουμε $p|q^{p-1} - 1$ και $q|p^{q-1} - 1$. Άρα

$$pq|(q^{p-1} - 1)(p^{q-1} - 1).$$

21.

22. *Λύση.*
    i) Έχουμε διαδοχικά
    $$\begin{aligned} A_d &= \{m \in \{1d, 2d, ..., \frac{n}{d}d\} : \mu\kappa\delta(m, n) = d\} \\ &= \{m \in \{1d, 2d, ..., \frac{n}{d}d\} : \mu\kappa\delta(\frac{m}{d}, \frac{n}{d}) = 1\} \\ &= \{i \in \{1, 2, ..., \frac{n}{d}\} : \mu\kappa\delta(i, \frac{n}{d}) = 1\} = \varphi(\frac{n}{d}). \end{aligned}$$
    ii) Είναι άμεσο από το προηγούμενο υποερώτημα.
    iii) Από την ξένη ένωση στο προηγούμενο υποερώτημα παίρνουμε άμεσα ότι
    $$n = \sum_{d|n} |A_d|$$
    και επομένως $n = \sum_{d|n} \varphi(\frac{n}{d})$. Καθώς το d διατρέχει τους θετικούς διαιρέτες του n, το ίδιο συμβαίνει με το $\frac{n}{d}$. Άρα $n = \sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$.

23. *Λύση.* i) Επειδή $n \neq 0$, το σύνολο Z_n είναι πεπερασμένο. Συνεπώς f_a είναι 1-1 $\Leftrightarrow$ f_a είναι επί. Έστω ότι η f_a είναι επί. Τότε υπάρχει $b \in \mathbb{Z}_n$ με $f_a(b) = [1]$, δηλαδή $ab = [1]$. Επειδή ο πολλαπλασιασμός του $\mathbb{Z}_n$ είναι μεταθετικός, αυτό σημαίνει ότι το a είναι αντιστρέψιμο. Αντίστροφα, αν το a είναι αντιστρέψιμο και $y \in \mathbb{Z}_n$, τότε έχουμε
    $$f_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1}y) = y,$$
    που σημαίνει ότι η f_a είναι επί.
    ii) Έστω $n > 1$. Θα δείξουμε την εξής πρόταση. Η f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\}$ $\Leftrightarrow$

ο n είναι πρώτος.
Απόδειξη. Από το πρώτο ερώτημα, f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\} \Leftrightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{[0]\}$. Από την Πρόταση 2.19, αυτό ισοδυναμεί με $\mu\kappa\delta(i,n) = 1$ για κάθε $i = 1, ..., n-1$. Καθώς $n > 1$, αυτό ισοδυναμεί με το ότι ο n είναι πρώτος γιατί αν $d > 1$ είναι διαιρέτης του n, τότε $\mu\kappa\delta(d,n) = d > 1$.

24. *Υπόδειξη.* Πρώτα δείξτε ότι αν $x \in U(\mathbb{Z}_{2^{n+2}})$, τότε $x = [a]$ για κάποιο περιττό ακέραιο a. Στην συνέχεια παρατηρήστε ότι $a^{2^n} - 1 = (a^{2^{n-1}} - 1)(a^{2^{n-1}} + 1)$ και δείξτε με επαγωγή στο $n \geq 1$ ότι $2^{n+2} | a^{2^n} - 1$.

25.

26.

Επαναληπτικές Ασκήσεις: Κεφάλαια 1-2

1. Διατυπώστε τον ορισμό του αντιστρέψιμου στοιχείου του $\mathbb{Z}_n$ και στη συνέχεια διατυπώστε μια ισοδύναμη συνθήκη. Αποδείξτε την ισοδυναμία.
2. Έστω $n > 1$ και $a \in \mathbb{Z}_n$. Θεωρούμε την απεικόνιση $f_a : \mathbb{Z}_n \to \mathbb{Z}_n, f_a(x) = ax$.
   i) Δείξτε ότι : f_a είναι 1-1 $\Leftrightarrow$ f_a είναι επί $\Leftrightarrow$ $a \in U(\mathbb{Z}_n)$.
   ii) Συμπληρώστε και αποδείξτε την πρόταση: Η f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\}$ $\Leftrightarrow$ ο n είναι ....
3. Δίνεται η απεικόνιση $f : \mathbb{Z}_{100} \to \mathbb{Z}_{50}, [a]_{100} \mapsto [a]_{50}$.
   i) Δείξτε ότι η f είναι καλά ορισμένη.
   ii) Πόσα στοιχεία έχει η αντίστροφη εικόνα κάθε στοιχείου του $\mathbb{Z}_{50}$;
   iii) Αληθεύει ότι ο περιορισμός της f στο $U(\mathbb{Z}_{100})$ επάγει απεικόνιση $U(\mathbb{Z}_{100}) \to U(\mathbb{Z}_{50})$; Πόσα στοιχεία έχει το σύνολο $f(U(\mathbb{Z}_{100}))$;
4. Πόσα στοιχεία έχει καθένα από τα παρακάτω σύνολα;
   i) $A = \{x \in \mathbb{Z}_{120} : [3]x = [2]\}$,
   ii) $B = \{x \in \mathbb{Z}_{120} : [7]x = [2]\}$,
   iii) $C = \{x \in \mathbb{Z}_{120} : x^2 = [0]\}$,
   iv) $D = \{x \in \mathbb{Z}_{120} : x^k = [0], k \geq 1\}$,
   v) $E = \{x \in \mathbb{Z}_{120} : x^{96} = [1]\}$.
5. Βρείτε
   i) τον ελάχιστο θετικό ακέραιο x ώστε στο $\mathbb{Z}_{100}$ να ισχύει $[7][x] = [2]$,
   ii) το υπόλοιπο της διαίρεσης του 157^{2020} με το 28.
6. Δείξτε ότι κάθε στοιχείο του $\mathbb{Z}_n, n > 0$, που δεν είναι αντιστρέψιμο είναι μηδενοδιαιρέτης.

Ενδεικτικές Λύσεις Επαναληπτικών Ασκήσεων

1. Πρόκειται για τον Ορισμό 2.18 και την Πρόταση 2.19 των σημειώσεων Ορισμός. Ένα στοιχείο $[a] \in \mathbb{Z}_n$ λέγεται αντιστρέψιμο αν υπάρχει $[a'] \in \mathbb{Z}_n$ με $[a][a'] = [a'][a] = [1]$.
Πρόταση. Το $[a] \in \mathbb{Z}_n$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(a, n) = 1$.
Απόδειξη. Έστω $[a]$ αντιστρέψιμο στο $\mathbb{Z}_n$. Τότε υπάρχει $[a'] \in \mathbb{Z}_n$ με $[a][a'] = 1$. Τότε $[aa'] = 1 \Rightarrow aa' = 1 \mod n$. Επομένως $aa' = 1 + kn$, $(k \in \mathbb{Z})$. Έπεται ότι $\mu\kappa\delta(a, n)|1$ άρα $\mu\kappa\delta(a, n) = 1$.
Αντίστροφα, έστω ότι $\mu\kappa\delta(a, n) = 1$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ ώστε $1 = ax + ny$. Επομένως

$$[1] = [ax + ny] = [a][x] + [n][y] = [a][x] + [0][y] = [a][x].$$

Άρα έχουμε $[1] = [a][x]$. Επειδή ο πολλαπλασιασμός του $\mathbb{Z}_n$είναι μεταθετικός, το $[a]$ είναι αντιστρέψιμο.

2. i) Επειδή $n \neq 0$, το σύνολο $\mathbb{Z}_n$ είναι πεπερασμένο. Συνεπώς f_a είναι 1-1 $\Leftrightarrow$ f_a είναι επί. Έστω ότι η f_a είναι επί. Τότε υπάρχει $b \in \mathbb{Z}_n$ με $f_a(b) = [1]$, δηλαδή $ab = [1]$. Επειδή ο πολλαπλασιασμός του $\mathbb{Z}_n$ είναι μεταθετικός, το a είναι αντιστρέψιμο.
Αντίστροφα, αν το a είναι αντιστρέψιμο και $y \in \mathbb{Z}_n$, τότε έχουμε

$$f_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1}y) = y,$$

που σημαίνει ότι η f_a είναι επί.

ii) Έστω $n > 1$. Θα δείξουμε την εξής πρόταση. Η f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\}$ $\Leftrightarrow$ ο n είναι πρώτος.
1η απόδειξη. Από το πρώτο ερώτημα, f_a είναι 1-1 για κάθε $a \in \mathbb{Z}_n - \{[0]\}$ $\Leftrightarrow$ $U(\mathbb{Z}_n) = \mathbb{Z}_n - \{[0]\}$. Από την πρώτη άσκηση, αυτό ισοδυναμεί με $\mu\kappa\delta(i, n) = 1$ για κάθε $i = 1, ..., n-1$. Καθώς $n > 1$, αυτό ισοδυναμεί με το ότι ο n είναι πρώτος γιατί αν $d > 1$ είναι διαιρέτης του n, τότε $\mu\kappa\delta(d, n) = d > 1$.

3. i) Αν $[a]_{100} = [b]_{100}$, τότε $100|a-b$ οπότε $50|a-b$. Άρα $[a]_{50} = [b]_{50}$, δηλαδή $f([a]_{100}) = f([b]_{100})$.

ii) Ξέρουμε ότι $\mathbb{Z}_{100} = \{[0]_{100}, [1]_{100}], \cdots, [99]_{100}\}$ και $\mathbb{Z}_{50} = \{[0]_{50}, [1]_{50}, \cdots, [49]_{50}\}$. Παρατηρούμε ότι

$$\begin{aligned} f([0]_{100}) &= f([50]_{100}) = [0]_{50}, \\ f([1]_{100}) &= f([51]_{100}) = [1]_{50}, \\ &\cdots \\ f([49]_{100}) &= f([99]_{100}) = [49]_{50}, \end{aligned}$$

δηλαδή για κάθε $y = 0, 1, ..., 49$, έχουμε $f^{-1}(\{[y]_{50}\}) = \{[y]_{100}, [y + 50]_{100}\}$. Άρα η αντίστροφη εικόνα κάθε στοιχείου του $\mathbb{Z}_{50}$ έχει 2 στοιχεία.

iii) Αν $[a]_{100} \in U(\mathbb{Z}_{100})$, τότε $\mu\kappa\delta(a, 100) = 1$. Επειδή $50|100$, έπεται ότι $\mu\kappa\delta(a, 50) = 1$ και συνεπώς $[a]_{100} \in U(\mathbb{Z}_{100})$. Αυτό σημαίνει ότι ο περιορισμός της απεικόνισης f στο υποσύνολο $U(\mathbb{Z}_{100})$ του $\mathbb{Z}_{100}$ επάγει απεικόνιση $g : U(\mathbb{Z}_{100}) \to U(\mathbb{Z}_{50}), g([a]_{100}) = f([a]_{100})$.
Θα δείξουμε τώρα ότι η g είναι επί. Πράγματι, αν $[y]_{50} \in \mathbb{Z}_{50}$, τότε $\mu\kappa\delta(y, 50) = 1$. Από αυτό έπεται ότι $\mu\kappa\delta(y, 100) = 1$ γιατί αν υπάρχει πρώτος p με $p|y$ και $p|100$, τότε $p|y$ και $p|50$ (αφού κάθε πρώτος που διαιρεί το 100 διαιρεί και το 50), οπότε $p|\mu\kappa\delta(y, 50) = 1$, αδύνατο. Άρα $[y]_{100} \in U(\mathbb{Z}_{100})$. Από $g([y]_{100}) = [y]_{50}$ έχουμε ότι η g είναι επί.
Άρα

$$|g(U(\mathbb{Z}_{100}))| = |U(\mathbb{Z}_{50})| = \varphi(50) = \varphi(2 \cdot 5^2) = (2 - 1)(5^2 - 5) = 20.$$

4. i) Έστω $x = [a]$. Τότε $[3]x = [2] \Rightarrow 3a = 2 + 120t, t \in \mathbb{Z}, \Rightarrow 3|2$, αδύνατο. Άρα $|A| = 0$.
   ii) Το $[7]$ είναι αντιστρέψιμο στο $\mathbb{Z}_{120}$ αφού $\mu\kappa\delta(7, 120) = 1$. Έχουμε $[7]x = [2] \Leftrightarrow [7]^{-1}[7]x = [7]^{-1}[2] \Leftrightarrow x = [7]^{-1}[2]$. Άρα $|B| = 1$.
   iii) Έστω $x = [a]$. Έχουμε

$$[a]^2 = [0] \Leftrightarrow [a^2] = [0] \Leftrightarrow 2^3 \cdot 3 \cdot 5 | a^2 \Leftrightarrow \begin{cases} 2^3|a^2 \\ 3|a^2 \\ 5|a^2 \end{cases}$$

   όπου στο αντίστροφο στην τελευταία ισοδυναμία χρησιμοποιήσαμε ότι οι $2^3, 3, 5$ είναι ανά δύο σχετικά πρώτοι(άσκηση 1.3 ii των σημειώσεων). Συνεχίζουμε

$$\begin{cases} 2^3|a^2 \\ 3|a^2 \\ 5|a^2 \end{cases} \Leftrightarrow \begin{cases} 2^2|a \\ 3|a \\ 5|a \end{cases} \Leftrightarrow 2^2 \cdot 3 \cdot 5 | a.$$

   Στη συνεπαγωγή $2^3|a^2 \Rightarrow 2^2|a$ χρησιμοποιήσαμε την Παρατήρηση (3) μετά το Θεώρημα 1.12 των σημειώσεων. Στις συνεπαγωγές $3|a^2 \Rightarrow 3|a$ και $5|a^2 \Rightarrow 5|a$ χρησιμοποιήσαμε το λήμμα του Ευκλείδη. Τέλος στο ευθύ της τελευταίας ισοδυναμίας, χρησιμοποιήσαμε ότι οι ακέραιοι $2^2, 3, 5$ είναι ανά δύο σχετικά πρώτοι. (Προσοχή. Σε γραπτά εξετάσεων αντίστοιχες δικαιολογήσεις τέτοιων επιχειρημάτων πρέπει να υπάρχουν). Οι φυσικοί αριθμοί που είναι πολλαπλάσιοι του $2^2 \cdot 3 \cdot 5 = 60$ και μικρότεροι του 120 είναι οι 0, 60 και συνεπώς οι ζητούμενες λύσεις είναι οι $x = [0], [60]$. Άρα $|C| = 2$.
   iv) Θα δείξουμε ότι $D = \{[0], [30], [60], [90]\}$, οπότε $|D| = 4$.
   Έστω $x = [a] \in D$, οπότε για κάποιο $k \geq 1$, $[a]^k = [0]$. Έχουμε

$$[a]^k = [0] \Rightarrow [a^k] = [0] \Rightarrow 2^3 \cdot 3 \cdot 5 | a^k \Rightarrow \begin{cases} 2^3|a^k \\ 3|a^k \\ 5|a^k \end{cases} \Rightarrow \begin{cases} 2|a \\ 3|a \\ 5|a \end{cases} \Rightarrow 30|a,$$

   όπου στην προτελευταία συνεπαγωγή χρησιμοποιήσαμε το λήμμα του Ευκλείδη τρεις φορές και στην τελευταία ότι οι 2,3,5 είναι ανά δύο σχετικά πρώτοι (άσκηση 1.3 ii). Άρα $D \subseteq \{[0], [30], [60], [90]\}$. Η σχέση $\{[0], [30], [60], [90]\} \subseteq D$ επαληθεύεται με άμεσο υπολογισμό: $[30]^3 = [2^3 \cdot 3^3 \cdot 5^3] = [0]$ και άρα για κάθε ακέραιο πολλαπλάσιο $30m$ του 30 έχουμε $[30m]^3 = [30]^3[m]^3 = [0]$.
   v) Θα δείξουμε ότι $E = U(\mathbb{Z}_{120})$, οπότε $|E| = \varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = (2^3 - 2^2)(3 - 1)(5 - 1) = 32$.
   Η σχέση $E \subseteq U(\mathbb{Z}_{120})$ είναι σαφής γιατί αν $x^{96} = [1]$, τότε $xx^{95} = x^{95}x = [1]$ που σημαίνει εξ ορισμού ότι το x είναι αντιστρέψιμο.
   Αντίστροφα, έστω $x \in U(\mathbb{Z}_{120})$. Από το θεώρημα του Euler έχουμε $x^{\varphi(120)} = [1]$, δηλαδή $x^{32} = [1]$. Άρα $x^{96} = (x^{32})^3 = [1]^3 = [1]$. Συνεπώς $U(\mathbb{Z}_{120}) \subseteq E$.

5. i) Επειδή $\mu\kappa\delta(7, 100) = 1$, το $[7] \in \mathbb{Z}_{100}$ είναι αντιστρέψιμο και έχουμε $[7][x] = [2] \Leftrightarrow [x] = [7]^{-1}[2]$. Θα υπολογίσουμε το $[7]^{-1}$ με τον Ευκλείδειο αλγόριθμο κατά τα γνωστά.

$$\begin{aligned} 100 &= 14 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

   και $1 = 7 - 3 \cdot 2 = 7 - 3(100 - 14 \cdot 7) = 43 \cdot 7 + (-3) \cdot 100$. Άρα $[7]^{-1} = [43]$ και $[x] = [43][2] = [86]$. Τώρα επειδή $[86] = \{86 + 100t : t \in \mathbb{Z}\} = \{\cdots, -14, 86, 186, \cdots\}$, είναι σαφές ότι ο ελάχιστος θετικός ακέραιος του συνόλου $[86]$ είναι ο 86.

ii) Έχουμε $157 \equiv 17 \mod 28$, $\varphi(28) = \varphi(2^2 \cdot 7) = 2 \cdot 6 = 12$ και $2020 = 168 \cdot 12 + 4$. Άρα
$$157^{2020} \equiv 17^{2020} \equiv (17^{12})^{168} \cdot 17^4 \mod 28.$$
Καθώς $\mu\kappa\delta(17, 28) = 1$, εφαρμόζει το θεώρημα του Euler και έχουμε
$$(17^{12})^{168} \cdot 17^4 \equiv 1^{168} \cdot 17^4 \equiv 17^4 \mod 28.$$
Με άμεσες πράξεις έχουμε $17^4 \equiv (-11)^4 \equiv 121^2 \equiv 9^2 \equiv 25 \mod 28$, οπότε το ζητούμενο υπόλοιπο είναι 25.

6. Πράγματι, αν το $x = [a]$ δεν είναι αντιστρέψιμο, τότε $d > 1$, όπου $d = \mu\kappa\delta(a, n)$. Για τον ακέραιο $m = \frac{n}{d}$ έχουμε $1 \leq m < n$ και άρα στο $\mathbb{Z}_n$ είναι $[m] \neq [0]$. Επειδή $[a][m] = [\frac{a}{d}][n] = [0]$, x είναι μηδενοδιαιρέτης.

Μέρος 2

Δακτύλιοι

Δακτύλιοι, περιοχές και σώματα

Στο Μέρος 2 (Κεφάλαια 3-6) εισάγουμε και μελετάμε τη δομή του δακτυλίου. Δίνουμε έμφαση στους δακτυλίους πολυωνύμων με συντελεστές από σώμα.

Ο σκοπός του Κεφαλαίου 3 είναι να εισάγουμε την έννοια του δακτυλίου. Θα αναφερθούμε σε δύο σημαντικές οικογένειες δακτυλίων που είναι οι περιοχές και τα σώματα. Μετά εξετάζουμε το διωνυμικό ανάπτυγμα για στοιχεία που μετατίθενται και την έννοια του υποδακτύλιου.

Βασικά σημεία

- δακτύλιοι, περιοχές και σώματα
- διωνυμικό ανάπτυγμα
- ευθύ γινόμενο δακτυλίων

3.1. Δακτύλιοι

Στο Κεφάλαιο 2 είχαμε αναφερθεί στην έννοια της πράξης. Θυμίζουμε ότι μια πράξη σε ένα μη κενό σύνολο A είναι μια απεικόνιση της μορφής $A \times A \to A$.

Παραδείγματα 3.1.

(1) Η συνήθης πρόσθεση ακεραίων $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto a + b$ και ο συνήθης πολλαπλασιασμός ακεραίων $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(a, b) \mapsto a \cdot b$ είναι πράξεις στο $\mathbb{Z}$.

(2) Στο $\mathbb{Z}_n$ είχαμε ορίσει τις πράξεις,

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad ([a], [b]) \mapsto [a + b]$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad ([a], [b]) \mapsto [a \cdot b].$$

(3) Η αντιστοιχία $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$, με $([a], [b]) \mapsto [c], \quad c = \max\{a, b\}$. δεν είναι πράξη (δηλαδή δεν είναι απεικόνιση). Πράγματι έχουμε,

$$([0], [1]) = ([2], [1]),\ ([0], [1]) \mapsto [1],\ ([2], [1]) \mapsto [2],$$

αλλά $[1] \neq [2]$.

(4) Συμβολίζουμε με $M_n(\mathbb{R})$ το σύνολο των $n \times n$ πινάκων με στοιχεία από το $\mathbb{R}$. Η συνήθης πρόσθεση πινάκων και ο συνήθης πολλαπλασιασμός πινάκων που ξέρουμε από τη Γραμμική Άλγεβρα είναι πράξεις στο $M_n(\mathbb{R})$

$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \mapsto M_n(\mathbb{R}), \quad (A, B) \mapsto A + B,$$
$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \mapsto M_n(\mathbb{R}), \quad (A, B) \mapsto A \cdot B.$$

Ορισμός 3.2.

- *Ένας* **δακτύλιος** *είναι ένα σύνολο R εφοδιασμένο με δύο πράξεις*

$$R \times R \to R, \quad (a, b) \mapsto a + b,$$
$$R \times R \to R, \quad (a, b) \mapsto a \cdot b,$$

που ικανοποιούν τις παρακάτω ιδιότητες.

(1) $\forall a, b, c \in R, (a+b)+c = a+(b+c)$ *(προσεταιριστική ιδιότητα της πρόσθεσης)*
(2) $\exists 0_R \in R, \forall a \in R, a + 0_R = 0_R + a = a$ *(ύπαρξη ουδετέρου στοιχείου)*
(3) $\forall a \in R, \exists a' \in R, a + a' = 0_R = a' + a$ *(ύπαρξη αντιθέτου)*
(4) $\forall a, b \in R, a + b = b + a$ *(μεταθετική ιδιότητα της πρόσθεσης)*
(5) $\forall a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(προσεταιριστική ιδιότητα του πολλαπλασιασμού)*
(6) $\forall a, b, c \in R, a(b + c) = a \cdot b + a \cdot c$ *(επιμεριστική ιδιότητα από αριστερά)*
(7) $\forall a, b, c \in R, (a + b) \cdot c = a \cdot c + b \cdot c$ *(επιμεριστική ιδιότητα από δεξιά)*

- *Έστω R δακτύλιος.*
  - *Αν $a \cdot b = b \cdot a \ \forall a, b \in R$, θα λέμε ότι ο R είναι* **μεταθετικός**.
  - *Αν $\exists 1_R \in R$ τέτοιο ώστε $1_R \cdot a = a \cdot 1_R = a \ \forall a \in R$, θα λέμε ότι ο R έχει* **μοναδιαίο στοιχείο** *το 1_R.*

Σημείωση. Όταν θέλουμε να τονίσουμε το συμβολισμό των πράξεων

$$R \times R \to R, \quad (a, b) \mapsto a + b,$$
$$R \times R \to R, \quad (a, b) \mapsto a \cdot b,$$

ενός δακτυλίου R, θα γράφουμε $(R, +, \cdot)$ στη θέση του R.

Παρατήρηση. Αν R είναι δακτύλιος, τότε:

(1) Το 0_R είναι μοναδικό.

(2) Για κάθε $a \in R$, το a' είναι μοναδικό.

(3) Αν ο R έχει μοναδιαίο στοιχείο, τότε το στοιχείο αυτό είναι μοναδικό.

Απόδειξη. (1) Έστω $0_R, 0'_R \in R$ ώστε $0_R + a = a + 0_R = a = 0'_R + a = a + 0'_R$, για κάθε $a \in R$. Τότε $0_R = 0_R + 0'_R = 0'_R$.
(2) Έστω $a, a', a'' \in R$ ώστε $a + a' = 0_R = a'' + a$. Τότε

$$a'' = a'' + 0_R = a'' + (a + a') = (a'' + a) + a' = 0_R + a' = a'.$$

(3) Είναι το πολλαπλασιαστικό ανάλογο της ιδιότητας (1) και η απόδειξη είναι ίδια με πολλαπλασιαστικό συμβολισμό. Δηλαδή, έστω $1_R, 1'_R \in R$ ώστε $1_R \cdot a = a \cdot 1_R = a = 1'_R \cdot a = a \cdot 1'_R$, για κάθε $a \in R$. Τότε $1_R = 1_R \cdot 1'_R = 1'_R$. □

Το στοιχείο 0_R του Ορισμού 3.2 λέγεται το **μηδενικό στοιχείο** του R, το στοιχείο a' λέγεται το **αντίθετο** του a και το στοιχείο 1_R (αν υπάρχει) λέγεται το **μοναδιαίο στοιχείο** του R (ή η **μονάδα** του R).

Παραδείγματα 3.3.

(1) Τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ με την πρόσθεση και τον πολλαπλασιασμό αριθμών είναι μεταθετικοί δακτύλιοι με μηδενικό στοιχείο τον αριθμό 0 και μοναδιαίο στοιχείο τον αριθμό 1. Με τις πράξεις αυτές το σύνολο $\mathbb{N}$ δεν είναι δακτύλιος καθώς δεν αληθεύει η ιδιότητα (3) του Ορισμού 3.2.

(2) **Ακέραιοι modulo n** Το σύνολο $\mathbb{Z}_n$ με τις πράξεις που ορίσαμε στην Παράγραφο 2.3 είναι μεταθετικός δακτύλιος με μηδενικό στοιχείο το $[0]$ και μοναδιαίο στοιχείο το $[1]$. Το αντίθετο του $[a]$, είναι το $[-a]$. Καλό είναι να συγκριθεί η Πρόταση 2.15 με τον Ορισμό 3.2.

(3) **Πίνακες** Το σύνολο $M_n(\mathbb{R})$ με τις πράξεις του Παραδείγματος 3.1(4) είναι δακτύλιος, όχι μεταθετικός αν $n > 1$, με μηδενικό στοιχείο τον μηδενικό πίνακα και μοναδιαίο στοιχείο το ταυτοτικό πίνακα $I_n = 1_{M_n(\mathbb{R})} = diag(1, 1, ..., 1)$. Οι ιδιότητες του Ορισμού 3.2, όπως για παράδειγμα η προσεταιριστικότητα του γινομένου πινάκων, είναι γνωστές από τη Γραμμική Άλγεβρα.

Με παρόμοιο τρόπο και το σύνολο $M_n(\mathbb{Z})$ των $n \times n$ πινάκων με στοιχεία ακέραιους είναι δακτύλιος με μοναδιαίο στοιχείο που δεν είναι μεταθετικός αν $n > 1$.

Πιο γενικά, έστω R δακτύλιος και $M_n(R)$ το σύνολο των $n \times n$ πινάκων με στοιχεία από το R εφοδιασμένος με τις πράξεις που ορίζονται από

$$A + B = (a_{ij} + b_{ij}),$$
$$AB = (c_{ij}),$$

όπου $A = (a_{ij}), B = (b_{ij}), c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$. Το $M_n(R)$ είναι δακτύλιος. Αν επιπλέον ο R έχει μοναδιαίο στοιχείο το 1_R, τότε ο $M_n(R)$ έχει μοναδιαίο στοιχείο το

$$diag(1_R, 1_R, ..., 1_R).$$

(4) Εύκολα επαληθεύεται ότι το σύνολο $2\mathbb{Z}$ των αρτίων ακεραίων είναι μεταθετικός δακτύλιος ως προς την πρόσθεση και τον πολλαπλασιασμό ακεραίων. Όμως δεν έχει μοναδιαίο στοιχείο καθώς δεν υπάρχει άρτιος ακέραιος m με $ma = a$ για κάθε $a \in 2\mathbb{Z}$.

(5) Ως προς την πρόσθεση και τον πολλαπλασιασμό πραγματικών αριθμών, το σύνολο

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Παρατηρούμε ότι αν $a, b, c, d \in \mathbb{Q}$, τότε

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + c + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}], \text{ και}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}],$$

(αφού $ac + 2bd, ad + bc \in \mathbb{Q}$). Άρα πράγματι η πρόσθεση και το γινόμενο πραγματικών αριθμών παρέχουν πράξεις πράξεις στο $\mathbb{Q}[\sqrt{2}]$. Η επαλήθευση των ιδιοτήτων του Ορισμού 3.2 για $\mathbb{Q}[\sqrt{2}]$ είναι άμεση.

(6) **Ακέραιοι του Gauss** Ως προς την πρόσθεση και τον πολλαπλασιασμό μιγαδικών αριθμών, το σύνολο

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\},$$

όπου $i^2 = -1$, είναι μεταθετικός δακτύλιος με μονάδα (το 1). Όπως πριν, αν $a, b, c, d \in \mathbb{Z}$ έχουμε

$$(a + bi) + (c + di) = a + c + (b + d)i \in \mathbb{Z}[i], \text{και}$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i],$$

και άρα οι συνήθεις πράξεις της $+$ και του $\cdot$ του $\mathbb{C}$ δίνουν πράξεις στο $\mathbb{Z}[i]$.

(7) Έστω V ένας $\mathbb{R}$- διανυσματικός χώρος και ·έστω

$$\mathcal{L}(V) = \{f : V \to V : f \text{ γραμμική}\}.$$

Από τη Γραμμική Άλγεβρα θυμόμαστε ότι το άθροισμα και η σύνθεση δύο γραμμικών απεικονίσεων $V \to V$ είναι γραμμικές απεικονίσεις. Συνεπώς έχουμε τις εξής πράξεις στο $\mathcal{L}(V)$,

$$+ : \mathcal{L}(V) \times \mathcal{L}(V) \to \mathcal{L}(V), (f + g)(v) = f(v) + g(v),$$
$$\cdot : \mathcal{L}(V) \times \mathcal{L}(V) \to \mathcal{L}(V), (f \circ g)(v) = f(g(v)) \text{ (σύνθεση απεικονίσεων)}$$

Εύκολα ελέγχουμε ότι ο $\mathcal{L}(V)$ είναι ένας δακτύλιος με μηδενικό στοιχείο τη μηδενική απεικόνιση $0 : V \to V, v \mapsto 0_V$. Ο δακτύλιος αυτός γενικά δεν είναι μεταθετικός αλλά έχει

μοναδιαίο στοιχείο (την ταυτοτική απεικόνιση $V \to V, v \mapsto v$). Ενδεικτικά Θα δείξουμε ότι $f \circ (g+h) = f \circ g + f \circ h$. Πράγματι έχουμε,

$$\begin{aligned} f \circ (g+h)(v) &= f((g+h)(v)) = f(g(v)+h(v)) \\ &= f(g(v)) + f(h(v)) = f \circ g(v) + f \circ h(v) \\ &= (f \circ g + f \circ h)(v), \end{aligned}$$

για κάθε $v \in V$. Επομένως $f \circ (g+h) = f \circ g + f \circ h$. Ο δακτύλιος αυτός δεν είναι γενικά μεταθετικός.

(8) Το σύνολο $F(\mathbb{R}, \mathbb{R})$ όλων των απεικονίσεων $f : \mathbb{R} \to \mathbb{R}$ είναι ένας δακτύλιος ως προς τις πράξεις

$$\begin{aligned} + &: F(\mathbb{R},\mathbb{R}) \times F(\mathbb{R},\mathbb{R}) \to F(\mathbb{R},\mathbb{R}), (f,g) \mapsto f+g, \\ \cdot &: F(\mathbb{R},\mathbb{R}) \times F(\mathbb{R},\mathbb{R}), (f,g) \mapsto f \cdot g \end{aligned}$$

όπου

$$\begin{aligned} f+g : \mathbb{R} \to \mathbb{R}, (f+g)(x) = f(x)+g(x), \quad \text{και} \\ f \cdot g : \mathbb{R} \to \mathbb{R}, (f \cdot g)(x) = f(x)g(x). \end{aligned}$$

Ο δακτύλιος αυτός έχει μοναδιαίο στοιχείο τη σταθερή απεικόνιση $\mathbb{R} \to \mathbb{R}$, $x \mapsto 1$, και είναι μεταθετικός.

Πιο γενικά, έστω X ένα μη κενό σύνολο και R ένας δακτύλιος. Στο σύνολο $F(X,R)$ όλων των απεικονίσεων $X \to R$ ορίζουμε πράξεις $+, \cdot$ με τρόπο παρόμοιο προς τον προηγούμενο. Δηλαδή αν $f, g \in F(X,R)$, ορίζουμε $f+g \in F(X,R)$ όπου $(f+g)(x) = f(x)+g(x)$ για κάθε $x \in X$, και $fg \in F(X,R)$, όπου $fg(x) = f(x)g(x)$ για κάθε $x \in X$. Ως προς τις πράξεις αυτές το $F(X,R)$ είναι ένας δακτύλιος.

(9) Θεωρούμε το σύνολο $\mathbb{Z}$ με πράξεις $a \oplus b = a - b$ και $a \cdot b = ab$. Ως προς τις πράξεις αυτές το $\mathbb{Z}$ δεν είναι δακτύλιος. Για παράδειγμα δεν αληθεύει γενικά ότι $a \oplus b = b \oplus a$ για κάθε $a, b \in \mathbb{Z}$, καθώς $2 - 1 \neq 1 - 2$.

Σε σχέση με τους συμβολισμούς του Ορισμού 3.2, από τώρα και στο εξής θα γράφουμε συνήθως ab αντί $a \cdot b$. Επίσης θα συμβολίζουμε το αντίθετο του a με $-a$. Συνεπώς εξ ορισμού έχουμε $a + (-a) = (-a) + a = 0_R$.

Αν ο δακτύλιος R έχει μοναδιαίο στοιχείο 1_R, τότε έχουμε το αντίθετο στοιχείο -1_R και το γινόμενο $(-1_R)a$ των στοιχείων -1_R και a, όπου $a \in R$. Επίσης έχουμε το αντίθετο $-a$ του a. Η επόμενη πρόταση λέει, μεταξύ των άλλων, ότι $(-1_R)a = -a$

Πρόταση 3.4. *Έστω R δακτύλιος και $a, b, c \in R$. Ισχύουν τα εξής.*

(1) *Αν $a + b = a + c$, τότε $b = c$.*
(2) $-(-a) = a$.
(3) $0_R a = a 0_R = 0_R$.
(4) $-(a+b) = (-a) + (-b)$.
(5) $(-a)b = a(-b) = -(ab)$.
(6) $(-a)(-b) = ab$.

Απόδειξη. (1) Έστω $a, b, c \in R$ με $a + b = a + c$. Τότε (αφού η $+$ είναι πράξη) έχουμε $a' + (a + b) = a' + (a + c)$, επομένως

$$(a' + a) + b = (a' + a) + c \Rightarrow 0_R + b = 0_R + c \Rightarrow b = c.$$

(2) Έπεται άμεσα από την ιδιότητα (4) του Ορισμού 3.2,

$$a + (-a) = (-a) + a = 0_R$$

(λόγω συμμετρίας) και την μοναδικότητα του $-(-a)$.
(3) Επειδή $0_R + 0_R = 0_R$ και ο πολλαπλασιασμός είναι πράξη, παίρνουμε

$$(0_R + 0_R)a = 0_R a \Rightarrow 0_R a + 0_R a = 0_R a + 0_R \Rightarrow 0_R a = 0_R.$$

(4) Παρατηρούμε ότι

$$\begin{aligned}(a+b)+((-a)+(-b)) &= (a+b)+((-b)+(-a))\\ &= ((a+b)+(-b))+(-a)\\ &= (a+(b+(-b)))+(-a)\\ &= (a+0_R)+(-a)\\ &= a+(-a)=0_R.\end{aligned}$$

Επομένως $-(a+b) = (-a)+(-b)$.
(5) Έχουμε $a+(-a) = 0_R \Rightarrow (a+(-a))b = 0_R b \Rightarrow ab + (-a)b = 0_R \Rightarrow (-a)b = -(ab)$. Η απόδειξη της $a(-b) = -(ab)$ είναι παρόμοια (άσκηση).
(6) Βάζουμε στη (5) όπου b το $-b$ και χρησιμοποιούμε την ιδιότητα (2). □

Ορισμός 3.5. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο 1_R. Ένα στοιχείο $r \in R$ λέγεται **αντιστρέψιμο**, αν υπάρχει $r' \in R$ ώστε $rr' = r'r = 1_R$. Στην περίπτωση αυτή θα λέμε ότι το r' είναι το **αντίστροφο** του r και το συμβολίζουμε με $r' = r^{-1}$. Το σύνολο των αντιστρέψιμων στοιχείων του R συμβολίζεται με $U(R)$.*

Ας δείξουμε ότι το αντίστροφο στοιχείο του προηγούμενου ορισμού είναι πράγματι μοναδικό. Αυτό έπεται από το πολλαπλασιαστικό ανάλογο της Παρατήρησης (1) που είδαμε αμέσως μετά τον Ορισμό 3.2. Επαναλαμβάνουμε το επιχείρημα για να είμαστε σαφείς. Έστω $r, r', r'' \in R$, όπου R δακτύλιος με μοναδιαίο στοιχείο, τέτοια ώστε

$$rr' = r'r = 1_R \quad \text{και} \quad rr'' = r''r = 1_R.$$

Τότε έχουμε $r'' = 1_R r'' = (r'r)r'' = r'(rr'') = r'(1_R) = r'$.

Παραδείγματα 3.6.

(1) Είναι σαφές ότι $U(\mathbb{Z}) = \{1, -1\}$ και $U(\mathbb{R}) = \mathbb{R} - \{0\}$.

(2) Σύμφωνα με την Πρόταση 2.18 έχουμε $U(\mathbb{Z}_n) = \{[a] \in \mathbb{Z}_n : \mu\kappa\delta(a,n) = 1\}$. Για παράδειγμα, $U(\mathbb{Z}_{10}) = \{[1], [3], [7], [9]\}$.

(3) Τα αντιστρέψιμα στοιχεία του δακτυλίου των ακεραίων του Gauss $\mathbb{Z}[i]$ είναι

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\},$$

Πράγματι, είναι σαφές ότι $\{1, -1, i, -i\} \subseteq U(\mathbb{Z}[i])$. (Για παράδειγμα $i(-i) = 1 \Rightarrow i, -i \in U(\mathbb{Z}[i])$, δηλαδή το $\pm i$ είναι αντιστρέψιμο.) Έστω $a + bi \in U(\mathbb{Z}[i])$, όπου $a, b \in \mathbb{Z}$. Τότε υπάρχουν $c, d \in \mathbb{Z}$ ώστε $(a+bi)(c+di) = 1$. Παίρνοντας μέτρα μιγαδικών και χρησιμοποιώντας ότι $|z_1 z_2| = |z_1||z_2|$, όπου $z_1, z_2 \in \mathbb{C}$, έχουμε,

$$|a+bi||c+di| = 1 \Rightarrow |a+bi|^2|c+di|^2 = 1 \Rightarrow (a^2+b^2)(c^2+d^2) = 1.$$

Επειδή $a, b, c, d \in \mathbb{Z}$, παίρνουμε $(a,b) = (1,0), (-1,0), (0,1), (0,-1)$. Άρα $a+bi = \pm 1, \pm i$.

(4) Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, Παράδειγμα 3.6(4), είναι

$$U(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}[\sqrt{2}] - \{0\}.$$

Παρατηρούμε πρώτα ότι αν $a, b \in \mathbb{Q}$ τότε $a + b\sqrt{2} = 0$ αν και μόνο αν $a = b = 0$. Πράγματι, αν $a + b\sqrt{2} = 0$, με $b \neq 0$, τότε $\sqrt{2} = -\frac{a}{b} \in \mathbb{Q}$, το οποίο είναι άτοπο ($\sqrt{2} \notin \mathbb{Q}$).

Έστω $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ με $a+b\sqrt{2} \neq 0$. Αρκεί να δείξουμε ότι το $a+b\sqrt{2}$ είναι αντιστρέψιμο. Πράγματι έχουμε,

$$\begin{aligned} \frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} \\ &= \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}], \end{aligned}$$

αφού $a^2-2b^2 \neq 0$ (διαφορετικά $\sqrt{2} \in \mathbb{Q}$, άτοπο) και $a, b, a^2-2b^2 \in \mathbb{Q}$.

(5) Από τη Γραμμική Άλγεβρα ξέρουμε ότι τα αντιστρέψιμα στοιχεία του δακτυλίου $M_n(\mathbb{R})$ είναι ακριβώς οι πίνακες $A \in M_n(\mathbb{R})$ που έχουν μη μηδενική ορίζουσα, $\det A \neq 0$. Για παράδειγμα, ο

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$$

είναι αντιστρέψιμο στοιχείο και $A^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{-1}{2} \\ 0 & 1 \end{pmatrix}$. Παρατηρούμε ότι αν και ο A έχει ακέραια στοιχεία, ο αντίστροφός του στο $M_2(\mathbb{R})$ δεν έχει ακέραια στοιχεία. Δηλαδή, ως στοιχείο του $M_2(\mathbb{Z})$ το A **δεν** είναι αντιστρέψιμο .
Θα δείξουμε τώρα ότι τα αντιστρέψιμα στοιχεία του δακτυλίου $M_n(\mathbb{Z})$ είναι ακριβώς οι πίνακες $A \in M_n(\mathbb{Z})$ με $\det A \in \{1, -1\}$, δηλαδή

$$U(M_n(\mathbb{Z})) = \{A \in M_n(\mathbb{Z}) : \det A \in \{1, -1\}\}.$$

Για το σκοπό αυτό υπενθυμίζουμε τη σχέση

$$A(adj(A)) = (adj(A))A = (detA)I_n,$$

όπου $A \in M_n(\mathbb{R})$, I_n είναι ο $n \times n$ ταυτοτικός πίνακας και $adj(A)$ είναι ο προσαρτημένος πίνακας του A, δηλαδή ο $n \times n$ πίνακας που στη θέση (i,j) έχει το στοιχείο $(-1)^{i+j} \det A_{ji}$, όπου A_{ji} είναι ο πίνακας που προκύπτει από τον A κατόπιν διαγραφής της j γραμμής και i στήλης. Αν $A \in M_n(\mathbb{Z})$ και $\det A \in \{1, -1\}$, τότε θέτοντας

$$B = \frac{1}{detA}(adj(A))$$

παρατηρούμε ότι τα στοιχεία του B είναι ακέραιοι, δηλαδή $B \in M_n(\mathbb{Z})$, και επίσης $AB = BA = I_n$. Άρα $A \in U(M_n(\mathbb{Z}))$. Αντίστροφα, έστω ότι $A \in U(M_n(\mathbb{Z}))$, δηλαδή ότι υπάρχει $B \in M_n(\mathbb{Z})$ με $AB = BA = I_n$. Λαμβάνοντας ορίζουσες παίρνουμε $\det A \det B = 1$ και επειδή οι A, B έχουν στοιχεία ακέραιους, παίρνουμε ότι ο ακέραιος $\det A$ διαιρεί το 1, οπότε $\det A \in \{1, -1\}$.

Παραλείποντας παρενθέσεις

Έστω R δακτύλιος και $a, b, c, d \in R$. Από την προσεταιριστική ιδιότητα της πρόσθεσης έχουμε

$$(a+b)+c = a+(b+c).$$

Το στοιχείο αυτό θα το συμβολίζουμε απλά $a+b+c$. Από την ίδια ιδιότητα έχουμε

$$a+(b+(c+d)) = (a+b)+(c+d) = ((a+b)+c)+d = (a+(b+c))+d = a+((b+c)+d).$$

Το στοιχείο αυτό θα το συμβολίζουμε απλά $a+b+c+d$.

Όμοια για τον πολλαπλασιασμό η αντίστοιχη προσεταιριστική ιδιότητα λέει ότι $(ab)c = a(bc)$. Το στοιχείο αυτό θα το συμβολίζουμε απλά abc. Επίσης,

$$a(b(cd)) = (ab)(cd) = ((ab)c)d = (a(bc))d = a((bc)d).$$

Το στοιχείο αυτό θα το συμβολίζουμε απλά $abcd$. (Η γενίκευση των παραπάνω σε περισσότερους παράγοντες καλείται η γενικευμένη προσεταιριστική ιδιότητα και παραπέμπουμε στην Παράγραφο 6.2 του βιβλίου για την αυστηρή διατύπωση και απόδειξη.)

3.2. Περιοχές και σώματα

Ορισμός 3.7. *Ένας δακτύλιος R λέγεται* **περιοχή** *(ή* **ακέραια περιοχή***) αν,*

(1) *είναι μεταθετικός,*
(2) *έχει μοναδιαίο στοιχείο $1_R \neq 0_R$, και*
(3) *αν $a, b \in R$ με $ab = 0_R$, τότε $a = 0_R$ ή $b = 0_R$.*

Νόμος διαγραφής σε περιοχή
Σημειώνουμε ότι αν ο R είναι περιοχή και ισχύει $ab = ac$, όπου $a, b, c \in R$ με $a \neq 0_R$, τότε $b = c$. Πράγματι, από $ab = ac$ έχουμε $a(b - c) = 0_R$ και η ιδιότητα (3) του ορισμού δίνει $b - c = 0_R$.

Παραδείγματα 3.8.

(1) Οι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι περιοχές.
(2) Οι $\mathbb{Z}[i]$ και $\mathbb{Q}[\sqrt{2}]$ (βλ. Παραδείγματα 3.3(5) και (6)) είναι περιοχές.
(3) Ο $\mathbb{Z}_6$ δεν είναι περιοχή. Πράγματι στο $\mathbb{Z}_6$ έχουμε $[2][3] = [6] = [0]$, ενώ $[2] \neq [0]$ και $[3] \neq [0]$.
(4) Θεωρούμε το δακτύλιο $F(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \text{ συνάρτηση}\}$ του Παραδείγματος 3.4(8). Ο $F(\mathbb{R}, \mathbb{R})$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο τη συνάρτηση $\mathbb{R} \to \mathbb{R}$, $x \mapsto 1$. Όμως ο $F(\mathbb{R}, \mathbb{R})$ δεν είναι περιοχή, αφού μπορούμε να βρούμε $f, g : \mathbb{R} \to \mathbb{R}$ με $f, g \neq 0$ και $f \cdot g = 0$. Για παράδειγμα,

$$f(x) = \begin{cases} 0, & x \leq 0 \\ x, & x > 0 \end{cases}, \quad g(x) = \begin{cases} x, & x \leq 0 \\ 0, & x > 0 \end{cases}.$$

Παρατηρήσεις.

- Η συνθήκη (2) στον Ορισμό 3.7 λέει ότι ο δακτύλιος R έχει μοναδιαίο στοιχείο και $R \neq \{0_R\}$.
- Ένα στοιχείο a μεταθετικού δακτυλίου R λέγεται **μηδενοδιαιρέτης** αν υπάρχει $b \in R$, $b \neq 0_R$, με $ab = 0_R$. Με την ορολογία αυτή, η συνθήκη (3) στον Ορισμό 3.7 ισοδυναμεί με τη μη ύπαρξη μη μηδενικών μηδενοδιαιρετών στο R.

Πρόταση 3.9. *Έστω $n \in \mathbb{N}$. Τότε $\mathbb{Z}_n$ είναι περιοχή αν και μόνο αν ο n είναι πρώτος ή $n = 0$.*

Απόδειξη. Έστω ότι $\mathbb{Z}_n$ είναι περιοχή. Τότε $n \neq 1$ (γιατί $\mathbb{Z}_1 = \{[0]\}$ δεν είναι περιοχή). Έστω λοιπόν $n > 1$ και έστω $n = ab$, $a, b \in \mathbb{N}$. Τότε $[n] = [ab]$, δηλαδή $[0] = [a][b]$. Επειδή $\mathbb{Z}_n$ περιοχή, έχουμε $[a] = [0]$ ή $[b] = [0]$, δηλαδή $n|a$ ή $n|b$. Άρα $n = a$ ή $n = b$, οπότε ο n είναι πρώτος.

Αντίστροφα, αν $n = [0]$, τότε $\mathbb{Z}_0 = \mathbb{Z}$ που είναι περιοχή. Έστω τώρα ότι ο n είναι πρώτος. Τότε $n > 1$, άρα $[1] \neq [0]$. Ο $\mathbb{Z}_n$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το $[1] \neq [0]$. Αν $[a][b] = [0]$, όπου $a, b \in \mathbb{Z}$, τότε $[ab] = [0] \Rightarrow n|ab$ και αφού ο n είναι πρώτος έπεται ότι $n|a$ ή $n|b$, δηλαδή $[a] = [0]$ ή $[b] = [0]$. □

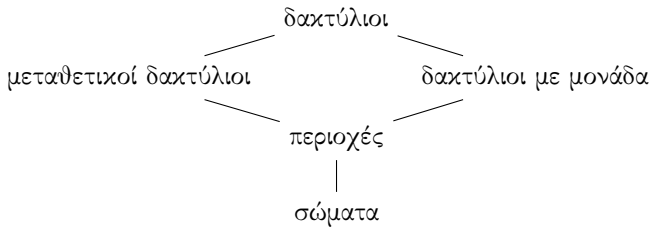
Ορισμός 3.10. *Ένας δακτύλιος R λέγεται* **σώμα** *αν,*

(1) *είναι μεταθετικός,*
(2) *έχει μοναδιαίο στοιχείο $1_R \neq 0_R$,*
(3) *κάθε $r \in R$, $r \neq 0_R$, είναι αντιστρέψιμο.*

Πρόταση 3.11. *Κάθε σώμα είναι περιοχή.*

Απόδειξη. Πράγματι, έστω $ab = 0_R$ $(a, b \in R)$ και $a \neq 0_R$. Τότε υπάρχει το αντίστροφο του a. Χρησιμοποιώντας την Πρόταση 3.4(2) παίρνουμε $0_R = a^{-1}0_R = a^{-1}(ab) = (a^{-1}a)b = 1_R b = b$. □

Σχηματικά έχουμε τις εξής σχέσεις υποσυνόλων,



Παραδείγματα 3.12.

(1) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα, ενώ ο $\mathbb{Z}$ δεν είναι σώμα.

(2) Ο δακτύλιος $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in R : a, b \in \mathbb{Q}\}$ είναι σώμα. Πράγματι είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1 \neq 0$ και στο Παράδειγμα 3.6(4) είδαμε ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο.

(3) Εύκολα επαληθεύεται ότι το σύνολο $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ είναι περιοχή. Δεν είναι σώμα, αφού για παράδειγμα το $2 \notin U(\mathbb{Z}[\sqrt{2}])$. Πράγματι, αρχικά παρατηρούμε ότι αν $a, b \in \mathbb{Z}$, τότε $a + b\sqrt{2} = 0 \Leftrightarrow a = b = 0$ (γιατί;) Τώρα αν $2 \in U(\mathbb{Z}[\sqrt{2}])$, τότε

$$2(x + y\sqrt{2}) = 1,$$

για κάποια $x, y \in \mathbb{Z}$. Συνεπώς $2x = 1$, αδύνατο αφού $x \in \mathbb{Z}$.

(4) Η περιοχή $\mathbb{Z}[i]$ των ακεραίων του Gauss δεν είναι σώμα καθώς διαθέτει μη μηδενικά μη αντιστρέψιμα στοιχεία, βλ. Παράδειγμα 3.6(3).

(5) Στο Παράδειγμα 3.8(4) είδαμε ότι ο δακτύλιος $F(\mathbb{R}, \mathbb{R})$ δεν είναι περιοχή και επομένως από την Πρόταση 3.11 έπεται ότι δεν είναι σώμα.

Πρόταση 3.13. *Έστω $n \in \mathbb{N}$. Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν ο n είναι πρώτος.*

Απόδειξη. Έστω $\mathbb{Z}_n$ σώμα. Τότε $n \neq 0$ ($\mathbb{Z}_0 = \mathbb{Z}$ δεν είναι σώμα) και $n \neq 1$ ($\mathbb{Z}_1 = \{[0]\}$ δεν είναι σώμα). Από την Πρόταση 3.11, $\mathbb{Z}_n$ είναι περιοχή, άρα ο n είναι πρώτος ή $n = 0$. Επομένως ο n είναι πρώτος.

Αντίστροφα, έστω ότι ο n είναι πρώτος. Τότε $n > 1$ και άρα $[1] \neq [0]$. Ο $\mathbb{Z}_n$ είναι μεταθετικός για κάθε n και επειδή ο n είναι πρώτος έχουμε $\mu\kappa\delta(a, n) = 1$, για κάθε $a = 1, 2, \ldots, n-1$. Επομένως τα $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{[0]\}$, δηλαδή $\mathbb{Z}_n$ είναι σώμα. □

Είδαμε πριν ότι κάθε σώμα είναι περιοχή και ότι το αντίστροφο δεν αληθεύει. Θα δούμε τώρα ότι κάθε *πεπερασμένη* περιοχή είναι σώμα.

Πρόταση 3.14. *Κάθε πεπερασμένη περιοχή είναι σώμα.*

Απόδειξη. Έστω $R = \{r_1, ..., r_n\}$ πεπερασμένη περιοχή και $r \in R, r \neq 0_R$. Επειδή ο R δεν έχει μη μηδενικούς μηδενοδιαιρέτες, τα ακόλουθα στοιχεία του R,

$$rr_1, rr_2, ..., rr_n$$

είναι διακεκριμένα. Πράγματι, αν $rr_i = rr_j$, τότε $r(r_i - r_j) = 0_R$ από το οποίο έπεται ότι $r_i - r_j = 0_R$ γιατί αλλιώς το r θα ήταν μη μηδενικός μηδενοδιαιρέτης

Άρα το πλήθος των παραπάνω στοιχείων είναι n. Επειδή το σύνολο R έχει n στοιχεία και το n είναι πεπερασμένο, παίρνουμε ότι $R = \{rr_1, rr_2, ..., rr_n\}$. Συνεπώς υπάρχει j με $1_R = rr_j$ που σημαίνει ότι το r είναι αντιστρέψιμο καθώς ο R είναι μεταθετικός. □

3.3. Διωνυμικό ανάπτυγμα

Στη συνέχεια θα αναφερθούμε σε ακέραια πολλαπλάσια στοιχείων δακτυλίου και δυνάμεις με θετικό ακέραιο εκθέτη. Έστω R δακτύλιος και $r \in R$.

- Έστω $m \in \mathbb{N}$. Ορίζουμε επαγωγικά το mr θέτοντας $0r = 0_R$ και $mr = r + (m-1)r$ αν $m > 0$. Επίσης, αν $m \in \mathbb{Z}, m < 0$, ορίζουμε $mr = (-m)(-r)$.
- Έστω $m \in \mathbb{Z}_{>0}$. Ορίζουμε επαγωγικά το r^m θέτοντας $r^1 = r$ και $r^m = rr^{m-1}$ αν $m > 1$.

Αφήνουμε ως άσκηση στη μαθηματική επαγωγή την απόδειξη των εξής ιδιοτήτων που θα χρησιμοποιούμε στα επόμενα χωρίς ιδιαίτερη μνεία.

Πρόταση 3.15. *Έστω R δακτύλιος, $r, s \in R$ και $m, n \in \mathbb{Z}$. Ισχύουν οι ακόλουθες ιδιότητες.*

(1) $(m+n)r = mr + nr$.
(2) $m(nr) = (mn)r$.
(3) $(-m)r = m(-r) = -(mr)$.
(4) $m(r+s) = mr + ms$.
(5) $(mr)(ns) = mn(rs)$.
(6) $r^{m+n} = r^m r^n$, *όπου* $m, n > 0$.
(7) $(r^m)^n = r^{mn}$, *όπου* $m, n > 0$.

Για παράδειγμα, στο $\mathbb{Z}_6$ έχουμε $-3[5] + 9[5] = (-3+9)[5] = 6[5] = [30] = [0]$.

Παράδειγμα Ένας δακτύλιος R είναι μεταθετικός αν και μόνο αν

$$(a+b)^2 = a^2 + 2ab + b^2,$$

για κάθε $a, b \in \mathbb{R}$.

Απόδειξη. Παρατηρούμε ότι για κάθε $a, b \in \mathbb{R}$,

$$(a+b)^2 = (a+b)(a+b) = a(a+b) + b(a+b) = a^2 + ab + ba + b^2.$$

Έχουμε

$$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2 \Leftrightarrow a^2 + ab + ab + b^2 = a^2 + 2ab + b^2 \Leftrightarrow \\ ab + ab &= 2ab \Leftrightarrow ba = ba. \end{aligned}$$

Επομένως ο R είναι μεταθετικός αν και μόνο αν $(a+b)^2 = a^2 + 2ab + b^2$, για κάθε $a, b \in \mathbb{R}$. □

Υπενθυμίζουμε στη συνέχεια τους διωνυμικούς συντελεστές. Θέτουμε $0! = 1$ και $i! = 1 \cdot 2 \cdot 3 \cdot ... \cdot i$ αν i θετικός ακέραιος. Αν $i \leq n$ είναι φυσικοί αριθμοί, θέτουμε

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

Στην περίπτωση που έχουμε $i > n$ συμφωνούμε ότι $\binom{n}{i} = 0$. Αφήνουμε ως άσκηση την απόδειξη της ταυτότητας του Pascal

$$\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1},$$

όπου $1 \leq i \leq n+1$. Με βάση τη σχέση αυτή έπεται με επαγωγή στο n ότι οι διωνυμικοί συντελεστές $\binom{n}{i}$ είναι ακέραιοι.

Πρόταση 3.16 (Διωνυμικό ανάπτυγμα). *Έστω R δακτύλιος, $a, b \in R$ και $n \in \mathbb{N}$, $n \geq 1$. Αν $ab = ba$, τότε*

$$(a+b)^n = a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i + b^n. \tag{3.1}$$

Απόδειξη. Επαγωγή στο n. Για $n = 1$ το ζητούμενο είναι σαφές. Έστω ότι ισχύει η (3.1). Θα δείξουμε ότι ισχύει για $n+1$ στη θέση του n. Πράγματι,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= a(a+b)^n + b(a+b)^n \\
&= a(a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i + b^n) + b(a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^{n-i} b^i + b^n) \\
&= a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=0}^{n-1} \binom{n}{i} a^{n-i} b^{i+1} + b^{n+1},
\end{aligned}$$

όπου στην τελευταία ισότητα χρησιμοποιήσαμε ότι $ba^k = a^k b$, k θετικός ακέραιος. Παρατηρούμε ότι το δεξί μέλος ισούται με

$$\begin{aligned}
&a^{n+1} + \sum_{i=1}^{n} \binom{n}{i} a^{n+1-i} b^i + \sum_{i=1}^{n} \binom{n}{i-1} a^{n+1-i} b^i + b^{n+1} \\
&= a^{n+1} + \sum_{i=1}^{n} (\binom{n}{i} + \binom{n}{i-1}) a^{n+1-i} b^i + b^{n+1} \\
&= a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} a^{n+1-i} b^i + b^{n+1}.
\end{aligned}$$

όπου στη δεύτερη ισότητα χρησιμοποιήσαμε την ταυτότητα του Pascal. Επομένως η (3.1) ισχύει για $n+1$ στην θέση του n. □

Παράδειγμα 3.17. Έστω p πρώτος.

(1) $p | \binom{p}{i}$ για κάθε $i = 1, ..., p-1$.

(2) (Όνειρο πρωτοετή). Έστω R μεταθετικός δακτύλιος τέτοιος ώστε $pr = 0_R$, για κάθε $r \in R$. Τότε για κάθε $a, b \in R$

$$(a+b)^p = a^p + b^p.$$

Απόδειξη. (1) Έχουμε $p! = \binom{p}{i} i!(p-i)!$. Το p διαιρεί το αριστερό μέλος και για κάθε $i = 1, .., p-1$ δεν διαιρεί το $i!(p-i)!$ λόγω του λήμματος του Ευκλείδη. Άρα πάλι από το λήμμα του Ευκλείδη το p διαιρεί το $\binom{p}{i}$.

(2) Επειδή $ab = ba$ έχουμε το διωνυμικό ανάπτυγμα

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p.$$

Από το (1) και την υπόθεση έχουμε $\binom{p}{i} a^{p-i} s b^i = 0_R$ για κάθε $i = 1, ..., p-1$. □

Παρατηρήσεις. (1) Ένα παράδειγμα δακτυλίου που ικανοποιεί τις υποθέσεις του Παραδείγματος 3.17(2) είναι ο $\mathbb{Z}_p$, p πρώτος.
(2) Χωρίς την υπόθεση $ab = ba$, η Πρόταση 3.16 γενικά δεν αληθεύει. Για παράδειγμα, έστω

$R = M_2(\mathbb{R}), a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Τότε

$$(a+b)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ a^2 + 2ab + b^2 = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}.$$

3.4. Υποδακτύλιοι

Ορισμός 3.18. *Έστω $\oplus : A \times A \to A$ μια πράξη στο A και έστω $B \subseteq A$. Θα λέμε ότι το B είναι* **κλειστό** *ως προς την πράξη $\oplus$, αν για κάθε $b_1, b_2 \in B$ έχουμε $b_1 \oplus b_2 \in B$.*

Για παράδειγμα, ως προς την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$, το σύνολο $\{2m : m \in \mathbb{Z}\}$ των άρτιων ακεραίων είναι κλειστό. Το σύνολο $\{2m+1 : m \in \mathbb{Z}\}$ των περιττών ακεραίων δεν είναι κλειστό ως προς την πρόσθεση, αλλά είναι κλειστό ως προς τον πολλαπλασιασμό.

Αν $\oplus : A \times A \to A$ είναι πράξη του A και $B \subseteq A$ κλειστό ως προς την $\oplus$ και $B \neq \emptyset$, τότε ορίζεται η πράξη $\boxplus : B \times B \to B : b_1 \boxplus b_2 = b_1 \oplus b_2$. Στην περίπτωση αυτή θα λέμε ότι η $\boxplus$ είναι **ο περιορισμός** της $\oplus$ στο B και συνήθως θα χρησιμοποιούμε τον ίδιο συμβολισμό.

Ορισμός 3.19. *Έστω R ένας δακτύλιος και $S \subseteq R$ ένα κλειστό σύνολο ως προς τις πράξεις του R. Αν ο S είναι δακτύλιος ως προς τους περιορισμούς των πράξεων του R, θα λέμε ότι ο S είναι ένας* **υποδακτύλιος** *του R.*

Παραδείγματα 3.20.

(1) Το $\mathbb{Z}$ είναι υποδακτύλιος των $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(2) Το $2\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{Z}$.

(3) Το $\mathbb{N}$ είναι κλειστό στο $\mathbb{Z}$ ως προς την πρόσθεση και τον πολλαπλασιασμό, αλλά δεν είναι υποδακτύλιος καθώς δεν έχει αντίθετα.

Πρόταση 3.21. *Έστω R δακτύλιος και $S \subseteq R$, $S \neq \emptyset$. Ο S είναι υποδακτύλιος του R αν και μόνο αν ισχύουν τα ακόλουθα.*

(1) *$a + b \in S$ για κάθε $a, b \in S$.*
(2) *$ab \in S$ για κάθε $a, b \in S$.*
(3) *$-a \in S$ για κάθε $a \in S$ (δηλαδή το αντίθετο του $a \in S$ στο δακτύλιο R ανήκει στο S).*

Απόδειξη. Έστω ότι ο S είναι υποδακτύλιος του R. Τότε οι (1) και (2) ισχύουν από τον ορισμό. Παρατηρούμε ότι $0_S = 0_R$. Πράγματι, επειδή $S \neq \emptyset$, υπάρχει αν $a \in S$, οπότε $a + 0_S = a$ και $a + 0_R = a$. Επομένως $a + 0_R = a + 0_S \Rightarrow 0_R = 0_S$, από το νόμο διαγραφής στο R. Τώρα για κάθε $a \in S$ έχουμε, $a + (-a) = 0_R = 0_S$. Άρα $-a \in S$.

Αντίστροφα έστω ότι ισχύουν οι (1)-(3). Τότε ο S είναι κλειστός ως προς τις πράξεις του R και συνεπώς οι περιορισμοί των πράξεων του R στο υποσύνολο S δίνουν πράξεις στο S. Ας δούμε την ύπαρξη του 0_S. Αφού $S \neq \emptyset$, υπάρχει $a \in S$, οπότε από την (3), $-a \in S$. Επομένως από την (1), $a + (-a) \in S$. Άρα $0_R \in S$. Θέτουμε $0_S = 0_R$. Τότε για κάθε $b \in R$ έχουμε $b + 0_S = 0_S a = b$.

Η ύπαρξη του $-a$ στο S έπεται άμεσα από την (3).

Οι υπόλοιπες ιδιότητες στον ορισμό του δακτυλίου ισχύουν στο S, αφού ισχύουν στο R και $S \subseteq R$. □

Πρόταση 3.22. *Έστω R δακτύλιος και $S \subseteq R$, $S \neq \emptyset$. Ο S είναι υποδακτύλιος του R αν και μόνο αν για κάθε $a, b \in S$ ισχύουν ότι $a - b \in S$ και $ab \in S$.*

Απόδειξη. Το ευθύ είναι σαφές από την προηγούμενη Πρόταση. Για το αντίστροφο, έστω $a \in S$. Τότε $a - a \in S$, άρα $0_R \in S$. Τότε $0_S - a \in S$, άρα $-a \in S$. Επίσης αν $a, b \in S$, τότε $a-(-b) \in S \Rightarrow a+b \in S$. Από την προηγούμενη Πρόταση, ο S είναι υποδακτύλιος του R. □

Παραδείγματα 3.23.

(1) Το σύνολο $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (ακέραιοι του Gauss) είναι υποδακτύλιος του $\mathbb{C}$.
Πράγματι, είναι μη κενό σύνολο και αν $a, b, c, d \in \mathbb{Z}$, τότε έχουμε

$$(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i], \text{ και}$$

$$(a + bi)(c + di) = (ac - bd) + (ab + bc)i \in \mathbb{Z}[i].$$

(2) Το σύνολο $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ είναι υποδακτύλιος του $\mathbb{R}$.
Πράγματι, είναι μη κενό σύνολο και αν $a, b, c, d \in \mathbb{Z}$, τότε έχουμε,

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \text{ και}$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ab + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

(3) Το σύνολο $S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R} \right\}$ είναι υποδακτύλιος του $M_2(\mathbb{R})$.
Πράγματι, $S \neq \emptyset$. Παρατηρούμε ότι αν $a, b \in \mathbb{R}$, τότε

$$\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a-b \end{pmatrix} \in S, \text{ και}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & ab \end{pmatrix} \in S.$$

Επομένως ο S είναι υποδακτύλιος του $M_2(\mathbb{R})$. Ο RS είναι μεταθετικός με μοναδιαίο στοιχείο το $1_R = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Παρατηρούμε ότι $1_R \notin U(M_2(\mathbb{R}))$ αλλά $1_S \in U(S)$.

(4) Εύκολα επαληθεύεται ότι το υποσύνολο $M_n(\mathbb{Z})$ του $M_n(\mathbb{R})$ είναι υποδακτύλιο του $M_n(\mathbb{R})$. Λίγο πιο γενικά, αν S είναι υποδακτύλιο του R, τότε ο $M_n(S)$ είναι υποδακτύλιος του $M_n(R)$. Για παράδειγμα, έχουμε τον υποδακτύλιος $M_n(2\mathbb{Z})$ που αποτελείται από τους πίνακες με στοιχεία άρτιους ακέραιους.

(5) **Άνω τριγωνικοί πίνακες, διαγώνιοι πίνακες** Έστω R δακτύλιος και
- $T_n(R)$ το υποσύνολο του $M_n(R)$ που αποτελείται από τους άνω τριγωνικούς πίνακες,
- $D_n(R)$ το υποσύνολο του $M_n(R)$ που αποτελείται από τους διαγώνιους πίνακες.

Εύκολα επαληθεύεται ότι τα $T_n(R)$ και $D_n(R)$ είναι υποδακτύλιοι του $M_n(R)$.

(6) Στο Παράδειγμα 3.3(8) είδαμε το δακτύλιο $F(\mathbb{R}, \mathbb{R})$ των συναρτήσεων $\mathbb{R} \to \mathbb{R}$. Το υποσύνολο αυτού που αποτελείται από τις συναρτήσεις f που ικανοποιούν $f(0) = 0$ είναι υποδακτύλιος του $F(\mathbb{R}, \mathbb{R})$.

Παρατηρήσεις. Έστω S υποδακτύλιος του δακτυλίου R.

(1) Είναι $0_S = 0_R$ (το είδαμε στην απόδειξη της Πρότασης 3.21).

(2) Αν οι S και R έχουν μοναδιαία στοιχεία, δεν είναι απαραίτητο ότι $1_R = 1_S$, βλ. Παράδειγμα 3.23(3).

(3) Αν το $a \in S$ είναι αντιστρέψιμο στο S, δεν είναι απαραίτητο ότι το a είναι αντιστρέψιμο στο R, βλ. Παράδειγμα 3.23(3).

(4) Είναι δυνατόν μόνο ένας από τους R, S να έχει μοναδιαίο στοιχείο. Για παράδειγμα, $S = 2\mathbb{Z}$ και $R = \mathbb{Z}$.

(5) Έστω ότι οι R και S έχουν μοναδιαία στοιχεία και ότι $1_R = 1_S$. Αν το s είναι αντιστρέψιμο στον S, τότε το $s \in R$ είναι αντιστρέψιμο και τα δύο αντίστροφα στοιχεία ταυτίζονται (άσκηση).

3.5. Ευθύ γινόμενο δακτυλίων

Έστω R, S δακτύλιοι. Στο καρτεσιανό γινόμενο $R \times S$ έχουμε τις πράξεις

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Για παράδειγμα, στο $\mathbb{Z} \times \mathbb{Z}_6$ έχουμε

$$(5, [4]) + (-3, [5]) = (5 - 3, [4] + [5]) = (2, [9]) = (2, [3]),$$
$$(5, [4])(-3, [5]) = (5(-3), [4][5]) = (-15, [20]) = (-15, [2]).$$

Είναι υπόθεση ρουτίνας να επαληθευθεί ότι με τις πράξεις αυτές το $R \times S$ καθίσταται δακτύλιος. Το μηδενικό στοιχείο του $R \times S$ είναι το $0_{R\times S} = (0_R, 0_S)$ και το αντίθετο του (r, s) είναι το $-(r, s) = (-r, -s)$. Ο δακτύλιος $R \times S$ λέγεται το **ευθύ γινόμενο** των R, S.

Χρησιμοποιώντας την Πρόταση 3.22 εύκολα προκύπτει ότι τα σύνολα

$$R \times 0_S = \{(r, 0_S) : r \in R\},$$
$$0_R \times S = \{(0_R, s) : s \in S\},$$

είναι υποδακτύλιοι του $R \times S$.

Ασκήσεις Κεφαλαίου 3

Ομάδα1: 1-5, 13, 14, 16, 21, 22.
Ομάδα2: 6-12, 15, 17-20, 23-28, 30-32.
Ομάδα3: 29, 33-35.

1. Αποδείξτε πλήρως τους ισχυρισμούς στα Παραδείγματα 3.23 (4)-(6).
2. Δείξτε ότι αν R είναι δακτύλιος με μοναδιαίο στοιχείο, τότε το σύνολο $U(R)$ είναι κλειστό ως προς τον πολλαπλασιασμό του R. Αληθεύει ότι το $U(\mathbb{Z}_{12})$ είναι κλειστό ως προς την πρόσθεση του $\mathbb{Z}_{12}$;
3. Εξετάστε αν το $R = \{[0], [4], [8]\}$ είναι υποδακτύλιος του $\mathbb{Z}_{12}$. Είναι το R σώμα;
4. Δείξτε ότι το σύνολο $R = \mathbb{Z}[\sqrt{-2}] = \{a + ib\sqrt{2} : a, b \in \mathbb{Z}\}$ είναι υποδακτύλιος του $\mathbb{C}$ και βρείτε τα αντιστρέψιμα στοιχεία του.
5. $\star$ Έστω ότι ο R είναι υποδακτύλιος του S και ότι έχουν μοναδιαία στοιχεία με $1_R = 1_S$. Αν το r είναι αντιστρέψιμο στο R, τότε το r είναι αντιστρέψιμο στο S και τα δύο αντίστροφα στοιχεία ταυτίζονται.
6. Αν ο δακτύλιος R έχει μοναδιαίο στοιχείο και $a, b, a + b \in U(R)$, τότε $a^{-1} + b^{-1} \in U(R)$. Στη συνέχεια δώστε ένα παράδειγμα που δείχνει ότι η συνεπαγωγή "$a, b \in U(R)$, τότε $a^{-1} + b^{-1} \in U(R)$" γενικά δεν αληθεύει.
7. Έστω R περιοχή τέτοια ώστε υπάρχει μη μηδενικό $a \in R$ με $6a = 0_R$. Δείξτε ότι ισχύει ακριβώς ένα από τα ακόλουθα.
   - $2r = 0_R$ για κάθε $r \in R$.
   - $3r = 0_R$ για κάθε $r \in R$.
8. Έστω $R = \left\{ \frac{m}{2^a 3^b} \in \mathbb{Q} : m \in \mathbb{Z}, a, b \in \mathbb{N} \right\}$.
   i) Δείξτε ότι ο R είναι υποδακτύλιος του $\mathbb{Q}$.
   ii) Δείξτε ότι ο R περιέχεται σε κάθε υποδακτύλιο του $\mathbb{Q}$ που περιέχει τα $\frac{1}{2}$ και $\frac{1}{3}$.
   iii) Αληθεύει ότι ο R είναι σώμα;
9. Δείξτε ότι το $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Z}\}$ δεν είναι υποδακτύλιος του $\mathbb{R}$.
10. Δείξτε ότι ο δακτύλιος το $R = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$ έχει άπειρο πλήθος αντιστρέψιμων στοιχείων.
11. Έστω R μη μηδενικός μεταθετικός δακτύλιος με μονάδα και $a \in R$. Θεωρούμε την απεικόνιση $f_a : R \to R, r \mapsto ar$. Συμπληρώστε και αποδείξτε τις εξής προτάσεις.
    i) Η απεικόνιση f_a είναι 1-1 για κάθε $a \neq 0$ αν και μόνο αν ο δακτύλιος R είναι ....
    ii) Η απεικόνιση f_a είναι επί για κάθε $a \neq 0$ αν και μόνο αν ο δακτύλιος R είναι ....
12. Ένα στοιχείο a δακτυλίου R λέγεται **δεξιός μηδενοδιαιρέτης** αν υπάρχει μη μηδενικό $x \in R$ με $xa = 0_R$.
    i) Δείξτε ότι αν το $b \in R$ δεν είναι δεξιός μηδενοδιαιρέτης, τότε το ίδιο συμβαίνει με το b^k για κάθε θετικό ακέραιο k.
    ii) Έστω R δακτύλιος και $a, b \in R$ τέτοια ώστε υπάρχουν σχετικά πρώτοι θετικοί ακέραιοι m, n με $a^m = b^m$ και $a^n = b^n$.Δείξτε ότι αν ένα από τα a, b δεν είναι δεξιός μηδενοδιαιρέτης, τότε $a = b$.
13. Έστω R, S δακτύλιοι.
    i) Δείξτε ότι αν οι R, S είναι μεταθετικοί, τότε ο $R \times S$ είναι μεταθετικός.
    ii) $\star$ Δείξτε ότι αν οι R, S έχουν μοναδιαία στοιχεία, τότε το $(1_R, 1_S)$ είναι μοναδιαίο στοιχείο του $R \times S$ και επιπλέον $U(R \times S) = U(R) \times U(S)$.
    iii) Αληθεύει ότι αν οι R, S είναι σώματα, τότε ο $R \times S$ είναι σώμα;
    iv) Αληθεύει το αντίστροφο του (i) ;
    v) Αληθεύει το αντίστροφο του (ii) ;

14. Δείξτε ότι το σύνολο $T_2(\mathbb{Z}) = \left\{ A \in M_2(\mathbb{Z}) : A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right\}$. είναι υποδακτύλιος του $M_2(\mathbb{Z})$ και βρείτε τα αντιστρέψιμα στοιχεία του.

15. Δίνεται το σύνολο $T_2(\mathbb{Z}_n) = \left\{ A \in M_2(\mathbb{Z}_n) : A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \right\}$.
    i) Δείξτε ότι το $T_2(\mathbb{Z}_n)$ είναι υποδακτύλιος του $M_2(\mathbb{Z}_n)$.
    ii) Αληθεύει ότι ο $T_2(\mathbb{Z}_n)$ είναι μεταθετικός;
    iii) Δείξτε ότι $|U(T_2(\mathbb{Z}_n)| = n\varphi(n)^2$,όπου φ η συνάρτηση του Euler.

16. Αληθεύει ότι αν ο R είναι υποδακτύλιος του S, τότε ο $M_n(R)$ είναι υποδακτύλιος του $M_n(S)$;

17. Έστω p πρώτος και R μεταθετικός δακτύλιος τέτοιος ώστε $pr = 0_R$ για κάθε $r \in R$. Δείξτε ότι $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ για κάθε $a, b \in R$ και κάθε θετικό ακέραιο n.

18. Έστω R δακτύλιος τέτοιος ώστε $r^2 = r$ για κάθε $r \in R$. Δείξτε ότι για κάθε $r \in R$ ισχύει $2r = 0_R$ και ότι ο R είναι μεταθετικός.

19. Για ποια n ισχύει ότι $(a+b)^4 = a^4 + b^4$ για κάθε $a, b \in \mathbb{Z}_n$;

20. $\star$ Έστω R ένας δακτύλιος και έστω $r \in R$. Το r λέγεται **μηδενοδύναμο**, αν $r^m = 0$ για κάποιο $m \in \mathbb{Z}_{>0}$. Ας συμβολίσουμε το σύνολο των μηδενοδύναμων στοιχείων του R με $nil(R)$.
    i) Βρείτε τα μηδενοδύναμα στοιχεία του $\mathbb{Z}_{30}$ και του $\mathbb{Z}_{60}$.
    ii) Δείξτε ότι ο $nil(\mathbb{Z}_n) = \{[0]\}$, $n > 0$, αν και μόνο αν το n δεν διαιρείται με το τετράγωνο πρώτου.
    iii) Αν ο R είναι μεταθετικός δακτύλιος, τότε το $nil(R)$ είναι υποδακτύλιος του R.

21. Δείξτε ότι $nil(R \times S) = nil(R) \times nil(S)$, όπου R, S δακτύλιοι. (Βλ. προηγούμενη άσκηση για το συμβολισμό.)

22. Ας συμβολίσουμε με $div(R)$ το σύνολο των δεξιών μηδενοδιαιρετών του δακτυλίου R. Δείξτε ότι $div(R \times S) = div(R) \times S \cup R \times div(S)$, όπου R, S δακτύλιοι.

23. Δείξτε ότι η τομή μιας οικογένειας υποδακτυλίων του δακτυλίου S είναι υποδακτύλιος του S. Στη συνέχεια βρείτε την τομή όλων των υποδακτυλίων του $\mathbb{C}$ που περιέχουν
    i) το 1
    ii) το 1 και το i.

24. Βρείτε την τομή όλων των υποσωμάτων του $\mathbb{C}$.

25. Αν ο δακτύλιος R έχει μοναδιαίο στοιχείο και το $r \in R$ είναι μηδενοδύναμο, τότε το $1_R - r$ είναι αντιστρέψιμο.

26. Έστω R υποδακτύλιος του $\mathbb{C}$ με $\mathbb{Q} \subseteq R$. Εύκολα επαληθεύεται ότι το R είναι $\mathbb{Q}$-διανυσματικός χώρος με πρόσθεση $R \times R \to R$ την πρόσθεση του δακτυλίου R και εξωτερικό πολλαπλασιασμό $\mathbb{Q} \times R \to R$ τον περιορισμό του πολλαπλασιασμού του δακτυλίου R. Δείξτε ότι αν $dim_{\mathbb{Q}} < \infty$, τότε ο δακτύλιος R είναι σώμα.

27. Βρείτε όλους του υποδακτύλιους του $M_2(\mathbb{R})$ που περιέχουν τους συμμετρικούς πίνακες.

28. Δώστε παράδειγμα
    i) δακτυλίου R και $a, b \in R$ με $ab = 0$ και $ba \neq 0$, και
    ii) μη μηδενικού δακτυλίου S με $a^2 = 0, \forall a \in S$.

29. 'Εστω R πεπερασμένος δακτύλιος. Δείξτε ότι αν το $a \in R$ δεν είναι δεξιός μηδενοδιαιρέτης, τότε υπάρχει $e \in R$ με $ea = ae = a$.

30. i) 'Εστω R πεπερασμένος μεταθετικός δακτύλιος με μονάδα. Δείξτε ότι κάθε στοιχείο του R είναι αντιστρέψιμο ή μηδενοδιαιρέτης.
    ii) Στη συνέχεια, αποδείξτε την εξής γενίκευση. Αν R είναι πεπερασμένος δακτύλιος με μονάδα, τότε κάθε στοιχείο του R είναι αντιστρέψιμο ή δεξιός μηδενοδιαιρέτης (βλ. άσκηση 3.12).
    iii) Βρείτε παράδειγμα περιοχής για την οποία το συμπέρασμα του i) δεν αληθεύει

iv) Βρείτε παράδειγμα άπειρου δακτυλίου με μονάδα για τον οποίο το συμπέρασμα του ii) αληθεύει

31. Έστω R δακτύλιος τέτοιος ώστε υπάρχει θετικός άρτιος ακέραιος n με $a^n = a$ για κάθε $a \in R$. Δείξτε ότι $-a = a$ για κάθε $a \in R$.

32. Έστω R δακτύλιος τέτοιος ώστε $a^3 = a$ για κάθε $a \in R$. Δείξτε ότι αν $ab = 0$ για κάποια $a, b \in R$, τότε $ba = 0$.

33. ≀ Έστω R δακτύλιος τέτοιος ώστε $a^3 = a$ για κάθε $a \in R$. Δείξτε ότι ο R είναι μεταθετικός.

34. Έστω R δακτύλιος με μονάδα τέτοιος ώστε $(ab)^2 = a^2b^2$ για κάθε $a, b \in R$. Δείξτε ότι ο R είναι μεταθετικός.

35. ≀ Έστω R δακτύλιος τέτοιος ώστε $(ab)^2 = a^2b^2$ για κάθε $a, b \in R$. Δείξτε ότι αν το μοναδικό μηδενοδύναμο στοιχείο του R είναι το 0, τότε ο R είναι μεταθετικός.

Υποδείξεις Κεφαλαίου 3

1.

2. *Λύση.* Αν $a, a', b, b' \in R$ με $aa' = a'a = 1_R$, $bb' = b'b = 1_R$, τότε
$$(ab)(b'a') = a(bb')a' = a1_Ra' = aa' = 1_R, \text{ και}$$
$$(b'a')(ab) = b'(a'a)a = b'1_Rb = b'ab = 1_R.$$
Άρα $ab \in U(R)$.

Σημείωση: Δείξαμε ότι αν $a, b \in U(R)$, τότε $ab \in U(R)$ και $(ab)^{-1} = b^{-1}a^{-1}$.

Δεν αληθεύει ότι το $U(\mathbb{Z}_{12})$ είναι κλειστό ως προς την πρόσθεση του $\mathbb{Z}_{12}$. Για παράδειγμα, τα στοιχεία $[1], [11]$ είναι αντιστρέψιμα ($\mu\kappa\delta(11, 12) = 1$) και $[1] + [11] = [12] = [0]$ που δεν είναι αντιστρέψιμο.

3. *Λύση.* Εύκολα επαληθεύουμε με πράξεις ότι $[a]-[b] \in R$ και $[a][b] \in R$ για κάθε $[a], [b] \in R$. Συνεπώς ο R είναι υποδακτύλιος του $\mathbb{Z}_{12}$. Επίσης έχει μοναδιαίο στοιχείο το $1_R = [4] \neq [0]$ και ισχύει $[8]^{-1} = [8]$. Άρα ο R είναι σώμα.

4. *Λύση.* Το σύνολο $\mathbb{Z}[\sqrt{-2}]$ είναι μη κενό και αν $a, b, c, d \in \mathbb{Z}$, τότε έχουμε,
$$(a + ib\sqrt{2}) - (c + id\sqrt{2}) = (a - c) + i(b - d)\sqrt{2} \in \mathbb{Z}[\sqrt{-2}], \text{ και}$$
$$(a + ib\sqrt{2})(c + id\sqrt{2}) = (ac - 2bd) + i(ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{-2}].$$
Άρα $\mathbb{Z}[\sqrt{-2}]$ είναι υποδακτύλιος του $\mathbb{C}$.

Χρησιμοποιώντας τη μέθοδο που είδαμε στο Παράδειγμα 3.6(3), θα δείξουμε ότι $U(R) = \{1, -1\}$,

Πράγματι, είναι σαφές ότι $\{1, -1\} \subseteq U(R)$.

Για να δείξουμε την άλλη σχέση εγκλεισμού, έστω $a + ib\sqrt{2} \in U(R)$, όπου $a, b \in \mathbb{Z}$. Τότε υπάρχουν $c, d \in \mathbb{Z}$ ώστε $(a + ib\sqrt{2})(c + id\sqrt{2}) = 1$. Παίρνοντας μέτρα μιγαδικών και χρησιμοποιώντας ότι $|z_1z_2| = |z_1||z_2|$, όπου $z_1, z_2 \in \mathbb{C}$, έχουμε,
$$|(a + ib\sqrt{2})||(c + id\sqrt{2}| = 1 \Rightarrow |a + ib\sqrt{2}|^2|(c + id\sqrt{2}|^2 = 1 \Rightarrow$$
$$(a^2 + 2b^2)(c^2 + 2d^2) = 1.$$
Από την τελευταία ισότητα, που είναι ισότητα ακεραίων, έπεται ότι $a^2 + 2b^2 = 1$. Αφού $a^2 + 2b^2 = 1$ και $a, b \in \mathbb{Z}$ έχουμε $a = \pm 1$ και $b = 0$. Άρα $a + bi = \pm 1$. Δείξαμε ότι $U(R) \subseteq \{1, -1\}$ και συνεπώς έχουμε ισότητα $U(R) = \{1, -1\}$

5. *Λύση.* Έστω $r \in U(R)$ με αντίστροφο το $r' \in R$. Τότε $rr' = r'r = 1_R$. Συνεπώς $rr' = r'r = 1_S$. Αυτή η σχέση σε συνδυασμό με $r' \in R \subseteq S$ λέει ότι $r \in U(S)$ και το αντίστροφο του r στο S είναι το r'.

6. *Λύση.* Έστω $c = a(a + b)^{-1}b$. Τότε
$$\begin{aligned}(a^{-1} + b^{-1})c &= (a^{-1} + b^{-1})a(a + b)^{-1}b \\ &= (1_R + b^{-1}a)(a + b)^{-1}b \\ &= b^{-1}(b + a)(a + b)^{-1}b \\ &= b^{-1}(a + b)(a + b)^{-1}b \\ &= b^{-1}1_Rb \\ &= 1_R.\end{aligned}$$
Ομοίως αποδεικνύεται ότι $c(a^{-1} + b^{-1}) = 1_R$. Άρα $a^{-1} + b^{-1} \in U(R)$.

Ένα παράδειγμα που δείχνει ότι η συνεπαγωγή της εκφώνησης είναι λάθος είναι $R = \mathbb{Z}, a = 1, b = -1$.

7. *Λύση.* Από την υπόθεση έχουμε $(61_R)a = 6(1_Ra) = 6a = 0_R$. Επειδή ο R είναι περιοχή και το $a \in R$ είναι μη μηδενικό παίρνουμε $61_R = 0_R$. Άρα $(21_R)(31_R) = 0_R$ και επειδή ο

R είναι περιοχή έπεται ότι $21_R = 0_R$ ή $31_R = 0_R$. Στην πρώτη περίπτωση έχουμε για κάθε $r \in R$ ότι $2r = (21_R)r = 0_R r = 0_R$. Όμοια στη δεύτερη περίπτωση έχουμε $3r = 0_R$ για κάθε $r \in R$.

Τέλος αν για κάθε $r \in R$ ισχύει $2r = 0_R$ και $3r = 0_R$, τότε $r = 3r - 2r = 0_R - 0_R = 0_R$. Δηλαδή $R = \{0_R\}$, αδύνατο επειδή ο R είναι περιοχή.

8. *Λύση.* i) Παρατηρούμε ότι το $0 \in R$, άρα $R \neq \emptyset$. Έστω $m, n \in \mathbb{Z}, a, b, c, d \in \mathbb{N}$. Τότε

$$\frac{m}{2^a 3^b} - \frac{n}{2^c 3^b} = \frac{m2^c 3^d - n2^a 3^b}{2^{a+c} 3^{b+d}} \in R, \text{ και}$$

$$\frac{m}{2^a 3^b} \frac{n}{2^c 3^b} = \frac{mn}{2^{a+c} 3^{b+d}} \in R.$$

Άρα ο R είναι υποδακτύλιος του $\mathbb{Q}$.

ii) Έστω S υποδακτύλιος του $\mathbb{Q}$ ώστε $\frac{1}{2}, \frac{1}{3} \in S$. Τότε αφού ο S είναι υποδακτύλιος και επειδή $1 = \frac{1}{2} + \frac{1}{2}$, έπεται ότι το $1 \in S$, άρα και $-1 \in S$. Επομένως κάθε στοιχείο της μορφής $\pm 1 \pm 1 \cdots \pm 1$ ανήκει στο S. Άρα $\mathbb{Z} \subseteq S$. Επίσης επειδή ο S είναι κλειστός ως προς τον πολλαπλασιασμό έχουμε

$$\frac{1}{2^a} = \left(\frac{1}{2}\right)^a \in S \quad \text{και} \quad \frac{1}{3^b} = \left(\frac{1}{3}\right)^b \in S$$

για κάθε $a, b \in \mathbb{N}$. (Αν $a = 0$, $\left(\frac{1}{2}\right)^0 = 1 \in S$.) Επομένως $m\frac{1}{2^a}\frac{1}{3^b} \in S$ πάλι από την κλειστότητα του πολλαπλασιασμού του S. Δηλαδή $R \subseteq S$.

iii) Θα δείξουμε ότι ο R δεν είναι σώμα. Παρατηρούμε ότι το $5 \in R$ ($m = 5, a = b = 0$). Αρκεί να δείξουμε ότι το 5 δεν είναι αντιστρέψιμο στον R. Πράγματι, ας υποθέσουμε ότι είναι αντιστρέψιμο. Τότε το αντίστροφό του στον R είναι ίσο με $\frac{1}{5}$ (γιατί το 5 είναι αντιστρέψιμο και στο $\mathbb{Q}$ και $1_R = 1_{\mathbb{Q}}$) . Επομένως

$$\frac{1}{5} = \frac{m}{2^a 3^b} \quad (m \in \mathbb{Z}, a, b \in \mathbb{N}).$$

Τότε έχουμε, $5m = 2^a 3^b \overset{5 \text{ πρώτος}}{\Longrightarrow} 5|2^a \quad \text{ή} \quad 5|3^b$, άτοπο.

9. *Υπόδειξη.* Δεν είναι υποδακτύλιος του $\mathbb{R}$, διότι δεν είναι κλειστό ως προς τον πολλαπλασιασμό. Ειδικά, $\sqrt[3]{3} \in R$, αλλά $(\sqrt[3]{3})(\sqrt[3]{3}) = \sqrt[3]{9} \notin R$. Δείξτε την τελευταία σχέση επιχειρηματολογώντας ότι δεν υπάρχουν ακέραιοι a, b με $\sqrt[3]{9} = a + b\sqrt[3]{3}$.

10. *Λύση.* Από τη σχέση $(2+\sqrt{3})(2-\sqrt{3}) = 1$ έπεται ότι $a = 2+\sqrt{3} \in U(R)$. Άρα για κάθε θετικό ακέραιο n έχουμε $a^n \in U(R)$ και τα a^n είναι διακεκριμένα.

11. *Απάντηση.* Περιοχή και σώμα αντίστοιχα.

12. *Λύση.* Επειδή οι m, n είναι σχετικά πρώτοι υπάρχουν ακέραιοι x, y με $1 = mx + ny$. Επειδή οι m, n είναι θετικοί, ακριβώς ένας από τους x, y είναι αρνητικός, έστω χωρίς περιορισμό της γενικότητας ότι αυτός είναι ο y.

Έστω χωρίς περιορισμό της γενικότητας ότι το b δεν είναι δεξιός μηδενοδιαιρέτης. Επειδή $1 + n(-y) = mx$ έχουμε

$$a(a^n)^{-y} = (a^m)^x \Rightarrow a(b^n)^{-y} = (b^m)^x \Rightarrow (a-b)b^{n(-y)} = 0.$$

Από το πρώτο ερώτημα παίρνουμε $a - b = 0$.

13. *Απάντηση* iii) Όχι. Για παράδειγμα, το $(1, 0) \in \mathbb{R} \times \mathbb{R}$ δεν είναι αντιστρέψιμο αφού $(1, 0)(x, y) = (x, 0) \neq (1, 1)$ για κάθε $(x, y) \in \mathbb{R} \times \mathbb{R}$.

iv) Ναι.

v) Ναι.

14. *Απάντηση.* $U(T_2(\mathbb{Z})) = \left\{ A \in M_2(\mathbb{Z}) : A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, a, c \in \{1, -1\} \right\}$.

15. *Λύση.* i) Άμεση εφαρμογή της Πρότασης 3.22.

ii) Παρατηρούμε ότι

$$\begin{pmatrix} [2] & [3] \\ [0] & [4] \end{pmatrix}\begin{pmatrix} [1] & [2] \\ [0] & [3] \end{pmatrix} = \begin{pmatrix} [2] & [13] \\ [0] & [12] \end{pmatrix}, \text{ και}$$
$$\begin{pmatrix} [1] & [2] \\ [0] & [3] \end{pmatrix}\begin{pmatrix} [2] & [3] \\ [0] & [4] \end{pmatrix} = \begin{pmatrix} [2] & [11] \\ [0] & [12] \end{pmatrix}.$$

Προφανώς,

$$\begin{pmatrix} [2] & [13] \\ [0] & [12] \end{pmatrix} \neq \begin{pmatrix} [2] & [11] \\ [0] & [12] \end{pmatrix},$$

άρα ο $T_2(\mathbb{Z}_n)$ δεν είναι μεταθετικός.

iii) Έστω

$$A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in M_2(\mathbb{Z}_n).$$

Αν $A \in U\left(M_2(\mathbb{Z}_n)\right)$, τότε υπάρχει $B \in U\left(M_2(\mathbb{Z}_n)\right)$ ώστε $AB = BA = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}$. Δηλαδή υπάρχουν $x, y, z \in \mathbb{Z}$ ώστε

$$\begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix}\begin{pmatrix} [x] & [y] \\ [0] & [z] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}.$$

Επομένως $\begin{pmatrix} [ax] & [ay+bz] \\ [0] & [cz] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}$. Έπεται ότι $[ax] = [cz] = [1]$, δηλαδή $[a][x] = [c][z] = 1$. Άρα $[a], [c] \in U(\mathbb{Z}_n)$.

Αντίστροφα, παρατηρούμε ότι αν $[a], [c] \in U(\mathbb{Z}_n)$, τότε επιλέγοντας

$$B = \begin{pmatrix} [a'] & [y] \\ [0] & [c'] \end{pmatrix},$$

όπου $[y] = -[a'][c'][b]$, $[a']$ το αντίστροφο του $[a]$ και $[c']$ το αντίστροφο του $[c]$ στο $\mathbb{Z}_n$, εύκολα ελέγχουμε με πράξεις ότι $AB = BA = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix}$. Δείξαμε την εξής ισοδυναμία,

$$A = \begin{pmatrix} [a] & [b] \\ [0] & [c] \end{pmatrix} \in U(M_2(\mathbb{Z}_n)) \quad \Leftrightarrow \quad [a], [c] \in U(\mathbb{Z}_n) \quad \text{και} \quad [b] \quad \text{τυχαίο}.$$

Επομένως $|U(M_2(\mathbb{Z}_n)| = |U(\mathbb{Z}_n)|^2 \cdot |\mathbb{Z}_n| = \varphi(n)^2 n$.

16. *Απάντηση.* Ναι και η απόδειξη είναι άμεση με την Πρόταση 3.22.

17. *Υπόδειξη.* Χρησιμοποιήστε επαγωγή στο n και ονειρευτείτε όπως ο πρωτοετής (Παράδειγμα 3.17).

18. *Λύση.* Χρησιμοποιώντας δύο φορές την υπόθεση έχουμε για κάθε $r \in R$

$$-r = (-r)^2 = (-1)^2 r^2 = r^2 = r \Rightarrow 2r = 0_R.$$

Για κάθε $a, b \in R$ έχουμε

$$a + b = (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 = a + ab + ba + b$$

και επομένως $ba = -(ab)$. Από την πρώτη σχέση έχουμε $-(ab) = ab$ οπότε ba=ab.

19. *Απάντηση.* $n = 1, 2$.

20. *Λύση.* i) Έστω $[a] \in \mathbb{Z}_{30}$ με $[a]^m = 0$, για κάποιο $m \in \mathbb{Z}_{>0}$. Τότε $[a^m] = [0]$, δηλαδή $30|a^m$. Αφού $30 = 2 \cdot 3 \cdot 5$, έχουμε

$$2|a^m,\ 3|a^m,\ 5|a^m.$$

Επειδή οι $2, 3, 5$ είναι πρώτοι, έχουμε $2|a,\ 3|a,\ 5|a$. Έπεται ότι $30|a$ (αφού $2, 3, 5$ είναι σχετικά πρώτοι). Τότε $[a] = [0]$, άρα στο $\mathbb{Z}_{30}$ υπάρχει μοναδικό μηδενοδύναμο στοιχείο, το $[0]$.

Έστω τώρα $[a] \in \mathbb{Z}_{60}$ με $[a]^m = 0$, για κάποιο $m \in \mathbb{Z}_{>0}$. Τότε $[a^m] = [0]$, δηλαδή $60|a^m$. Αφού $60 = 2^2 \cdot 3 \cdot 5$, έχουμε

$$2|a^m,\ 3|a^m,\ 5|a^m.$$

Αφού $2, 3, 5$ είναι πρώτοι, έχουμε $2|a,\ 3|a,\ 5|a$. Έπεται ότι $30|a$ (αφού $2, 3, 5$ είναι σχετικά πρώτοι). Άρα $[a] = [0]$ ή $[a] = [30]$ (στο $\mathbb{Z}_{60}$). Παρατηρούμε ότι το $[30]$ είναι μηδενοδύναμο ($[30]^2 = [900] = [0]$). Άρα υπάρχουν ακριβώς δύο μηδενοδύναμα στοιχεία στο $\mathbb{Z}_{60}$, το $[0]$ και το $[30]$.

ii) Έστω ότι ο $\mathbb{Z}_n$, $n > 1$, δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο. Έστω $n = p_1^{n_1} \cdots p_k^{n_k}$, η ανάλυση του n σε γινόμενο πρώτων παραγόντων και έστω

$$a = p_1 p_2 \cdots p_k,\ N = \max\{n_1, \cdots n_k\}.$$

Παρατηρούμε ότι

$$[a]^N = [a^N] = [0],$$

αφού $n|a^N$. Από την υπόθεση έχουμε $[a] = [0]$, δηλαδή $n|a$. Άρα

$$n = a = p_1^{n_1} \cdots p_k^{n_k}.$$

Αντίστροφα, έστω ότι δεν υπάρχει πρώτος p ώστε $p^2|n$. Τότε η ανάλυση του n σε γινόμενο πρώτων είναι $n = p_1 p_2 \cdots p_k$ (p_i διακεκριμένοι πρώτοι). Έστω $[a] \in \mathbb{Z}_n$ ώστε $[a]^m = [0]$. Τότε

$$[a^m] = [0] \Rightarrow n|a^m \Rightarrow p_i|a,$$

για κάθε i. Επειδή οι $p_1, p_2, \ldots, p_n$ είναι ανά δύο σχετικά πρώτοι, έπεται ότι

$$p_1 p_2 \cdots p_n|a.$$

Άρα $n|a$, δηλαδή $[a] = [0]$.

iii) Προφανώς $nil(R) \neq \emptyset$, αφού $0_R \in nil(R)$. Έστω $r, s \in nil(R)$, οπότε $r^m = s^n = 0_R$ για κάποια $m, n \in \mathbb{Z}_{>0}$.

Θα δείξουμε ότι $rs \in nil(R)$. Πράγματι έχουμε,

$$(rs)^m = r^m s^m = 0_R s^m = 0_R,$$

όπου στην πρώτη ισότητα χρησιμοποιήσαμε το γεγονός ότι ο R είναι μεταθετικός.

Επίσης $-r \in nil(R)$. Πράγματι, $(-r)^m = (-1)^m r^m = 0_R$.

Τέλος θα δείξουμε ότι $r + s \in nil(R)$. Επειδή ο R είναι μεταθετικός, έχουμε

$$(r+s)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} r^{m+n-i} s^i. \tag{3.2}$$

Παρατηρούμε ότι αν $i \geq n$, τότε

$$r^{m+n-i} s^i = r^{m+n-i} 0_R = 0_R.$$

Αν $i \leq n$, τότε $m + n - i \geq m$ και

$$r^{m+n-i} s^i = 0_R s^i = 0_R.$$

Επομένως από την (3.2) έπεται ότι $(r+s)^{m+n} = 0_R$, οπότε $r + s \in nil(R)$. Η απόδειξη είναι πλήρης.

21. *Λύση.* Αν $(r, s) \in nil(R \times S)$ τότε υπάρχει θετικός ακέραιος n με

$$(0_R, 0_S) = (r, s)^n = (r^n, s^n) \Rightarrow r^n = 0_R, s^n = 0_S \Rightarrow r \in nil(R), s \in nil(S).$$

Συνεπώς $nil(R \times S) \subseteq nil(R) \times nil(S)$.

Αν $(r, s) \in nil(R) \times nil(S)$, τότε υπάρχουν θετικοί ακέραιοι m, n με $r^n = 0_R, s^m = 0_S$. Επιλέγοντας $k = max(m, n)$ έχουμε

$$(0_R, 0_S) = (r^k, s^k) = (r, s)^k \Rightarrow (r, s) \in nil(R \times S).$$

Συνεπώς $nil(R) \times nil(S) \subseteq nil(R \times S)$. Επομένως $nil(R \times S) = nil(R) \times nil(S)$.

22.

23. *Λύση.* $(R_i)_{i\in I}$ μια οικογένεια υποδακτυλίων του S και $R=\cap R_i$. Επειδή $1_S\in R_i$ για κάθε i, έχουμε ότι $1_S\in R$, οπότε το R είναι μη κενό σύνολο. Έστω $a,b\in R$ οπότε $a,b\in R_i$ για κάθε $i\in I$. Επειδή ο R_i είναι υποδακτύλιος του S, έχουμε $a-b,\ ab\in R_i$ για κάθε $i\in I$. Συνεπώς $a-b,ab\in R$. Άρα το R είναι υποδακτύλιος του S σύμφωνα με την Πρόταση 3.22.

i) Έστω τώρα $R=\cap R_i$, όπου το R_i διατρέχει όλου τους υποδακτύλιους του $\mathbb{C}$ που περιέχουν το 1. Από το πρώτο ερώτημα, το R είναι υποδακτύλιος του $\mathbb{C}$. Επειδή $1\in R$ έχουμε $m1\in R$ για κάθε ακέραιο m, οπότε $\mathbb{Z}\subseteq R$.

Από τον ορισμό του R έχουμε ότι $R\subseteq R_i$ για κάθε i. Το $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{C}$ που περιέχει το 1. Δηλαδή ένας από τους R_i είναι ο $\mathbb{Z}$. Άρα $R\subseteq\mathbb{Z}$. Συνεπώς $R=\mathbb{Z}$.

ii) Η τομή όλων των υποδακτυλίων του $\mathbb{C}$ που περιέχουν το 1 και το i είναι ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss. Η απόδειξη είναι παρόμοια με αυτή του i) και παραλείπεται.

24. *Απάντηση.* Η τομή όλων των υποσωμάτων του $\mathbb{C}$ είναι το $\mathbb{Q}$.

25. *Λύση.* Από την υπόθεση υπάρχει θετικός ακέραιος n με $r^n=0_R$. Παρατηρούμε ότι

$$(1_R-r)(1_R+r+r^2+\cdots+r^{n-1})=1_R-r^n=1_R,$$
$$(1_R+r+r^2+\cdots+r^{n-1})(1_R-r)=1_R-r^n=1_R.$$

Άρα $1_R-r\in U(R)$.

26. *Λύση.* Ως υποδακτύλιος μεταθετικού δακτυλίου, ο R είναι μεταθετικός. Περιέχει εξ ορισμού το 1. Συνεπώς για να δείξουμε ότι ο R είναι σώμα αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο. Έστω $a\in R-0$. Θεωρούμε την απεικόνιση

$$f:R\times R\to R, f(r)=ar.$$

Εύκολα επαληθεύεται ότι f είναι $\mathbb{Q}$ - γραμμική. Επίσης είναι 1-1 γιατί αν $ar=ar'$, Τότε επειδή το $\mathbb{C}$ είναι περιοχή και $a\neq 0$, έχουμε $r=r'$. Θυμόμαστε από τη Γραμμική Άλγεβρα ότι κάθε 1-1 γραμμική απεικόνιση $V\to V$, όπου V πεπερασμένης διάστασης διανυσματικός χώρος, είναι επί. Συνεπώς υπάρχει $r\in R$ με $ar=1$. Άρα το a είναι αντιστρέψιμο.

27. *Λύση.* Έστω R υποδακτύλιος του $M_2(\mathbb{R})$ που περιέχει τους συμμετρικούς πίνακες. Συνεπώς $\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\1&0\end{pmatrix}\in R$. Άρα ο R περιέχει το γινόμενο $\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\1&0\end{pmatrix}$ και τη διαφορά $\begin{pmatrix}0&1\\1&0\end{pmatrix}-\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$.

Τελικά ο R περιέχει τους $\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}$. Από αυτό έπεται ότι $R=M_2(\mathbb{R})$ καθώς

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}=a\begin{pmatrix}1&0\\0&0\end{pmatrix}+b\begin{pmatrix}0&1\\0&0\end{pmatrix}+c\begin{pmatrix}0&0\\1&0\end{pmatrix}+d\begin{pmatrix}0&0\\0&1\end{pmatrix}\in R$$

για κάθε $a,b,c,d\in\mathbb{R}$.

28. Μια επιλογή παραδειγμάτων είναι:

i) $R=M_2(\mathbb{R}), a=\begin{pmatrix}1&0\\0&0\end{pmatrix}, b=\begin{pmatrix}0&1\\0&0\end{pmatrix}$.

ii) $S=\{\begin{pmatrix}0&a\\0&0\end{pmatrix}\in M_2(\mathbb{R}):a\in\mathbb{R}\}$.

29. *Λύση.* Επειδή το a δεν είναι δεξιός μηδενοδιαιρέτης, η απεικόνιση $R\to R, r\mapsto ra$, είναι 1-1. (Πράγματι, αν $r_1a=r_2a=0$, τότε $(r_1-r_2)a=0$ και επομένως $r_1-r_2=0$ αφού το a δεν είναι δεξιός μηδενοδιαιρέτες). Επειδή το σύνολο R είναι πεπερασμένο, η απεικόνιση αυτή είναι επί. Συνεπώς υπάρχει $e\in R$ με $ea=a$. Παρατηρούμε ότι

$$(ae-a)a=(ae)a-a^2=a(ea)-a^2=aa-a^2=0_R.$$

Επειδή το a δεν είναι δεξιός μηδενοδιαιρέτης παίρνουμε $ae=a$.

30. *Λύση.* Έστω ότι το $a \in R$ δεν είναι μηδενοδιαιρέτης. Τότε η απεικόνιση $R \to R, r \mapsto ra$, είναι 1-1 (βλ. λύση προηγούμενης άσκησης). Επειδή το σύνολο R είναι πεπερασμένο, η απεικόνιση αυτή είναι επί. Συνεπώς υπάρχει $b \in R$ με $ba = 1$. Επειδή ο R είναι μεταθετικός, αυτό σημαίνει ότι το a είναι αντιστρέψιμο.
Σημείωση. Καλό είναι το παραπάνω επιχείρημα να συγκριθεί με την απόδειξη της Πρότασης 3.14.
Λύση της γενίκευσης: Θεωρώντας τα στοιχεία $a, a^2, a^3, ...$ του R υπάρχουν $m > n \geq 0$ με $a^m = a^n$. Επειδή το a δεν είναι αντιστρέψιμο ισχύει $n > 0$. Θεωρούμε μια επιλογή των m, n με m ελάχιστο. Για $b = a^{m-1} - a^{n-1} \in R$ έχουμε $ab = ba = 0$. Από το ελάχιστο του m έπεται ότι $b \neq 0_R$.

31. *Λύση.* Για κάθε $a \in R$ έχουμε $-a = (-a)^n = (-1)^n a^n = (-1)^n a = a$.

32. *Λύση.* Από την υπόθεση έχουμε $0 = ab = b(ab)a = (ba)^2 = ba$.

33. Δύσκολη άσκηση. *Υπόδειξη.* Έστω $x, y \in R$.
    (1) Αναπτύσσοντας το αριστερό μέλος της $(x+y)^3 - (x-y)^3 = (x+y) - (x-y) = 2y$, δείξτε ότι $A = 0$, όπου $A = 2x^2y + 2xyx + 2yx^2$. Χρησιμοποιώντας $xA - Ax = 0$, δείξτε ότι $2xy = 2yx$.
    (2) Από $(x+x)^3 = x + x$ έπεται ότι $6x = 0$.
    (3) Αναπτύσσοντας τη $(x+y)^3 - (x^3 + y^3) = 0$, θέτοντας $y = x^2$ και χρησιμοποιώντας το (2), δείξτε ότι $3x^2 = 3x$.
    (4) Χρησιμοποιώντας τα (3) και (2), δείξτε ότι $3xy = 3yx$. Το ζητούμενο έπεται από τις (4) και (1).

34. *Υπόδειξη.* Στη θέση του a θέστε $1+a$ στη σχέση $(ab)^2 = a^2b^2$ για να δείξετε ότι $bab = ab^2$. Στη σχέση αυτή θέστε $1 + b$ στη θέση του b για να δείξετε ότι $ab = ba$.

35. *Υπόδειξη.* Δείξτε αρχικά ότι $b^2ab = bab^2$ για κάθε $a, b \in R$. Στη συνέχεια βρείτε με τη χρήση αυτού, κατάλληλη δύναμη του $ab - ba$ που ισούται με 0.

Πολυώνυμα

Εδώ μελετάμε πολυωνυμικούς δακτυλίους. Θα δούμε ότι όταν οι συντελεστές είναι από σώμα, ο δακτύλιος των πολυωνύμων έχει αρκετές κοινές ιδιότητες με το δακτύλιο των ακεραίων, που εξετάσαμε στο Κεφάλαιο 1. Επίσης εξετάζουμε το πολυώνυμο $x^p - x$ πάνω από το σώμα $\mathbb{Z}_p, p$ πρώτος, και πολυωνυμικές συναρτήσεις. Τέλος μελετάμε ανάγωγα πολυώνυμα.

Βασικά σημεία

- δακτύλιος πολυωνύμων
- διαιρετότητα πολυωνύμων και Ευκλείδειος αλγόριθμος
- ρίζες πολυωνύμων
- το πολυώνυμο $x^p - x$
- ανάγωγα πολυώνυμα

4.1. Ο δακτύλιος των πολυωνύμων

Πρόταση 4.1. *Έστω R δακτύλιος με 1_R. Τότε υπάρχει δακτύλιος $\overline{R}$ με $1_{\overline{R}} = 1_R$, ώστε*

(1) *Ο R είναι υποδακτύλιος του $\overline{R}$.*
(2) *Υπάρχει $x \in \overline{R}$ ώστε $rx = xr$, για κάθε $r \in R$.*
(3) *Κάθε στοιχείο του $\overline{R}$ έχει μια παράσταση της μορφής*
$$r_0 + r_1 x + r_2 x^2 + \cdots + r_m x^m \quad (r_i \in R).$$
(4) *Αν $r_0 + r_1 x + \cdots + r_m x^m = s_0 + s_1 x + \cdots + s_n x^n \quad (r_i, s_i \in R), m \leq n$, τότε*
$$r_0 = s_0, r_1 = s_1, \ldots, r_m = s_m \text{ και } s_{m+1} = \cdots = s_n = 0_R.$$

Σκιαγράφηση της απόδειξης. Έστω $R^{\mathbb{N}}$ το σύνολο των ακολουθιών $(a_0, a_1, a_2, \ldots)$, όπου $a_i \in R$ για κάθε $i \in \mathbb{N}$. Αν $(a_0, a_1, a_2, \ldots,), (b_0, b_1, b_2, \ldots) \in R^{\mathbb{N}}$ ορίζουμε το άθροισμα

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

και το γινόμενο

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

με $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0$ για κάθε $n \in \mathbb{N}$. Είναι θέμα ρουτίνας η επαλήθευση ότι το $R^{\mathbb{N}}$ με τις παραπάνω πράξεις είναι ένας δακτύλιος με μοναδιαίο στοιχείο το

$$(1_R, 0_R, 0_R, \ldots).$$

Ένα στοιχείο $(a_0, a_1, a_2, \ldots)$ του $R^{\mathbb{N}}$ ονομάζεται **πολυώνυμο** αν υπάρχει $m \in \mathbb{N}$ με $a_k = 0$ για κάθε $k > m$.

Έστω $\overline{R}$ το σύνολο των πολυωνύμων του $R^{\mathbb{N}}$. Είναι φανερό ότι το $\overline{R}$ είναι ένας υποδακτύλιος του $R^{\mathbb{N}}$.

Θα ταυτίζουμε ένα $a \in R$ με το αντίστοιχο πολυώνυμο $(a, 0_R, 0_R, \ldots)$. Κάτω από αυτή την ταύτιση, το μηδενικό στοιχείο του $\overline{R}$, δηλαδή το $(0_R, 0_R, \ldots)$, ταυτίζεται με το 0_R και το μοναδιαίο στοιχείο του $\overline{R}$ ταυτίζεται με το 1_R. Κάτω από αυτή την ταύτιση, οι πράξεις του R είναι οι περιορισμοί των πράξεων του $\overline{R}$. Έτσι ο R μπορεί να θεωρηθεί σαν υποδακτύλιος του $\overline{R}$. Θέτουμε

$$x = (0_R, 1_R, 0_R, \ldots),$$

τότε με επαγωγή στο n αποδεικνύεται εύκολα ότι

$$x^n = (0_R, 0_R, \ldots, 1_R, 0_R, \ldots)$$

για κάθε $n \in \mathbb{N}$, όπου το 1_R ευρίσκεται στη θέση $n+1$. Από τον ορισμό, κάθε στοιχείο του $\overline{R}$ είναι της μορφής $(a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots)$. Παρατηρούμε ότι $(a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots) =$

$$\begin{aligned}
&= (a_0, 0_R, \ldots) + (0_R, a_1, 0_R, \ldots) + \cdots + (0_R, \ldots, 0_R, a_m, 0_R, \ldots) \\
&= (a_0, 0_R, \ldots)(1_R, 0_R, \ldots) + (a_1, 0_R, \ldots)(0_R, 1_R, 0_R, \ldots) \\
&\quad + \cdots + (a_m, 0_R, \ldots)(0_R, \ldots, 0_R, 1_R, 0_R, \ldots) \\
&= (a_0, 0_R, \ldots)x^0 + (a_1, 0_R, \ldots)x + \cdots + (a_m, 0_R, \ldots)x^m.
\end{aligned}$$

Άρα το στοιχείο $(a_0, a_1, \ldots, a_m, 0_R, \ldots)$, κάτω από την ταύτιση που αναφέραμε πριν, έχει μια παράσταση της μορφής

$$a_0 + a_1x + \cdots + a_mx^m.$$

Είναι σαφές ότι $ax = xa$ για κάθε $a \in R$. Τέλος είναι σαφές ότι αν $a_0 + a_1x + \cdots + a_mx^m = b_0 + b_1x + \cdots b_nx^n$ με $m \geq n$, τότε $a_i = b_i$ για κάθε $i \leq n$ και $a_j = 0$ για κάθε $j = n+1, \ldots, m$. Ιδιαίτερα αν $a_0 + a_1x + \cdots + a_mx^m = 0_R$, τότε $a_i = 0_R$ για κάθε $i = 0, 1, \ldots, m$. □

Το δακτύλιο $\overline{R}$ συμβολίζουμε με $R[x]$ και τον ονομάζουμε το **δακτύλιο των πολυωνύμων** με συντελεστές από το R.

Παρατηρήσεις. Με τις προηγούμενες υποθέσεις και συμβολισμούς σημειώνουμε τα εξής.

(1) $0_{R[x]} = 0_R$ (αφού R υποδακτύλιος του $R[x]$).

(2) $0_Rx^k = 0_R$, για κάθε $k \in \mathbb{Z}_{>0}$.

(3) Αν $f(x), g(x) \in R[x]$, μπορούμε να γράψουμε

$$\begin{aligned}
f(x) &= f_0 + f_1x + \cdots + f_mx^m \ \ (f_i \in R), \\
g(x) &= g_0 + g_1x + \cdots + g_mx^m \ \ (g_i \in R)
\end{aligned}$$

(όπου το m είναι το ίδιο).

(4) Οι πράξεις στον δακτύλιο $R[x]$ λαμβάνουν την εξής μορφή. Αν $f(x), g(x)$ όπως πριν, τότε

$$f(x) + g(x) = f_0 + g_0 + (f_1 + g_1)x + \cdots + (f_m + g_m)x^m.$$

Αν $f(x) = f_0 + f_1x + \cdots + f_mx^m$ και $g(x) = g_0 + g_1x + \cdots + g_nx^n$, τότε

$$f(x)g(x) = c_1x + c_2x^2 + \cdots c_{m+n}x^{m+n},$$

όπου $c_k = \sum_{i=0}^{k} f_ig_{k-i}$.

(5) Από το (4) έπεται ότι αν ο R είναι *μεταθετικός* με μονάδα, τότε και ο $R[x]$ είναι μεταθετικός.

Παράδειγμα 4.2. Έστω p πρώτος. Τότε για κάθε $f(x) \in \mathbb{Z}_p[x]$ και κάθε θετικό ακέραιο n ισχύει

$$(f(x))^{p^n} = f(x^{p^n}),$$

δηλαδή $(f_0 + f_1x + \cdots + f_mx_m)^{p^n} = f_0 + f_1x^{p^n} + \cdots + f_m(x^{p^n})^m$. Για παράδειγμα, στο $\mathbb{Z}_3[x]$ και για $n = 1$ έχουμε $([1] + [1]x + [2]x^5)^3 = [1] + [1]x^3 + [2]x^{15}$.

Απόδειξη. Έστω $n = 1$. Από το Παράδειγμα 3.17, έχουμε

$$\begin{aligned}(f_0 + f_1x + \cdots + f_mx^m)^p &= (f_0)^p + (f_1x)^p + \cdots + (f_mx^m)^p \\ &= f_0^p + f_1^p x^p + \cdots + f_m^p (x^m)^p.\end{aligned}$$

Παρατηρούμε όμως ότι για κάθε i, έχουμε $f_i^p = f_i$ από το μικρό θεώρημα του Fermat. Έστω ότι $n \geq 1$ και $(f(x))^{p^n} = f(x^{p^n})$ για κάθε $f(x) \in \mathbb{Z}_p[x]$. Έχουμε διαδοχικά,

$$(f(x))^{p^{n+1}} = ((f(x))^{p^n})^p = (f(x^{p^n}))^p = f(x^{p^{n+1}}).$$

□

Έστω R δακτύλιος με 1_R. Ο δακτύλιος $R[x]$ έχει μοναδιαίο στοιχείο $1_{R[x]} = 1_R$. Δεχόμαστε το συμβολισμό $x^0 = 1$. Κάθε $f(x) \in R[x]$ με $f(x) \neq 0$ γράφεται μοναδικά στην μορφή

$$f(x) = f_0x^0 + f_1x^1 + \cdots + f_mx^m, \quad f_i \in R, \quad f_m \neq 0.$$

Το στοιχείο $f_m \neq 0$ λέγεται ο **μεγιστοβάθμιος συντελεστής** του $f(x)$ και το m λέγεται ο **βαθμός** του $f(x)$ (συμβολίζουμε με $m = \deg f(x)$). Αν $f(x) \neq 0$ (μηδενικό στοιχείο του $R[x]$), δεχόμαστε ότι $\deg f(x) = -\infty$, $-\infty < n$ για κάθε $n \in \mathbb{N}$ και $-\infty + n = -\infty$ για κάθε $n \in \mathbb{N}$. Για παράδειγμα, όταν λέμε $f(x) \in R[x]$, $\deg f(x) \leq 2$, εννοούμε ότι $f(x) = 0$ ή $f(x) \neq 0$ και $\deg f(x) = 0, 1, 2$..

Πρόταση 4.3. *Έστω R δακτύλιος με μοναδιαίο στοιχείο και $f(x), g(x) \in R[x]$. Τότε ισχύουν τα ακόλουθα.*

(1) $\deg(f(x)+g(x)) \leq \max\{\deg f(x), \deg g(x)\}$. *Ειδικά, αν για τους μεγιστοβάθμιους συντελεστές f_m και g_n των $f(x)$, $g(x)$ αντίστοιχα έχουμε $f_mx^m + g_nx^n \neq 0$, τότε ισχύει η ισότητα.*

(2) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$. *Ειδικά, αν για τους μεγιστοβάθμιους συντελεστές f_m και g_n των $f(x)$, $g(x)$ αντίστοιχα έχουμε $f_mg_n \neq 0$, τότε ισχύει η ισότητα.*

Απόδειξη. Άμεση από τον ορισμό του βαθμού. □

Για παράδειγμα, αν $f(x) = 4x^3 - 2x + 1, g(x) = -4x^3 + x^2 + 5 \in \mathbb{Z}[x]$, τότε $f(x) + g(x) = x^2 - 2x + 6$ που έχει βαθμό $2 < 3$.

Παράδειγμα 4.4. Πόσα πολυώνυμα στο $\mathbb{Z}_5[x]$ έχουν βαθμό ≤ 3; Πόσα έχουν βαθμό 3; Παρατηρούμε ότι κάθε πολυώνυμο του πρώτου ερωτήματος της εκφώνησης γράφεται μοναδικά στη μορφή

$$f(x) = f_0 + f_1x + f_2x^2 + f_3x^3 \ \ (f_i \in \mathbb{Z}_5).$$

Επειδή το $\mathbb{Z}_5$ έχει 5 στοιχεία, το ζητούμενο πλήθος είναι $5 \cdot 5 \cdot 5 \cdot 5 = 5^4$. Για το δεύτερο ερώτημα παρατηρούμε ότι κάθε πολυώνυμο βαθμού 3 γράφεται μοναδικά στη μορφή $f(x) = f_0+f_1x+f_2x^2+f_3x^3$ $(f_i \in \mathbb{Z}_5)$, όπου $f_3 \neq [0]$. Άρα το ζητούμενο πλήθος είναι $5 \cdot 5 \cdot 5 \cdot 4 = 4 \cdot 5^3$.

Πρόταση 4.5. *Έστω R περιοχή. Τότε ισχύουν τα επόμενα.*
(1) *$R[x]$ είναι περιοχή.*
(2) *Αν $f(x), g(x) \in R[x]$, τότε $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.*
(3) *$U(R[x]) = U(R)$.*

Απόδειξη. (1) Γνωρίζουμε ότι ο $R[x]$ είναι δακτύλιος με $1_{R[x]} = 1_R$. Επειδή R είναι περιοχή, $1_R \neq 0_R$. Επομένως $1_{R[x]} \neq 0_{R[x]}$. Αφού ο R είναι μεταθετικός, είναι και ο $R[x]$. Έστω $f(x), g(x) \in R[x]$ με $f(x), g(x) \neq 0 (= 0_R)$. Έστω f_m, g_n οι μεγιστοβάθμιοι συντελεστές των $f(x), g(x)$ αντίστοιχα. Τότε $f_m, g_n \neq 0$ και επειδή R περιοχή, έπεται $f_m g_n \neq 0$. Δηλαδή ο μεγιστοβάθμιος συντελεστής των $f(x), g(x)$ δεν είναι μηδέν. Άρα $f(x)g(x) \neq 0$, δηλαδή $R[x]$ είναι περιοχή.
(2) Το είδαμε στην Πρόταση 4.3.
(3) Ο εγκλεισμός $U(R) \subseteq U(R[x])$ είναι σαφής, αφού ο R είναι υποδακτύλιος του $R[x]$ και $1_R = 1_{R[x]}$.

Αντίστροφα, έστω $f(x) \in U(R[x])$. Τότε υπάρχει $g(x) \in U(R[x])$ ώστε,

$$f(x)g(x) = 1 \Rightarrow \deg f(x) + \deg g(x) = 0 \Rightarrow \deg f(x) = \deg g(x) = 0.$$

Επομένως $f(x), g(x) \in R$ και επειδή $f(x)g(x) = 1$, έχουμε ότι $f(x) \in U(R)$. □

Σε σχέση με το (3) της προηγούμενης πρότασης, σημειώνουμε ότι στο $\mathbb{Z}_4[x]$ (που δεν είναι περιοχή), έχουμε

$$([2]x + [1])(2[x] + [1]) = [4]x^2 + [4]x + [1] = [1].$$

Δηλαδή βρήκαμε πολυώνυμο πρώτου βαθμού, το $[2]x + [1] \in U(\mathbb{Z}_4[x])$, που είναι αντιστρέψιμο.

Σημείωση. Συμβολισμός πολυωνύμων με συντελεστές στο $\mathbb{Z}_n$.
Από τώρα και στο εξής, αντί να γράφουμε $f(x) = [2]x + [1] \in \mathbb{Z}_4[x]$, θα γράφουμε απλά $f(x) = 2x + 1 \in \mathbb{Z}_4[x]$ κατανοώντας ότι οι συντελεστές 2 και 1 του $f(x) = 2x + 1$ είναι τα στοιχεία $[2], [1]$ αντίστοιχα του $\mathbb{Z}_4$. Έτσι η προηγούμενη ισότητα στο $\mathbb{Z}_4[x]$ γράφεται $(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1$.

Παράδειγμα 4.6.

Έστω R περιοχή. Τότε δεν υπάρχει $f(x) \in R[x]$ ώστε,

$$(x + 1)^{2020} + (x^2 + 1)^{40} = f(x)^{30}.$$

Πράγματι, $\deg(x + 1)^{2020} = 2020$, $\deg(x^2 + 1)^{40} = 80$. Επομένως η Πρόταση 4.3 δίνει $2020 = 30\deg f(x)$, που είναι αδύνατο καθώς το 30 δεν διαιρεί το 2020.

Πολυωνυμικές συναρτήσεις Έστω R μεταθετικός δακτύλιος με 1_R και $f(x) \in R[x]$,

$$f(x) = f_0 + f_1 x + \cdots f_m x^m.$$

Αν $r \in R$, θέτουμε

$$f(r) = f_0 + f_1 r + \cdots f_m r^m$$

που είναι στοιχείο του R. Εύκολα επαληθεύεται ότι αν $f(x), g(x) \in F[x]$, $a(x) = f(x) + g(x)$ και $b(x) = f(x)g(x)$, τότε για κάθε $r \in R$ έχουμε

$$a(r) = f(r) + g(r),\ b(r) = f(r)g(r).$$

(Χρειαζόμαστε τη μεταθετικότητα του R στη δεύτερη ισότητα). Για παράδειγμα, αν έχουμε την ισότητα πολυωνύμων $f(x) = q(x)g(x) + h(x)$, τότε για κάθε $r \in R$ έχουμε την ισότητα $f(r) = q(r)g(r) + h(r)$ στοιχείων του R.

Η συνάρτηση $\bar{f} : R \to R$, $\bar{f}(r) = f(r)$ λέγεται η **πολυωνυμική συνάρτηση** που επάγεται από το $f(x)$. Έχουμε λοιπόν μια συνάρτηση

$$\psi : R[x] \to F(R, R),$$

$\psi(f(x)) = \bar{f}$, όπου $F(R,R)$ είναι ο δακτύλιος του Παραδείγματος 3.3(8), η οποία ικανοποιεί τις ιδιότητες

- $\psi(f(x)+g(x)) = \psi(f(x)) + \psi(g(x))$,
- $\psi(f(x)g(x)) = \psi(f(x))\psi(g(x))$

για κάθε $f(x), g(x) \in F[x]$.

Προσοχή. Η ψ γενικά δεν είναι $1-1$. (Συνεπώς δεν μπορούμε γενικά να ταυτίζουμε πολυώνυμα με τις αντίστοιχες πολυωνυμικές συναρτήσεις). Πράγματι, έστω p πρώτος και $R = \mathbb{Z}_p$. Έστω $f_1(x) = x^p - x \in \mathbb{Z}_p[x]$ και $f_2(x) = 0$. Τότε για κάθε $r \in \mathbb{Z}_p$, $\bar{f}_1(r) = r^p - r = 0$ (μικρό θεώρημα Fermat). Δηλαδή,

$$\psi(f_1(x)) = \psi(f_2(x)), \quad \text{αλλά} \quad f_1(x) \neq f_2(x).$$

Σημείωση. Θα δούμε παρακάτω (Πρόταση 4.25) ότι αν το R είναι άπειρο σώμα (για παράδειγμα $R = \mathbb{R}$ ή $R = \mathbb{C}$), τότε η ψ είναι $1-1$ (και στην περίπτωση αυτή μπορούμε να ταυτίζουμε πολυώνυμα με τις αντίστοιχες πολυωνυμικές συναρτήσεις, όπως κάναμε στο Γυμνάσιο).

4.2. Διαιρετότητα πολυωνύμων

Ορισμός 4.7. *Έστω R δακτύλιος με 1_R και $a(x), b(x) \in R[x]$. Θα λέμε ότι το $a(x)$ **διαιρεί** το $b(x)$ στο $R[x]$, αν υπάρχει $c(x) \in R[x]$ ώστε $b(x) = a(x)c(x)$. Στην περίπτωση αυτή θα χρησιμοποιούμε το συμβολισμός $a(x)|b(x)$.*

Πρόταση 4.8. *Έστω R μεταθετικός δακτύλιος με 1_R. Τότε ισχύουν τα ακόλουθα.*

(1) *Αν $f(x), a(x), b(x) \in R[x]$, με $f(x)|a(x)$ και $f(x)|b(x)$, τότε*
$$f(x)|a(x)g(x) + b(x)h(x),$$
για κάθε $g(x), h(x) \in R[x]$.

(2) *Αν $a(x), b(x), c(x) \in R[x]$ και $a(x)|b(x)$, $b(x)|c(x)$, τότε $a(x)|c(x)$.*

(3) *Αν R περιοχή και $a(x), b(x) \in R[x]$ με $a(x)|b(x)$, τότε $\deg a(x) \leq \deg b(x)$ ή $b(x) = 0$.*

(4) *Αν R περιοχή και $a(x), b(x) \in R[x]$ με $a(x)|b(x)$ και $b(x)|a(x)$, τότε υπάρχει $u \in U(R)$ ώστε $b(x) = ua(x)$.*

Απόδειξη. Τα (1), (2), (3) έπονται άμεσα (το (3) έπεται από την ιδιότητα (2) της Πρότασης 4.5).

(4) Αφού $a(x)|b(x)$ και $b(x)|a(x)$ υπάρχουν $c(x), d(x) \in R[x]$, ώστε
$$b(x) = c(x)a(x) \quad \text{και} \quad a(x) = d(x)b(x).$$
Τότε $b(x) = c(x)d(x)b(x)$. Έστω $b(x) \neq 0$. Επειδή ο R είναι περιοχή, ο $R[x]$ είναι περιοχή, άρα $1 = c(x)d(x)$, δηλαδή $c(x) \in U(R[x])$. Τότε από την ιδιότητα (3) της Πρότασης 4.5 έπεται $c(x) = u \in U(R)$. Αν $b(x) = 0$, αφού $b(x)|a(x)$, έπεται $a(x) = 0$ και το ζητούμενο έπεται. □

Ορισμός 4.9. *Έστω R μεταθετικός δακτύλιος με 1_R. Ένα $p(x) \in R[x]$ θα λέγεται **ανάγωγο** αν $\deg p(x) \geq 1$ και δεν υπάρχουν $a(x), b(x) \in R[x]$ ώστε*
$$p(x) = a(x)b(x) \quad \text{με} \quad \deg a(x) \geq 1,\ \deg b(x) \geq 1.$$

Παρατήρηση. Στην ειδική περίπτωση που ο δακτύλιος R είναι περιοχή, παρατηρούμε ότι ένα $p(x) \in R[x]$ θετικού βαθμού είναι ανάγωγο αν και μόνο αν δεν υπάρχουν $a(x), b(x) \in R[x]$ ώστε
$$p(x) = a(x)b(x) \quad \text{με} \quad \deg a(x) < \deg p(x) \text{ και } \deg b(x) < \deg p(x).$$

Πράγματι, αυτό έπεται άμεσα από τον προηγούμενο ορισμό και το γεγονός ότι όταν ο R είναι περιοχή έχουμε τη σχέση $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$ σύμφωνα με την Πρόταση 4.5(2).

Παραδείγματα 4.10.

(1) Αν R περιοχή, τότε κάθε $p(x) \in R[x]$ με $\deg p(x) = 1$ είναι ανάγωγο στον $R[x]$ (έπεται από τον ορισμό και από την ιδιότητα (2) της Πρόταση 4.5).

(2) Το $2x \in \mathbb{Z}_4[x]$ δεν είναι ανάγωγο στο $\mathbb{Z}_4[x]$ αφού $2x = 2x(2x+1)$.

(3) Το $5x+1 \in \mathbb{Z}_6[x]$ δεν είναι ανάγωγο στο $\mathbb{Z}_6[x]$ αφού $5x+1 = (2x+1)(3x+1)$.

(4) Το $x^2+1 \in \mathbb{R}[x]$ είναι ανάγωγο στο $\mathbb{R}[x]$, αλλά το $x^2+1 \in \mathbb{C}[x]$ δεν είναι ανάγωγο στο $\mathbb{C}[x]$, αφού $x^2+1 = (x+i)(x-i)$.

(5) Το $x^4+x^2+1 \in \mathbb{Z}_2[x]$ δεν είναι ανάγωγο στο $\mathbb{Z}_2[x]$, αφού $(x^2+x+1)^2 = x^4+x^2+1$.

(6) Αν p πρώτος, τότε το $x^p+a \in \mathbb{Z}_p[x]$ δεν είναι ανάγωγο, αφού

$$x^p + a = x^p + a^p = (x+a)^p,$$

όπου στην πρώτη ισότητα χρησιμοποιήσαμε το μικρό θεώρημα του Fermat και στην δεύτερη ισότητα το Παράδειγμα 3.17(2) για $R = \mathbb{Z}_p[x]$.

Θεώρημα 4.11 (Ευκλείδεια διαίρεση για πολυώνυμα.)**.** *Έστω F σώμα και $f(x)$, $g(x) \in F(x)$ με $g(x) \neq 0$. Τότε υπάρχουν μοναδικά $q(x), r(x) \in F(x)$ ώστε*

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x).$$

Απόδειξη. Ύπαρξη. Έστω ότι $\deg f(x) < \deg g(x)$. Τότε $f(x) = 0 \cdot f(x) + f(x)$.

Έστω $\deg f(x) \geq \deg g(x)$. Έστω

$$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n, \text{ και}$$

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_m x^m, \quad g_m \neq 0.$$

Η απόδειξη θα γίνει με επαγωγή στο $\deg f(x)$. Αν $\deg f(x) = 0$, τότε

$$f(x) = f_0 = (f_0 g_0^{-1}) g_0 + 0.$$

Έστω ότι ισχύει η ύπαρξη για κάθε $f(x)$ με βαθμό $< n$. Έστω

$$h(x) = f(x) - f_n g_m^{-1} g(x) x^{n-m} \in F[x].$$

Στο $h(x)$ ο συντελεστής του x^n είναι

$$f_n - f_n g_m^{-1} g_m = f_n - f_n = 0.$$

Άρα $\deg h(x) < n$. Από την επαγωγική υπόθεση υπάρχουν $q_1(x), r_1(x) \in F[x]$ ώστε

$$h(x) = q_1(x)g(x) + r(x), \quad \deg r(x) < \deg g(x).$$

Άρα $f(x) = (f_n g_m^{-1} x^{n-m}) g(x) + r(x)$.

Μοναδικότητα. Έστω

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x), \text{ και}$$

$$f(x) = q_1(x)g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x).$$

Τότε $(q(x) - q_1(x))g(x) = r_1(x) - r(x)$. Αν $q(x) - q_1(x) \neq 0$, τότε

$$\deg(r_1(x) - r(x)) = \deg(q(x) - q_1(x)) + \deg g(x) \geq \deg g(x),$$

το οποίο είναι άτοπο γιατί $\deg r(x) < \deg g(x)$ και $\deg r_1(x) < \deg g(x)$. □

Παράδειγμα 4.12. Έστω $f(x), g(x) \in \mathbb{Z}_5[x]$ με $f(x) = x^4+4x^2+x+1$ και $g(x) = 2x^2+1$. Παρατηρούμε ότι στο $\mathbb{Z}_5$ έχουμε $2^{-1} = 3$, αφού $2 \cdot 3 = 6$ στο $\mathbb{Z}_5$. Τότε από την Ευκλείδεια διαίρεση παίρνουμε

$$f(x) = (3x^2+3)g(x) + x - 2.$$

Οι αναλυτικές πράξεις της Ευκλείδειας διαίρεσης του παραδείγματος φαίνονται στο σχήμα:

$$\begin{array}{rr|l} x^4+4x^2+ & x+1 & 2x^2+1 \\ -6x^4-3x^2 & & \hline 3x^2+3 \\ \hline x^2+x+1 & & \\ -6x^2 & -3 & \\ \hline x-2 & & \end{array}$$

Ένα πολυώνυμο $f(x) \in R[x]$ ονομάζεται **μονικό** αν ο μεγιστοβάθμιος συντελεστής του είναι το 1. Παρατηρούμε ότι αν το F είναι σώμα και $f(x) \in F[x]$ είναι μη μηδενικό με μεγιστοβάθμιο συντελεστή $c \in F$, τότε το $c^{-1}f(x)$ είναι μονικό. Θα το λέμε το **αντίστοιχο** μονικό πολυώνυμο του $f(x)$. Για παράδειγμα, το αντίστοιχο μονικό πολυώνυμο του $3x+1 \in \mathbb{R}[x]$ είναι το $x+\frac{1}{3}$ και το αντίστοιχο μονικό πολυώνυμο του $3x+1 \in \mathbb{Z}_5[x]$ είναι το $3^{-1}(3x+1) = x+2$.

Ορισμός 4.13. *Έστω F σώμα και $f(x), g(x) \in F[x]$, όχι και τα δύο μηδέν. Ένα μονικό πολυώνυμο $d(x) \in F[x]$ ονομάζεται **μέγιστος κοινός διαιρέτης** των $f(x)$ και $g(x)$ αν ικανοποιεί τις επόμενες ιδιότητες.*

(1) *$d(x)|f(x)$ και $d(x)|g(x)$, και*
(2) *αν $c(x) \in F[x]$ με $c(x)|f(x)$ και $c(x)|g(x)$, τότε $c(x)|d(x)$.*

Θεώρημα 4.14. *Έστω $f(x), g(x) \in F(x)$ όχι και τα δύο μηδέν. Τότε υπάρχει μοναδικός μκδ των $f(x), g(x)$. Επιπλέον υπάρχουν $a(x), b(x) \in F[x]$ ώστε*

$$\text{μκδ}(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

Απόδειξη. Έστω

$$I = \{a(x)f(x) + b(x)g(x) : a(x), b(x) \in F[x]\}.$$

Τότε το I περιέχει πολυώνυμα βαθμού ≥ 0 (αφού $f(x) \neq 0$ ή $g(x) \neq 0$). Έστω $d(x) \in I$ με ελάχιστο βαθμό και $d(x) \neq 0$. Τότε

$$d(x) = a(x)f(x) + b(x)g(x), \tag{4.1}$$

για κάποια $a(x), b(x) \in F[x]$.

Ισχυρισμός 1. $d(x)|f(x)$ και $d(x)|g(x)$. Πράγματι από την Ευκλείδεια διαίρεση υπάρχουν $q(x), r(x) \in F[x]$ ώστε $f(x) = q(x)d(x) + r(x)$, $\deg r(x) < \deg d(x)$. Επομένως

$$\begin{aligned} r(x) &= f(x) - q(x)(a(x)f(x) + b(x)g(x)) \\ &= (1 - q(x)a(x))f(x) + (-q(x)b(x))g(x) \in I. \end{aligned}$$

Αφού $r(x) \in I$ και $\deg r(x) < \deg d(x)$ έχουμε $r(x) = 0$. Άρα $d(x)|f(x)$. Ομοίως αποδεικνύεται ότι $d(x)|g(x)$.

Ισχυρισμός 2. Έστω $c(x)|f(x)$ και $c(x)|g(x)$. Τότε $c(x)|d(x)$. Πράγματι αφού $c(x)|f(x)$ και $c(x)|g(x)$ από τη (4.1) έπεται ότι $c(x)|d(x)$.

Καθώς $d(x) \neq 0$, θεωρούμε το αντίστοιχο μονικό πολυώνυμο, δηλαδή το το $d_n^{-1}d(x)$, όπου d_n ο μεγιστοβάθμιος συντελεστής του $d(x)$. Παρατηρούμε ότι το $d_n^{-1}d(x)$ είναι μονικό και ικανοποιεί τους δύο ισχυρισμούς που δείξαμε παραπάνω. Επομένως το $d_n^{-1}d(x)$ ικανοποιεί τις ιδιότητες (1) και (2) του Ορισμού 4.13. Επίσης

$$d_n^{-1}d(x) = (d_n^{-1}a(x))f(x) + (d_n^{-1}b(x))g(x).$$

Θα δείξουμε τώρα την μοναδικότητα. Έστω $d_1(x)$ και $d_2(x)$ δύο μονικά πολυώνυμα που ικανοποιούν τις ιδιότητες (1) και (2) του Ορισμού 4.13. Τότε επειδή $d_1(x)|f(x)$, $d_1(x)|f(x)$ και το $d_2(x)$ είναι μέγιστος κοινός διαιρέτης, από την ιδιότητα (2) του Ορισμού 4.13. έπεται ότι $d_1(x)|d_2(x)$. Ομοίως παίρνουμε ότι $d_2(x)|d_1(x)$. Επειδή F περιοχή, υπάρχει $u \in F$, $u \neq 0$ ώστε $d_2(x) = ud_1(x)$. Αφού τα $d_1(x), d_2(x)$ είναι μονικά πολυώνυμα, έχουμε $u = 1$. Έπεται $d_2(x) = d_1(x)$. □

Δύο πολυώνυμα $f(x), g(x) \in F[x]$ θα λέγονται **σχετικά πρώτα** αν

$$\mu\kappa\delta(f(x), g(x)) = 1.$$

Λήμμα 4.15. *Έστω F σώμα και $f(x), g(x), h(x) \in F[x]$.*
(1) *Αν $f(x), g(x)$ σχετικά πρώτα και $f(x)|g(x)h(x)$, τότε $f(x)|h(x)$.*
(2) *Αν το $f(x)$ είναι ανάγωγο, $f(x)|g(x)h(x)$ και $f(x) \not| g(x)$, τότε $f(x)|h(x)$.*
(3) *Αν $f(x), g(x)$ σχετικά πρώτα, $f(x)|h(x)$ και $g(x)|h(x)$, τότε $f(x)g(x)|h(x)$.*

Απόδειξη. (1) Από το Θεώρημα 4.14 υπάρχουν $a(x), b(x) \in F[x]$ ώστε $1 = a(x)f(x) + b(x)g(x)$. Άρα

$$h(x) = a(x)f(x)h(x) + b(x)g(x)h(x). \tag{4.2}$$

Από την υπόθεση έπεται ότι το $f(x)$ διαιρεί τους δύο προσθετέους στο δεξιό μέλος της (4.2) και επομένως διαιρεί το αριστερό.
(2) Έπεται άμεσα από το (1) καθώς από τις υποθέσεις του (2) έπεται ότι τα $f(x), g(x)$ είναι σχετικά πρώτα.
(3) Από την υπόθεση έπεται ότι το $f(x)g(x)$ διαιρεί τους δύο προσθετέους στο δεξιό μέλος της (4.2) και επομένως διαιρεί το αριστερό. □

Θεώρημα 4.16 (ανάλυση σε γινόμενο ανάγωγων)**.** *Έστω F σώμα και $f(x) \in F[x]$ θετικού βαθμού. Τότε υπάρχουν ανάγωγα $p_1(x), p_2(x), \ldots, p_n(x) \in F[x]$ ώστε*

$$f(x) = p_1(x)p_2(x)\cdots p_n(x).$$

Αν επιπλέον $f(x) = q_1(x)q_2(x)\cdots q_m(x)$, όπου $q_i(x) \in F[x]$ ανάγωγο, τότε $m = n$ και μετά ενδεχομένως από αναδιάταξη υπάρχουν $c_i \in F - 0$ με $q_i(x) = c_i p_i(x)$.

Απόδειξη. Έστω

$$M = \{f(x) \in F[x] : \deg f(x) \geq 1, \text{ το } f(x) \text{ δεν γράφεται ως γινόμενο ανάγωγων}\}.$$

Έστω $M \neq \emptyset$ και έστω $f(x) \in M$ ελαχίστου βαθμού. Παρατηρούμε ότι το $f(x)$ δεν είναι ανάγωγο (αν ήταν, θα ήταν γινόμενο ανάγωγων κατά τετριμμένο τρόπο), άρα

$$f(x) = a(x)b(x), \ \ \deg a(x) \geq 1, \ \ \deg b(x) \geq 1.$$

Επειδή F περιοχή, $\deg f(x) = \deg a(x) + \deg b(x)$. Επομένως $\deg a(x), \deg b(x) < \deg f(x)$, οπότε $a(x), b(x) \notin M$. Επειδή τα $a(x), b(x)$ είναι θετικού βαθμού και $a(x), b(x) \notin M$, έπεται ότι και τα $a(x)$ και $b(x)$ είναι γινόμενο ανάγωγων. Άρα το ίδιο συμβαίνει και με το $f(x) = a(x)b(x)$, που είναι άτοπο.

Ας δείξουμε τώρα την μοναδικότητα. Με τον συμβολισμό της εκφώνησης έχουμε,

$$p_1(x)p_2(x)\cdots p_n(x) = q_1(x)q_2(x)\cdots q_m(x). \tag{4.3}$$

Υποθέτουμε ότι $n \geq m$ και εφαρμόζουμε επαγωγή στο n. Τότε από την (4.3) και από το Λήμμα 4.15, έπεται ότι $p_1(x)|q_j(x)$ για κάποιο j (αφού $p_1(x)$ ανάγωγο). Έστω $p_1(x)|q_1(x)$. Αφού το $q_1(x)$ είναι ανάγωγο και $\deg p_1(x) \geq 1$, υπάρχει $c_i \in F \setminus \{0\}$ ώστε $q_1(x) = c_1 p_1(x)$. Επομένως $p_1(x)p_2(x)\cdots p_n(x) = c_1 p_1(x)q_2(x)\cdots q_m(x)$. Άρα $p_2(x)\cdots p_n(x) = c_1 q_2(x)\cdots q_m(x)$. Εφαρμόζοντας την επαγωγική υπόθεση παίρνουμε το ζητούμενο. □

Έστω F σώμα και $p(x) \in F[x]$. Από τον Ορισμό 4.7 και την Πρόταση 4.5(2) προκύπτει άμεσα ότι το $p(x)$ είναι ανάγωγο αν και μόνο αν το αντίστοιχο μονικό πολυώνυμο είναι ανάγωγο. Συνεπώς το Θεώρημα 4.16 λέει ότι για κάθε $f(x) \in F[x]$ θετικού βαθμού, όπου F σώμα, υπάρχουν μοναδικά (χωρίς να λαμβάνεται υπόψη η σειρά) μονικά ανάγωγα $p_1(x), p_2(x), \ldots, p_n(x) \in F[x]$ και μοναδικό $c \in F$ ώστε

$$f(x) = cp_1(x)p_2(x)\cdots p_n(x).$$

Θα καλούμε μια τέτοια παράσταση την **ανάλυση** του $f(x)$ σε γινόμενο μονικών ανάγωγων πολυωνύμων στο $F[x]$. Για παράδειγμα, η ανάλυση του $f(x) = 2x^2 + 2 \in F[x]$ σε γινόμενο μονικών ανάγωγων πολυωνύμων στο $F[x]$ είναι

- $2(x^2 + 1)$ αν $F = \mathbb{R}$,
- $2(x - i)(x + i)$ αν $F = \mathbb{C}$.

4.3. Ευκλείδειος αλγόριθμος πολυωνύμων

Έστω F σώμα. Ο Ευκλείδειος αλγόριθμος στο $F[x]$ χρησιμοποιείται για τον υπολογισμό του $\mu\kappa\delta$ δύο πολυωνύμων $f(x), g(x) \in F[x]$ και την εύρεση πολυωνύμων $a(x)$ και $b(x)$ ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$. Όπως στον αντίστοιχο αλγόριθμο του $\mathbb{Z}$, ο αλγόριθμος αυτός αποτελείται από διαδοχικές εφαρμογές του Ευκλείδειας διαίρεσης στο $F[x]$ και της ακόλουθης παρατήρησης: αν στο $F[x]$ ισχύει $f(x) = q(x)g(x) + r(x)$, τότε $\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), r(x))$ (γιατί;).

Έστω $f(x), g(x) \in F[x]$ με $g(x) \neq 0$. Από την Ευκλείδεια διαίρεση έχουμε διαδοχικά

$$\begin{aligned}
f(x) &= q_0(x)g(x) + r_0(x), && \deg r_0(x) < \deg g(x)\\
g(x) &= q_1(x)r_0(x) + r_1(x), && \deg r_1(x) < \deg r_0(x)\\
r_0(x) &= q_2(x)r_1(x) + r_2(x), && \deg r_2(x) < \deg r_1(x)\\
&\cdots\cdots\cdots\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x), && \deg r_n(x) < \deg r_{n-1}(x)\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x) + 0,
\end{aligned}$$

Μετά από πεπερασμένο πλήθος βημάτων θα βρούμε υπόλοιπο που είναι ίσο με μηδέν, $r_{n+1}(x) = 0$, γιατί η ακολουθία των φυσικών αριθμών

$$\deg g(x) > \deg r_0(x) > \deg r_1(x) > \deg r_2(x) > \dots$$

είναι γνήσια φθίνουσα. Υποθέτουμε ότι το $r_{n+1}(x)$ είναι το πρώτο υπόλοιπο που είναι ίσο με μηδέν. Εφαρμόζοντας διαδοχικά την παρατήρηση που επισημάναμε πριν, παίρνουμε

$$\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), r_0(x)) = \mu\kappa\delta(r_0(x), r_1(x)) = \cdots = \mu\kappa\delta(r_n(x), 0).$$

Αν s είναι ο μεγιστοβάθμιος όρος του (μη μηδενικού πολυωνύμου) $r_n(x)$, τότε είναι φανερό ότι

$$\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(r_n(x), 0) = s^{-1}r_n(x).$$

Τα $a(x), b(x)$ προσδιορίζονται με διαδοχικές αντικαταστάσεις ξεκινώντας από την προτελευταία ισότητα, την (n), και εφαρμόζοντας την παρακάτω διαδικασία. Γράφουμε τις παραπάνω ισότητες ως εξής

$$\begin{aligned}
r_0(x) &= f(x) - q_0(x)g(x) && (0')\\
r_1(x) &= g(x) - q_1(x)r_0(x) && (1')\\
r_2(x) &= r_0(x) - q_2(x)r_1(x) && (2')\\
&\cdots\cdots\cdots\\
r_{n-1}(x) &= r_{n-3}(x) - q_{n-1}(x)r_{n-2}(x) && (n-1')\\
r_n(x) &= r_{n-2}(x) - q_n(x)r_{n-1}(x). && (n')
\end{aligned}$$

Αντικαθιστούμε τώρα το $r_{n-1}(x)$ από την $(n-1)'$ στην $(n)'$. Λαμβάνουμε έτσι μια παράσταση της μορφής

$$r_n(x) = a_{n-3}(x)r_{n-3}(x) + b_{n-2}(x)r_{n-2}(x).$$

Στην ισότητα αυτή αντικαθιστούμε το $r_{n-3}(x)$ από την ισότητα $(n-2)'$, κοκ. Στο τέλος θα προκύψει μια παράσταση της μορφής

$$r_n(x) = A(x)f(x) + B(x)g(x).$$

Αν s είναι ο μεγιστοβάθμιος συντελεστής του $r_n(x)$ έχουμε

$$s^{-1}r_n(x) = s^{-1}A(x)f(x) + s^{-1}B(x)g(x)$$

οπότε μπορούμε να θέσουμε $a(x) = s^{-1}A(x)$ και $b(x) = s^{-1}B(x)$.

Παράδειγμα 4.17. Έστω $f(x), g(x) \in \mathbb{Z}_7[x]$ όπου

$$f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 \text{ και } g(x) = 3x^3 + 5x^2 + 6x.$$

Θα υπολογίσουμε τον $\mu\kappa\delta(f(x), g(x))$, χρησιμοποιώντας τον Ευκλείδειο αλγόριθμο, και θα προσδιορίσουμε πολυώνυμα $a(x)$ και $b(x)$ τέτοια ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x) + b(x)g(x)$. Με διαδοχικές Ευκλείδειες διαιρέσεις βρίσκουμε τα εξής

$$\begin{aligned} f(x) &= (6x)g(x) + 5x^2 + 4x + 5 \\ g(x) &= (2x + 5)(5x^2 + 4x + 5) + 4x + 3 \\ 5x^2 + 4x + 5 &= (3x + 4)(4x + 3) + 0. \end{aligned}$$

Το τελευταίο μη μηδενικό υπόλοιπο είναι το $4x + 3$. Το αντίστροφο του 4 στο $\mathbb{Z}_7$ είναι το 2. Άρα

$$\mu\kappa\delta(f(x), g(x)) = 2(4x + 3) = x + 6.$$

Για να προσδιορίσουμε πολυώνυμα $a(x)$ και $b(x)$, ώστε $\mu\kappa\delta(f(x), g(x)) = a(x)f(x)+b(x)g(x)$, γράφουμε την προτελευταία ισότητα ως

$$4x + 3 = g(x) - (2x + 5)(5x^2 + 4x + 5)$$

και αντικαθιστούμε το $5x^2 + 4x + 5$ από την πρώτη,

$$4x + 3 = g(x) - (2x + 5)(f(x) - (6x)g(x)).$$

Μετά από πράξεις βρίσκουμε

$$4x + 3 = (5x + 2)f(x) + (5x^2 + 2x + 1)g(x).$$

Πολλαπλασιάζοντας με το αντίστροφο του 4 στο $\mathbb{Z}_7$, δηλαδή το 2, έχουμε

$$x + 6 = (3x + 4)f(x) + (3x^2 + 4x + 2)g(x),$$

οπότε μπορούμε να θέσουμε $a(x) = 3x + 4$ και $b(x) = 3x^2 + 4x + 2$.

4.4. Ρίζες πολυωνύμων

Ορισμός 4.18. *Έστω R μεταθετικός δακτύλιος με 1_R και έστω $f(x) \in R[x]$. Ένα $r \in R$ λέγεται **ρίζα** του $f(x)$ στο R αν $f(r) = 0_R$.*

Πρόταση 4.19. *Έστω F σώμα και $a \in F$. Τότε το υπόλοιπο της διαίρεσης του $f(x) \in F[x]$ με το $x - a$ είναι ίσο με $f(a)$ και*

$$x - a | f(x) \Leftrightarrow f(a) = 0_F.$$

Απόδειξη. Από την Ευκλείδεια διαίρεση έχουμε,

$$f(x) = q(x)(x - a) + r(x), \ \ \deg r(x) < \deg(x - a) = 1.$$

Άρα $r(x) = c \in F$. Έχουμε (βλ. το εδάφιο 'πολυωνυμικές συναρτήσεις' στην παράγραφο 4.1)

$$f(a) = q(a)0_F + r(a).$$

Επομένως το υπόλοιπο είναι $r(x) = f(a)$.

Έχουμε λοιπόν ότι $f(x) = q(x)(x - a) + f(a)$. Αν $x - a | f(x)$, τότε $x - a | f(a)$. Από την Πρόταση 4.7(3), έπεται ότι $f(a) = 0_F$. Αντίστροφα, αν $f(a) = 0_F$, τότε $f(x) = q(x)(x - a)$ και άρα $x - a | f(x)$. □

Σημειώνουμε ότι κάθε πολυώνυμο $f(x) \in F[x]$ βαθμού 1, όπου F σώμα, έχει ρίζα στο F. Πράγματι, καθώς είναι της μορφής $f(x) = ax + b, a \neq 0_F$, ισχύει ότι $f(r) = 0_F$, όπου $r = -a^{-1}b$. Αν το F δεν είναι σώμα, η προηγούμενη ιδιότητα δεν ισχύει γενικά. Για παράδειγμα, το $f(x) = 2x - 1 \in \mathbb{Z}[x]$ δεν έχει ρίζα στο $\mathbb{Z}$.

Πρόταση 4.20. *Έστω F σώμα και $f(x) \in F[x]$ βαθμού τουλάχιστον 2.*

(1) *Αν το $f(x) \in F[x]$ είναι ανάγωγο, τότε δεν έχει ρίζα στο F.*
(2) *Αν $\deg f(x) = 2, 3$ και το $f(x)$ δεν έχει ρίζα στο F, τότε το $f(x)$ είναι ανάγωγο στο $F[x]$.*

Απόδειξη. (1) Έστω $f(x) \in F[x]$ με $\deg f(x) \geq 2$. Αν το $a \in F$ είναι ρίζα του $f(x)$, τότε από την Πρόταση 4.19 υπάρχει $b(x) \in F[x]$ με $f(x) = (x - a)b(x)$. Από την Πρόταση 4.5(2) και το γεγονός ότι κάθε σώμα είναι περιοχή, έπεται ότι $\deg b(x) \geq 1$.

(2) Έστω $\deg f(x) = 2$ ή 3 και έστω ότι το $f(x)$ δεν έχει ρίζα στο F. Αν το $f(x)$ δεν είναι ανάγωγο, τότε υπάρχουν $a(x)$, $b(x) \in F[x]$ θετικού βαθμού ώστε

$$f(x) = a(x)b(x).$$

Από την Πρόταση 4.5(2), $\deg a(x) + \deg b(x) = \deg f(x) = 2 \quad$ ή $\quad 3$, και άρα $\deg a(x) = 1$ ή $\deg b(x) = 1$. Καθώς το F είναι σώμα συμπεραίνουμε ότι τουλάχιστον ένα από τα $a(x), b(x)$ έχει ρίζα στο F. Άρα το $f(x)$ έχει ρίζα στο F, άτοπο. □

Πρόταση 4.21. *Έστω F σώμα και $f(x) \in F[x]$ με $\deg f(x) = n \geq 1$. Τότε το $f(x)$ έχει το πολύ n ρίζες στο F.*

Απόδειξη. Επαγωγή στο n. Αν $n = 1$, τότε $f(x) = ax + b, a \neq 0$. Επειδή το F είναι σώμα, το a είναι αντιστρέψιμο οπότε αν $ar + b = 0$, όπου $r \in F$, παίρνουμε $ar = -b \Rightarrow r = -a^{-1}b$. Συνεπώς το $f(x)$ έχει μοναδική ρίζα στο F.

Έστω ότι $n > 1$. Αν το $f(x)$ δεν έχει ρίζα στο F, τότε δεν υπάρχει κάτι να αποδειχθεί. Έστω $r \in F$ ρίζα του $f(x)$. Από την Πρόταση 4.19 έχουμε $f(x) = (x - r)g(x)$ για κάποιο $g(x) \in F[x]$. Λόγω της Πρότασης 4.5(2) και του γεγονότος ότι το F είναι περιοχή, το $g(x)$ έχει βαθμό $n - 1$. Από την επαγωγική υπόθεση, το $g(x)$ έχει το πολύ $n - 1$ ρίζες στο F. Από την ισότητα $f(x) = (x - r)g(x)$ και το γεγονός ότι το F είναι περιοχή έπεται ότι κάθε ρίζα του $f(x)$ στο F είναι το r ή ρίζα του $g(x)$. Κατά συνέπεια το $f(x)$ έχει το πολύ $1 + n - 1 = n$ ρίζες. □

Παραδείγματα 4.22.

(1) Με πράξεις επαληθεύεται ότι κάθε στοιχείο του $\mathbb{Z}_6$ είναι ρίζα του $f(x) = x^3 - x \in \mathbb{Z}_6[x]$. Δηλαδή το $f(x)$ έχει 6 ρίζες στο $\mathbb{Z}_6$. Άρα το συμπέρασμα της Πρότασης 4.21 δεν αληθεύει για τυχαίο R στην θέση του σώματος F.

(2) Βρείτε τις αναλύσεις των $f(x) = x^3 + x + 1 \in \mathbb{Z}_3[x]$ και $g(x) = x^9 + x^3 + 1 \in \mathbb{Z}_3[x]$ σε γινόμενο μονικών ανάγωγων

Παρατηρούμε ότι $f(1) = 1 + 1 + 1 = 3 = 0$ στο $\mathbb{Z}_3[x]$. Τότε από την Πρόταση 4.19 ισχύει ότι $x - 1 | f(x)$. Από την Ευκλείδεια διαίρεση έχουμε,

$$f(x) = (x - 1)(x^2 + x + 2),$$

όπου το $x - 1$ είναι ανάγωγο. Το $x^2 + x + 2 \in \mathbb{Z}_3[x]$ είναι βαθμού 2 και δεν έχει ρίζα στο $\mathbb{Z}_3$, οπότε από την Πρόταση 2.18 έπεται ότι και το $x^2 + x + 2$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$.

Για το $g(x)$ παρατηρούμε ότι

$$g(x) = (x^3)^3 + x^3 + 1 = (x^3 + x + 1)^3 = (f(x))^3.$$

σύμφωνα με το Παράδειγμα 4.2. Άρα η ζητούμενη ανάλυση είναι

$$g(x) = (x-1)^3(x^2+x+2)^3.$$

(3) Βρείτε την ανάλυση του $x^p + a \in \mathbb{Z}_p[x]$ σε γινόμενο μονικών ανάγωγων
Στο Παράδειγμα 4.10(6) είδαμε ότι $x^p + a = (x+a)^p$.

(4) (**Κριτήριο του Euler**) Ένας ακέραιος a λέγεται **τετραγωνικό υπόλοιπο** $\bmod n$ αν υπάρχει ακέραιος x με $a \equiv x^2 \mod n$. Έστω $p > 2$ πρώτος. Θα δείξουμε ότι ένας ακέραιος a σχετικά πρώτος με το p είναι τετραγωνικό υπόλοιπο $\bmod p$ αν και μόνο αν

$$a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

Πράγματι, έστω $q = \frac{p-1}{2}$. Θεωρούμε τα εξής υποσύνολα του $\mathbb{Z}_p$,

$$S = \{b \in \mathbb{Z}_p - \{0\} | b = x^2 \text{ για κάποιο } x \in \mathbb{Z}_p\}, \text{ και}$$
$$T = \{b \in \mathbb{Z}_p | b^q = 1\}.$$

Θα δείξουμε ότι $S = T$. Παρατηρούμε τα εξής:

- Ισχύει $S \subseteq T$. Πράγματι, αν $s \in S$, τότε $s = x^2$ για κάποιο μη μηδενικό $x \in \mathbb{Z}_p$, οπότε από το μικρό θεώρημα του Fermat παίρνουμε $s^q = x^{2q} = x^{p-1} = 1$.
- Τα στοιχεία $[1^2], [2^2], \ldots, [q^2]$ του S είναι διακεκριμένα.
Πράγματι, αν $[i^2] = [j^2]$ τότε $[i-j][i+j] = [0]$ και επειδή ο $\mathbb{Z}_p$ είναι περιοχή παίρνουμε $[i-j] = [0]$ ή $[i+j] = [0]$. Όμως δεν είναι δυνατό να ισχύει η τελευταία ισότητα, αφού το $[i+j]$ ανήκει στο σύνολο $\{[2], [3], \ldots, [2q] = [p-1]\}$ που δεν περιέχει το $[0]$.
- Το σύνολο T περιέχει το πολύ q στοιχεία.
Αυτό έπεται από την Πρόταση 4.21, γιατί κάθε στοιχείο του T είναι ρίζα του πολυωνύμου $x^q - 1 \in \mathbb{Z}_p[x]$ που έχει συντελεστές σε σώμα

Άρα $S = T$.

4.5. Το πολυώνυμο $x^p - x$

Έστω p πρώτος. Ξέρουμε ότι ο δακτύλιος $\mathbb{Z}_p$ είναι σώμα. Εδώ θα θεωρήσουμε το πολυώνυμο $x^p - x \in \mathbb{Z}_p[x]$ και θα δείξουμε ότι ισούται με το γινόμενο όλων των μονικών πρωτοβαθμίων πολυωνύμων του $\mathbb{Z}_p[x]$.

Πρόταση 4.23. *Έστω p πρώτος. Στο $\mathbb{Z}_p[x]$ έχουμε*

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Απόδειξη. Από το μικρό θεώρημα του Fermat έχουμε $a^p = a$ για κάθε $a \in \mathbb{Z}_p$. Συνεπώς από την Πρόταση 4.19, $x - a | x^p - x$ για κάθε $a \in \mathbb{Z}$. Επειδή τα $x, x-1, ..., x-(p-1)$ είναι ανά δύο σχετικά πρώτα, το Λήμμα 4.15(3) δίνει ότι

$$x(x-1)...(x-(p-1)) | x^p - x.$$

Επειδή τα δύο αυτά πολυώνυμα έχουν τον ίδιο βαθμό και το $\mathbb{Z}_p$ είναι σώμα, προκύπτει ότι υπάρχει $u \in \mathbb{Z}_p$ με $x^p - x = ux(x-1)...(x-(p-1))$. Συγκρίνοντας μεγιστοβάθμιους όρους στα δύο μέλη παίρνουμε $u = 1$. □

Πόρισμα 4.24 (θεώρημα του Wilson)**.** *Για κάθε πρώτο p,*

$$(p-1)! \equiv -1 \mod p.$$

Απόδειξη. Το ζητούμενο είναι σαφές όταν $p = 2$. Έστω λοιπόν p περιττός πρώτος. Συγκρίνοντας συντελεστές του x στην ισότητα της Πρότασης 4.23 παίρνουμε

$$-1 = (-1)(-2)\cdots(-(p-1))$$

στο $\mathbb{Z}_p$. Καθώς ο p είναι περιττός, έχουμε

$$(-1)(-2)\cdots(-(p-1)) = (-1)^{p-1}1\cdot 2\cdots(p-1) = 1\cdot 2\cdots(p-1).$$

Δηλαδή έχουμε $-1 = 1\cdot 2\cdots(p-1)$. Συνεπώς στο $\mathbb{Z}$ έχουμε $-1 \equiv (p-1)!\mod p$. □

Αναφερθήκαμε στις πολυωνυμικές συναρτήσεις στο τέλος της Παραγράφου 4.1. Θα εξετάσουμε τώρα το πρόβλημα πότε δύο πολυώνυμα ορίζουν την ίδια πολυωνυμική συνάρτηση, ελπίζοντας να κόψουμε την κακή παιδική συνήθεια που ίσως έχουμε από τα μαθητικά χρόνια μας να ταυτίζουμε ένα πολυώνυμο με την αντίστοιχη συνάρτηση.

Πρόταση 4.25. *Έστω F σώμα και $f(x), g(x) \in F[x]$.*

(1) *Έστω ότι το σύνολο F είναι άπειρο. Τότε*

$$f(a) = g(a)\ \forall a \in F \Leftrightarrow f(x) = g(x).$$

(2) *Έστω ότι $F = \mathbb{Z}_p$, όπου p πρώτος. Τότε*

$$f(a) = g(a)\ \forall a \in F \Leftrightarrow x^p - x | f(x) - g(x).$$

Απόδειξη. Θέτουμε $h(x) = f(x) - g(x)$.
(1) Αν $f(a) = g(a)\ \forall a \in F$, τότε το $h(x)$ έχει άπειρες ρίζες στο σώμα F και από την Πρόταση 4.21 έπεται ότι $h(x) = 0$. Η αντίστροφη συνεπαγωγή είναι σαφής.
(2) Αν $f(a) = g(a)\ \forall a \in \mathbb{Z}_p$, τότε ακριβώς όπως στην απόδειξη της Πρότασης 4.23 συμπεραίνουμε ότι $x(x-1)...(x-(p-1))|h(x)$. Από την Πρόταση 4.23, $x(x-1)...(x-(p-1)) = x^p - x$.

Αντίστροφα, αν $x^p - x | h(x)$, τότε υπάρχει $k(x) \in F[x]$ με $h(x) = (x^p - x)k(x)$. Από το μικρό θεώρημα του Fermat έχουμε $a^p - a = 0$ για κάθε $a \in \mathbb{Z}_p$ και επομένως $h(a) = 0$ για κάθε $a \in \mathbb{Z}_p$. □

4.6. Τα ανάγωγα πολυώνυμα στο $\mathbb{C}[x]$ και $\mathbb{R}[x]$

Αναφέρουμε χωρίς απόδειξη το ακόλουθο θεώρημα. Αποδείξεις μπορείτε να δείτε στα μαθήματα Θεωρία Galois και Μιγαδική Ανάλυση.

Θεώρημα 4.26 (Θεμελιώδες θεώρημα της Άλγεβρας)**.** *Κάθε $f(x) \in \mathbb{C}[x]$ θετικού βαθμού έχει τουλάχιστον μια ρίζα στο $\mathbb{C}$.*

Πόρισμα 4.27. *Έστω $f(x) \in \mathbb{C}[x]$ βαθμού $n > 0$. Τότε υπάρχουν $c, z_1, z_2, \ldots, z_n \in \mathbb{C}$ ώστε*

$$f(x) = c(x - z_1)(x - z_2)\cdots(x - z_n).$$

Απόδειξη. Με επαγωγή στο n (άσκηση.). □

Πόρισμα 4.28. *Τα ανάγωγα πολυώνυμα στο $\mathbb{C}[x]$ είναι ακριβώς τα πρωτοβάθμια πολυώνυμα.*

Στη συνέχεια θα προσδιορίσουμε τα ανάγωγα πολυώνυμα στο $\mathbb{R}[x]$.

Λήμμα 4.29. *Έστω $f(x), g(x) \in \mathbb{R}[x]$. Αν $f(x)|g(x)$ στο $\mathbb{C}[x]$, τότε $f(x)|g(x)$ στο $\mathbb{R}[x]$.*

Απόδειξη. Έστω $f(x)|g(x)$ στο $\mathbb{C}[x]$. Τότε υπάρχει $h(x) \in \mathbb{C}[x]$ ώστε $g(x) = h(x)f(x)$. Από την Ευκλείδεια διαίρεση στο $\mathbb{R}[x]$ υπάρχουν μοναδικά $q(x), r(x) \in \mathbb{R}[x]$ με

$$g(x) = q(x)f(x) + r(x), \quad \deg r(x) < \deg f(x).$$

Από τη μοναδικότητα και τις δύο τελευταίες ισότητες έπεται ότι $h(x) = q(x) \in \mathbb{R}[x]$. □

Ο **συζυγής** του μιγαδικού αριθμού $z = a+bi$, όπου $a, b \in \mathbb{R}$, είναι $\overline{z} = a-bi$. Θυμίζουμε ότι αν $z_1, z_2 \in \mathbb{C}$, τότε ισχύουν τα ακόλουθα.

(1) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.

(2) $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$.

Χρησιμοποιώντας τις σχέσεις αυτές εύκολα επαληθεύεται ότι αν $f(x) \in \mathbb{R}[x]$, τότε $\overline{f(z)} = f(\overline{z})$ για κάθε $z \in \mathbb{C}$.

Λήμμα 4.30. *Έστω $f(x) \in \mathbb{R}[x]$. Αν το $z \in \mathbb{C}$ είναι ρίζα του $f(x)$ τότε το $\overline{z} \in \mathbb{C}$ είναι ρίζα του $f(x)$.*

Απόδειξη. Έστω $f(z) = 0$. Τότε $0 = \overline{f(z)} = f(\overline{z})$. □

Πόρισμα 4.31. *Κάθε $f(x) \in \mathbb{R}[x]$ περιττού βαθμού έχει τουλάχιστον μια πραγματική ρίζα.*

Θεώρημα 4.32. *Ένα $f(x) \in \mathbb{R}[x]$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν*

(1) $\deg f(x) = 1$, *ή*

(2) $f(x) = ax^2 + bx + c$, *με* $\Delta = b^2 - 4ac < 0$.

Απόδειξη. Έστω $f(x) = ax^2+bx+c \in \mathbb{R}[x]$. Από την Πρόταση 4.20, το $f(x)$ είναι ανάγωγο στο $\mathbb{R}[x]$ αν και μόνο αν δεν έχει πραγματική ρίζα, δηλαδή αν και μόνο αν $\Delta = b^2 - 4ac < 0$.

Έστω τώρα $f(x) \in \mathbb{R}[x]$ με $\deg f(x) \geq 3$. Θα δείξουμε ότι το $f(x)$ δεν είναι ανάγωγο. Από το Πόρισμα 4.27 και το Λήμμα 4.30,

$$f(x) = c(x-\varrho_1)\cdots(x-\varrho_k)(x-z_1)\cdots(x-z_m)(x-\overline{z}_1)\cdots(x-\overline{z}_m),$$

όπου $\varrho_1, \ldots, \varrho_k \in \mathbb{R}$, $z_1, \ldots, z_m \in \mathbb{C} \setminus \mathbb{R}$, $c \in \mathbb{C}$. Παρατηρούμε ότι

$$(x-z_i)(x-\overline{z}_i) = x^2 - (z_i + \overline{z}_i)x + z_i\overline{z}_i \in \mathbb{R}[x],$$

αφού $z_i + \overline{z}_i \in \mathbb{R}$ και $z_i\overline{z}_i \in \mathbb{R}$. Επομένως $x^2 - (z_i + \overline{z}_i) + z_i\overline{z}_i | f(x)$, στο $\mathbb{C}[x]$, όπου $x^2 - (z_i + \overline{z}_i) + z_i\overline{z}_i \in \mathbb{R}[x]$ και $f(x) \in \mathbb{R}[x]$. Από το Λήμμα 4.30 έπεται ότι $x^2 - (z_i + \overline{z}_i) + z_i\overline{z}_i | f(x)$ στο $\mathbb{R}[x]$. Άρα το $f(x)$ δεν είναι ανάγωγο στο $\mathbb{R}[x]$. □

Παράδειγμα 4.33. Έστω $n \in \mathbb{Z}_{>0}$. Δείξτε ότι

$$x^2 + x + 1 | (x+1)^n + x^n + 1 \ \text{ στο } \ \mathbb{R}[x] \ \Leftrightarrow \ n = 2 \ \text{ή} \ 4 \mod 6.$$

Θα δείξουμε πρώτα τον εξής ισχυρισμό.

$$x^2 + x + 1 | f(x) \ \text{ στο } \ \mathbb{R}[x] \ \Leftrightarrow \ f(a) = 0,$$

όπου $f(x) = (x+1)^n + x^n + 1$ και το a είναι ρίζα του $x^2 + x + 1$.

Πράγματι, έστω $f(a) = 0$. Από το Λήμμα 4.25, $f(\overline{a}) = 0$. Επομένως

$$x - a | f(x) \quad \text{και} \quad x - \overline{a} | f(x)$$

στο $\mathbb{C}[x]$. Επειδή $a \neq \overline{a}$, τα πολυώνυμα $x-a, x-\overline{a}$ είναι σχετικά πρώτα και επομένως έχουμε $(x-a)(x-\overline{a}) | f(x)$. Δηλαδή, $x^2 + x + 1 | f(x)$ στο $\mathbb{C}[x]$. Από το Λήμμα 4.29, έχουμε ότι $x^2 + x + 1 | f(x)$ στο $\mathbb{R}[x]$. Το αντίστροφο είναι σαφές.

Θα δείξουμε τώρα το ζητούμενο. Υπολογίζουμε πότε ισχύει $f(a) = 0$. Έχουμε

$$f(a) = (a+1)^n + a^n + 1 = (-1)^n a^{2n} + a^n + 1.$$

Από $a^2 + a + 1 = 0$ έπεται ότι $a^3 = 1$. Διακρίνουμε τις ακόλουθες περιπτώσεις.

(1) Έστω $n = 6k,\ k \in \mathbb{Z}_{>0}$. Τότε
$$f(a) = (a^3)^{4k} + (a^3)^{2k} + 1 = 1 + 1 + 1 = 3 \neq 0.$$
(2) Έστω $n = 6k+1,\ k \in \mathbb{Z}_{>0}$. Τότε
$$f(a) = -(a^3)^4 k \cdot a^2 + (a^3)^{2k} \cdot a + 1 = -a^2 + a + 1 = 2a + 2 \neq 0.$$
(3) Έστω $n = 6k+2,\ k \in \mathbb{Z}_{>0}$. Τότε
$$f(a) = (a^3)^{4k+1} \cdot a + (a^3)^{2k} \cdot a^2 + 1 = a + a^2 + 1 = 0.$$
(4) Έστω $n = 6k+3,\ k \in \mathbb{Z}_{>0}$. Τότε όπως πριν, $f(a) = 1 \neq 0$.
(5) Έστω $n = 6k+4,\ k \in \mathbb{Z}_{>0}$. Τότε όπως πριν, $f(a) = 0$.
(6) Έστω $n = 6k+5,\ k \in \mathbb{Z}_{>0}$. Τότε όπως πριν, $f(a) = 2a^2 + 2 \neq 0$.

Τελικά $f(a) = 0$ αν και μόνο αν $n = 2$ ή $4 \mod 6$.

Ασκήσεις Κεφαλαίου 4

Ομάδα1: 1-3, 5-7, 17, 19.
Ομάδα2: 4, 8-10, 12-16, 21-25, 27, 28, 31.
Ομάδα3: 11, 18, 20, 26, 29, 30.

1. Δείξτε ότι $|U(\mathbb{Z}_3[x])| = 2$ και $|U(\mathbb{Z}_4[x])| = \infty$.
2. Βρείτε όλα τα $f(x) \in \mathbb{C}[x]$ τέτοια ώστε $f(x+2) - 2f(x+1) = f(x)$.
3. Βρείτε όλα τα μονικά ανάγωγα $p(x), q(x) \in \mathbb{Q}[x]$ με $(x^2-1)p(x)+(x+2)q(x) = p(x)q(x)$.
4. Έστω p πρώτος και $f(x), g(x) \in \mathbb{Z}_p[x]$, όπου $f(x) = x^4 + 2x^3 + 4x^2 + 8x + 9$, $g(x) = x^2 + 2x + 3$. Βρείτε το $\mu\kappa\delta(f(x), g(x))$ για τις διάφορες τιμές του p.
5. i) Βρείτε την ανάλυση του $x^3 + 6 \in \mathbb{Z}_7[x]$ σε γινόμενο ανάγωγων
   ii) Αληθεύει ότι υπάρχει πολυώνυμο στο $\mathbb{Q}[x]$ βαθμού 4 τέτοιο ώστε τα $1, 1+2i, 2+3i$ να είναι ρίζες του;
6. i) Έστω $f(x) = a_n x^n + ... + a_0 \in \mathbb{Z}[x]$. Δείξτε ότι αν ο ρητός αριθμός a/b, όπου a, b σχετικά πρώτοι ακέραιοι, είναι ρίζα του $f(x)$, τότε $a|a_0$ και $b|a_n$.
   ii) Δείξτε ότι το πολυώνυμο $f(x) = x^5 + 2x^3 + x + 3 \in \mathbb{Z}[x]$ δεν έχει ρητή ρίζα.
7. Βρείτε όλα τα $f(x) \in \mathbb{C}[x]$ με $f(x) = f(x-1)$.
8. Βρείτε όλα τα μονικά $f(x) \in \mathbb{C}[x]$ τέτοια ώστε $xf(x-1) = (x-2020)f(x)$.
9. Έστω F σώμα και m, n θετικοί ακέραιοι και $d = \mu\kappa\delta(m, n)$. Δείξτε ότι
$$\mu\kappa\delta(x^m - 1, x^n - 1) = x^d - 1.$$
10. Έστω πρώτος $p > 3$. Δείξτε ότι $\sum_{0<i<j<p} ij \equiv 0 \mod p$.
11. Δείξτε ότι το πολυώνυμο $(x-1)(x-2)\cdots(x-2020) - 1 \in \mathbb{Z}[x]$ είναι ανάγωγο.
12. Έστω p πρώτος. Δείξτε ότι το πλήθος των μονικών ανάγωγων πολυωνύμων του $\mathbb{Z}_p[x]$ βαθμού 2 ισούται με $\frac{p(p-1)}{2}$.
13. Βρείτε όλα τα ανάγωγα πολυώνυμα στο $\mathbb{Z}_2[x]$ βαθμού το πολύ 4. Στη συνέχεια δείξτε ότι ένα πολυώνυμο στο $\mathbb{Z}_2[x]$ βαθμού 5 είναι ανάγωγο αν και μόνο αν δεν έχει ρίζα στο $\mathbb{Z}_2$ και δεν διαιρείται με το $x^2 + x + 1$.
14. Έστω F σώμα.
   i) Δείξτε ότι υπάρχουν άπειρα το πλήθος ανάγωγα πολυώνυμα στο $F[x]$.
   ii) Έστω ότι το F είναι πεπερασμένο σώμα. Τότε για κάθε $n \in \mathbb{N}$ υπάρχει ανάγωγο πολυώνυμο του $F[x]$ βαθμού $\geq n$.
15. Έστω p πρώτος. Ποια απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p$ επάγει το $x^{p^n} - x \in \mathbb{Z}_p[x]$, $n \in \mathbb{N}$;
16. Βρείτε όλα τα μονικά πολυώνυμα $f(x) \in \mathbb{R}[x]$ βαθμού 3 ώστε $\mu\kappa\delta(f(x), x^2 + 1) \neq 1$ και $\mu\kappa\delta(f(x), x^2 - 3x + 2) \neq 1$.
17. Δίνεται ότι μια ρίζα του $f(x) = x^4 - x^3 + 4x^2 + 3x + 5 \in \mathbb{C}[x]$ είναι το $1 + 2i$. Βρείτε όλες τις ρίζες του $f(x)$ στο $\mathbb{C}$.
18. Έστω p πρώτος και $f(x) = x^p - x + 1_{\mathbb{Z}_p} \in \mathbb{Z}_p[x]$.
   i) Δείξτε ότι το $f(x)$ δεν έχει ρίζα στο $\mathbb{Z}_p$.
   ii) Έστω F σώμα που περιέχει το $\mathbb{Z}_p$ ως υποδακτύλιο.
      (i) Δείξτε ότι $1_F = 1_{\mathbb{Z}_p}$ και $pr = 0$ για κάθε $r \in F$.
      (ii) ≀ Δείξτε ότι αν το F περιέχει μια ρίζα του $f(x)$, τότε περιέχει p διακεκριμένες ρίζες του $f(x)$
19. Έστω $f(x), g(x) \in \mathbb{C}[x]$, με $f(x) = x(x^4-1)$ και $g(x) = x^9-1$. Βρείτε το $\mu\kappa\delta(g(x), f(x))$ και $a(x), b(x)$ ώστε $x^{2011} - 1 = a(x)f(x) + b(x)g(x)$.
20. Δείξτε ότι δεν υπάρχει $f(x) \in \mathbb{Z}[x]$ θετικού βαθμού ώστε για κάθε $m \in \mathbb{Z}$, το $f(m)$ να είναι πρώτος.

21. Βρείτε το υπόλοιπο της διαίρεσης του 98! με το 101.
22. Δείξτε ότι για κάθε σώμα F το πολυώνυμο $f(x) = 1 + x + x^4 + x^5 \in F[x]$ δεν είναι ανάγωγο.
23. Έστω p πρώτος. Βρείτε την ανάλυση του $f(x) = x^{p^2} - x^p \in \mathbb{Z}_p[x]$ σε γινόμενο μονικών ανάγωγων
24. Έστω p πρώτος και $f(x) = (x^2 + x + 1)^p - (x^2 + x + 1) \in \mathbb{Z}_p[x]$.
    i) Δείξτε ότι $x^p - x | f(x)$ στο $\mathbb{Z}_p[x]$.
    ii) Βρείτε την ανάλυση του $f(x) \in \mathbb{Z}_p[x]$ σε γινόμενο μονικών αναγώγων για $p = 2$ και $p = 3$.
25. Έστω k σώμα. Θεωρούμε την απεικόνιση
$$\psi : k[x] \to F(k, k), \;\; \psi(f(x)) = \overline{f},$$
όπου $F(k, k)$ ο δακτύλιος των απεικονίσεων $k \to k$ και $\overline{f}$ η πολυωνυμική συνάρτηση που επάγεται από το $f(x)$ (βλ. Παράγραφο 4.1). Δείξτε ότι η ψ είναι 1-1 αν και μόνο αν το σύνολο k είναι άπειρο.
26. Έστω p περιττός πρώτος a, b ακέραιοι με $1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b}$. Δείξτε ότι $p|a$.
27. Έστω R μεταθετικός δακτύλιος με μονάδα και $a \in R$. Δείξτε ότι το πολυώνυμο $1 - ax \in R[x]$ είναι αντιστρέψιμο στοιχείο του $R[x]$ αν και μόνο αν το στοιχείο a είναι μηδενοδύναμο.
28. Έστω R μεταθετικός δακτύλιος με μονάδα που δεν έχει μη μηδενικό μηδενοδύναμο στοιχείο. Έστω $f(x) = a_n x^n + ... + a_1 x + a_0 \in R[x]$ μηδενοδιαιρέτης. Δείξτε ότι υπάρχει μη μηδενικό $b \in R$ τέτοιο ώστε $ba_n = ... = ba_1 = ba_0 = 0$.
29. ≀ Λύστε την προηγούμενη άσκηση για τυχαίο μεταθετικό δακτύλιο με μονάδα.
30. Έστω $p > 2$ πρώτος και $q = \frac{p-1}{2}$. Δείξτε ότι στο $\mathbb{Z}_p[x]$ είναι
$$x^q - 1 = (x - 1^2)(x - 2^2)...(x - q^2).$$
31. Έστω k σώμα και $p(x) \in k[x]$ θετικού βαθμού.
    i) ($p(x)$-αδική παράσταση). Δείξτε ότι για κάθε $f(x) \in k[x]$ υπάρχουν μοναδικά $r_0(x), ..., r_m(x) \in k[x]$ με $f(x) = r_m(x)p(x)^m + ... + r_1(x)p(x) + r_0(x)$ και $\deg r_i(x) < \deg p(x)$.
    ii) (Ανάπτυγμα Taylor). Έστω $k = \mathbb{R}$ και $p(x) = x - a$. Δείξτε ότι $r_i = \dfrac{1}{i!} f^{(i)}(a)$, όπου $f^{(i)}(x)$ είναι η παράγωγος του $f(x)$ τάξης i.

Υποδείξεις Ασκήσεων Κεφαλαίου 4

1. *Λύση.* Η πρώτη ισότητα έπεται άμεσα από την Πρόταση 4.5 (3). Η δεύτερη ισότητα έπεται άμεσα από την παρατήρηση ότι για κάθε θετικό ακέραιο n, $(f_n(x))^2 = 1$, όπου $f_n(x) = 2x^n + 1 \in \mathbb{Z}_4[x]$.

2. *Υπόδειξη.* Θεωρήστε μεγιστοβάθμιους όρους για να δείξετε ότι $f(x) = 0$.

3. *Λύση.* Από την υπόθεση έπεται ότι $p(x)|(x+2)q(x)$ και επειδή το $p(x)$ είναι ανάγωγο παίρνουμε $p(x)|(x+2)$ ή $p(x)|q(x)$. Συνεπώς
$$p(x) = x + 2 \quad \eta \quad p(x) = q(x)$$
διότι το $p(x)$ είναι μονικό θετικού βαθμού και τα $x+2, q(x)$ ανάγωγα. Ο δακτύλιος $\mathbb{Q}[x]$ είναι περιοχή. Στην πρώτη περίπτωση παίρνουμε από την υπόθεση κατόπιν διαγραφής του $p(x) = x + 2$,
$$x^2 - 1 + q(x) = q(x) \Rightarrow x^2 - 1 = 0$$
που είναι αδύνατο, και στη δεύτερη παίρνουμε κατόπιν διαγραφής του $p(x) = q(x)$,
$$x^2 - 1 + x + 2 = q(x) \Rightarrow p(x) = q(x) = x^2 + x + 1.$$
Παρατηρούμε ότι πράγματι για $p(x) = q(x) = x^2 + x + 1$ επαληθεύεται ότι $(x^2-1)p(x) + (x+2)q(x) = p(x)q(x)$. Τέλος, το $x^2 + x + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο καθώς είναι δευτέρου βαθμού και δεν έχει ρίζα στο $\mathbb{Q}$. Άρα υπάρχει μοναδικό ζεύγος πολυωνύμων με τις ιδιότητες της εκφώνησης, $p(x) = q(x) = x^2 + x + 1$.

4. *Λύση.* Από την Ευκλείδεια διαίρεση στο $\mathbb{Z}_p[x]$ βρίσκουμε
$$f(x) = (x^2 + 1)g(x) + 6x + 6. \tag{4.0}$$
i) Έστω ότι $p = 2, 3$. Τότε το υπόλοιπο $6x + 6$ είναι 0 και επομένως
$$\mu\kappa\delta(f(x), g(x)) = g(x)$$
γιατί το $g(x)$ είναι μονικό.
ii) Έστω $p \neq 2, 3$. Τότε στο $\mathbb{Z}_p$ το 6 είναι αντιστρέψιμο. Από την ισότητα (4.0) έχουμε
$$\mu\kappa\delta(f(x), g(x)) = \mu\kappa\delta(g(x), 6x + 6) = \mu\kappa\delta(g(x), x + 1).$$
Το υπόλοιπο της διαίρεσης του $g(x)$ με το $x + 1$ είναι $g(-1) = 2 \neq 0$. Επειδή το $x + 1$ είναι ανάγωγο συμπεραίνουμε ότι $\mu\kappa\delta(g(x), x + 1) = 1$. Συνεπώς $\mu\kappa\delta(f(x), g(x)) = 1$.

5. *Απάντηση.* i)$(x-1)(x-2)(x-4)$. ii) Δεν αληθεύει διότι λόγω του Λήμματος 4.30 θα είχε τουλάχιστον 5 ρίζες στο σώμα $\mathbb{C}$ και $5 > 4$ που είναι άτοπο από την Πρόταση 4.21.

6. *Λύση.* i) Με απαλοιφή παρονομαστών στη σχέση $f(a/b) = 0$ προκύπτει ότι
$$a_n a^n + a_{n-1}a^{n-1}b + ... + a_1 ab^{n-1} + a_0 b^n = 0.$$
Άρα $a|a_0 b^n$ και $b|a_n a^n$. Επειδή οι a, b είναι σχετικά πρώτοι, παίρνουμε αντίστοιχα $a|a_0$ και $b|a_n$.

ii) Από το προηγούμενο υποερώτημα, οι υποψήφιες ρητές ρίζες του $f(x)$ είναι οι $1, -1, 3, -3$. Με πράξεις επαληθεύεται ότι καθένα από τα $f(1), f(-1), f(3), f(-3)$ είναι μη μηδενικό. Συνεπώς το $f(x)$ δεν έχει ρητή ρίζα.

7. *Λύση.* Έστω $f(x) \in \mathbb{C}[x]$ με $f(x) = f(x-1)$. Παρατηρούμε ότι αν το $a \in \mathbb{C}$ είναι ρίζα του $f(x)$, τότε και το $a + 1$ είναι ρίζα του $f(x)$. Επομένως επαγωγικά, το $a + n$ είναι ρίζα του $f(x)$ για κάθε $n \in \mathbb{N}$. Από την Πρόταση 4.21 έπεται ότι $f(x) = c \in \mathbb{C}$.

Αντίστροφα, είναι σαφές ότι κάθε πολυώνυμο της μορφής $f(x) = c \in \mathbb{C}$ ικανοποιεί την ιδιότητα $f(x) = f(x-1)$.

8. *Υπόδειξη.* Δείξτε ότι για κάθε $n = 0, 1, ..., 2019$, $x - n|f(x)$. Από το Λήμμα 4.15(1) έπεται ότι $x(x-1)...(x-2019)|f(x)$. Δείξτε ότι έχουμε ισότητα χρησιμοποιώντας την προηγούμενη άσκηση.

9. *Υπόδειξη.* Τροποποιείστε κατάλληλα τη λύση της άσκησης 1.12.
10. *Υπόδειξη.* Στην ισότητα της Πρότασης 4.23 θεωρήστε συντελεστές του x^{p-2}.
11. *Λύση.* Έστω $a(x), b(x) \in \mathbb{Z}[x]$ θετικού βαθμού με

$$(x-1)(x-2)\cdots(x-2020)-1 = a(x)b(x).$$

Έχουμε $\deg(a(x)b(x)) = 2020$ και επειδή το $\mathbb{Z}$ είναι περιοχή, έπεται ότι $\deg(a(x)b(x)) = \deg a(x) + \deg b(x)$. Συνεπώς $\deg a(x), \deg b(x) < 2020$. Για κάθε $n = 1, 2, \cdots, 2020$, έχουμε $-1 = a(n)b(n)$ και επειδή τα πολυώνυμα $a(x), b(x)$ έχουν ακέραιους συντελεστές, παίρνουμε ότι $(a(n), b(n)) = (1,-1), (-1,1)$ και επομένως $a(n) + b(n) = 0$. Επειδή

$$\deg(a(x)+b(x)) \leq max(\deg a(x), \deg b(x)) < 2020,$$

από την Πρόταση 4.21 έπεται ότι $a(x) + b(x) = 0$. Τότε

$$(x-1)(x-2)\cdots(x-2020)-1 = -a(x)^2.$$

Θεωρώντας μεγιστοβάθμιους όρους στην τελευταία σχέση βλέπουμε ότι αυτή είναι αδύνατη.

12. *Λύση.* Θεωρούμε τα εξής σύνολα.
    - Το σύνολο A όλων των μονικών πολυωνύμων του $\mathbb{Z}_p[x]$ βαθμού 2.
    - Το υποσύνολο B του A όλων των μη ανάγωγων πολυωνύμων του A.
    - Το υποσύνολο C του A όλων των ανάγωγων πολυωνύμων του A.

    Είναι σαφές ότι έχουμε την ξένη ένωση $A = B \cup C$ και επομένως

$$|C| = |A| - |B|.$$

Ισχύει $|A| = p^2$, γιατί κάθε στοιχείο του A γράφεται μοναδικά στη μορφή $x^2 + ax + b$, όπου $a, b \in \mathbb{Z}_p$, και $|\mathbb{Z}_p| = p$. Επειδή κάθε στοιχείο $f(x)$ του B είναι μη ανάγωγο πολυώνυμο βαθμού 2, από την Πρόταση 4.20(2) έπεται το $f(x)$ έχει ρίζα a στο $\mathbb{Z}_p$. Καθώς $\deg f(x) = 2$, από την Ευκλείδεια διαίρεση στο $\mathbb{Z}_p[x]$ συνάγουμε ότι $f(x) = (x-a)(x-b)$, όπου $b \in \mathbb{Z}_p$. Δηλαδή,

$$B = \{(x-a)(x-b) : a, b \in \mathbb{Z}_p\}.$$

Επειδή $(x-a)(x-b) = (x-b)(x-a)$, το πλήθος των στοιχείων του B ισούται με το πλήθος των επιλογών δύο στοιχείων χωρίς διάταξη και με επανατοποθέτηση από σύνολο p στοιχείων. Κατά συνέπεια $|B| = \frac{(p+1)p}{2}$. Τελικά,

$$|C| = p^2 - \frac{(p+1)p}{2} = \frac{p(p-1)}{2}.$$

13. *Απάντηση.* Τα ανάγωγα πολυώνυμα στο $\mathbb{Z}_2[x]$ βαθμού το πολύ 4 είναι τα εξής.
    - $x, x+1$,
    - $x^2 + x + 1$,
    - $x^3 + x^2 + 1, x^3 + x + 1$,
    - $x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + 1, x^4 + x + 1$.
14. *Λύση.* i) Η απόδειξη είναι παρόμοια με αυτήν της ύπαρξης άπειρων πρώτων στους ακεραίους (Θεώρημα 1.5) και αφήνεται ως άσκηση.

    ii) Υποθέτουμε ότι υπάρχει $n \in \mathbb{N}$ ώστε κάθε ανάγωγο πολυώνυμο του $F[x]$ να έχει βαθμό μικρότερο του n. Επειδή το F είναι πεπερασμένο σύνολο, το σύνολο

$$\{f(x) \in F[x] : \deg f(x) < n\}$$

είναι πεπερασμένο, άρα το $\{f(x) \in F[x] : f(x)$ ανάγωγο$\}$ είναι πεπερασμένο και ας υποθέσουμε ότι είναι το $\{p_1(x), p_2(x), \ldots, p_m(x)\}$. Θέτουμε

$$P(x) = p_1(x)p_2(x)\cdots p_m(x) + 1.$$

Τότε $\deg P(x) \geq 1$, οπότε το $P(x)$ έχει έναν ανάγωγο διαιρέτη, δηλαδή $P_i(x)|P(x)$ για κάποιο i. Επομένως $p_i(x)|1$, το οποίο είναι άτοπο.

15. *Λύση.* Από το μικρό θεώρημα του Fermat έχουμε $a^p = a$, για κάθε $a \in \mathbb{Z}_p$. Επαγωγικά παίρνουμε,

$$a^{p^n} = \left(a^{p^{n-1}}\right)^p = a^p = a.$$

Κατά συνέπεια το $x^{p^n} - x \in \mathbb{Z}_p[x]$ επάγει τη μηδενική απεικόνιση $\mathbb{Z}_p \to \mathbb{Z}_p$ για κάθε n.

16. *Λύση.* Το $x^2 + 1 \in \mathbb{R}[x]$ είναι ανάγωγο στο $\mathbb{R}[x]$, άρα κάθε διαιρέτης στο $\mathbb{R}[x]$ είναι της μορφής c ή $c(x^2+1)$, όπου $c \in \mathbb{R} \setminus \{0\}$. Επειδή $\mu\kappa\delta(f(x), x^2+1) \neq 1$, έπεται ότι $\mu\kappa\delta(f(x), x^2+1) = x^2+1$. Δηλαδή

$$x^2 + 1 | f(x). \tag{4.1}$$

Παρατηρούμε ότι $x^2 - 3x + 2 = (x-1)(x-2)$, επομένως

$$\mu\kappa\delta(f(x), x^2-3x+2) = \begin{cases} 1 & \text{ή} \\ x-1 & \text{ή} \\ x-2 & \text{ή} \\ (x-1)(x-2) = x^2-3x+2 \end{cases}$$

Παρατηρούμε ότι αν $\mu\kappa\delta(f(x), x^2-3x+2) = x^2-3x+2$, τότε

$$x^2 - 3x + 2 | f(x). \tag{4.2}$$

Από τις (4.1), (4.2) και από το γεγονός ότι $\mu\kappa\delta(x^2+1, x^2-3x+2) = 1$, έπεται ότι $(x^2+1)(x^2-3x+2)|f(x)$, δηλαδή $\deg f(x) \geq 4$, το οποίο είναι άτοπο. Συνεπώς

$$\mu\kappa\delta(f(x), x^2-3x+2) = \begin{cases} x-1 & \text{ή} \\ x-2 \end{cases}$$

Έστω ότι $\mu\kappa\delta(f(x), x^2-3x+2) = x-1$. Τότε $x-1|f(x)$, $x^2+1|f(x)$ και επειδή $\mu\kappa\delta(x-1, x^2+1) = 1$, έπεται ότι $(x-1)(x^2+1)|f(x)$. Αλλά επειδή $\deg f(x) = 3$ και το $f(x)$ είναι μονικό, έπεται ότι $f(x) = (x-1)(x^2+1)$. Αν $\mu\kappa\delta(f(x), x^2-3x+2) = x-2$, ομοίως παίρνουμε ότι $f(x) = (x-2)(x^2+1)$.

17. *Υπόδειξη.* Επειδή το $f(x)$ έχει πραγματικούς συντελεστές, μια ρίζα του είναι το $1-2i$ σύμφωνα με το Λήμμα 4.30. Από το Λήμμα 4.15 (3) έπεται ότι

$$(x - (1+2i))(x - (1-2i)) | f(x),$$

δηλαδή $x^2 - 2x + 5 | f(x)$. Υπολογίστε το πηλίκο με την Ευκλείδεια διαίρεση.

18. *Λύση.* i) Από το μικρό θεώρημα του Fermat έχουμε $a^p = a$, για κάθε $a \in \mathbb{Z}_p$. Επομένως

$$f(a) = a^p - a + 1_{\mathbb{Z}_p} = a - a + 1_{\mathbb{Z}_p} = 1_{\mathbb{Z}_p} \neq 0$$

ii) i. Έχουμε ότι $\mathbb{Z}_p$ και F είναι σώματα και $\mathbb{Z}_p \subseteq F$. Συμβολίζουμε με $R = \mathbb{Z}_p$ και με $S = F$, δηλαδή $R \subseteq S$. Παρατηρούμε ότι

$$1_S 1_R = 1_R = 1_R 1_R \Rightarrow (1_S - 1_R)1_R = 0_S = 0_R.$$

Αν $1_S - 1_R \neq 0_R$, τότε $1_R = 0_R$, το οποίο είναι άτοπο, αφού R περιοχή. Άρα $1_R = 1_S$.
Σημείωση. Δείξαμε ότι αν S περιοχή που περιέχει ως υποδακτύλιο περιοχή R, τότε $1_R = 1_S$.

Παρατηρούμε ότι για κάθε $r \in F$ έχουμε,

$$pr = p(1_F r) = (p1_F)r = (p1_{\mathbb{Z}_p})r = 0_{\mathbb{Z}_p} r = 0_F r = 0_F.$$

ii. Θα χρησιμοποιήσουμε το Παράδειγμα 3.17(2). Έστω $a \in F$ ρίζα του $f(x)$,

$$f(a) = a^p - a + 1_F = 0.$$

Θα δείξουμε ότι το $a+1_F$ είναι ρίζα του $f(x)$. Παρατηρούμε ότι

$$\begin{aligned} f(a+1_F) &= (a+1_F)^p - (a+1_F) + 1 \\ &= (a+1_F)^p - a \\ &= a^p + 1_F^p - a \\ &= a^p + 1_F - a = 0, \end{aligned}$$

όπου στην τρίτη ισότητα χρησιμοποιήσαμε το όνειρο του πρωτοετή.

Επομένως καθένα από τα στοιχεία

$$a, a+1_F, a+21_F \ldots, a+(p-1)1_F$$

είναι ρίζα του $f(x)$ στο F. Αυτά είναι διακεκριμένα Πράγματι, αν $a+i1_F = a+j1_F$, όπου $i,j \in \{0,1,\ldots,p-1\}$, τότε $i1_F = j1_F$, δηλαδή $[i]=[j]$ στο $\mathbb{Z}_p$, που σημαίνει ότι $p|i-j$. Η σχέση αυτή δίνει $i-j=0$ αφού $-p < i-j < p$.

19. *Λύση.* Από τον Ευκλείδειο αλγόριθμο παίρνουμε,

$$\begin{aligned} x^9 - 1 &= (x^5 - x)(x^4+1) + x - 1 \\ x^5 - x &= (x-1)(x^4 + x^3 + x^2 + x) + 0. \end{aligned}$$

Άρα $\mu\kappa\delta(x^5-x, x^9-1) = x-1$. Επομένως

$$x - 1 = x^9 - 1 + (-x^4 - 1)(x^5 - x).$$

Πολλαπλασιάζοντας με $x^{2010} + x^{2009} + \cdots + x + 1$, βρίσκουμε τα $a(x)$ και $b(x)$.

20. *Λύση.* Έστω ότι υπάρχει $f(x) \in \mathbb{Z}[x]$ θετικού βαθμού και $m \in \mathbb{Z}$ ώστε $f(m) = p$ πρώτος. Παρατηρούμε ότι για κάθε $k \in \mathbb{Z}$, $m + kp \equiv m \mod p$. Επομένως για κάθε $n \in \mathbb{Z}_{>0}$ έχουμε $(m+kp)^n \equiv m^n \mod p$, οπότε

$$f(m+kp) \equiv f(m) \equiv 0 \mod p.$$

Άρα $p|f(m+kp)$. Αλλά $f(m+kp)$ είναι πρώτος από υπόθεση, οπότε $f(m+kp) = p$ για κάθε $k \in \mathbb{Z}$. Τότε το πολυώνυμο $f(x) - p \in \mathbb{Z}[x] \subseteq \mathbb{R}[x]$ έχει άπειρες ρίζες, οπότε η Πρόταση 4.20 δίνει $f(x) - p = 0$. Άρα $f(x) = p$, άτοπο αφού $\deg f(x) > 0$.

21. *Λύση.*Το 101 είναι πρώτος, οπότε από το θεώρημα Wilson έχουμε

$$100! \equiv -1 \mod 101,$$

δηλαδή $[1][2]\cdots[98][99][100] = [-1]$ στο $\mathbb{Z}_{101}$. Από τον Ευκλείδειο αλγόριθμο βρίσκουμε ότι το αντίστροφο του $[99][100]$ είναι το $[-50]$. Πολλαπλασιάζοντας κατά μέλη με $[-50]$ παίρνουμε, $[98!] = [50]$. Επομένως το ζητούμενο υπόλοιπο είναι 50.

22. *Λύση.* Το -1 είναι ρίζα του $f(x)$. Επειδή είναι θετικού βαθμού, δεν είναι ανάγωγο.

23. *Λύση.* Από το Παράδειγμα 4.2 ξέρουμε ότι αν $g(x) \in \mathbb{Z}_p[x]$, τότε $(g(x))^p = g(x^p)$. Επομένως

$$(x^p - x)^p = (x^p)^p - x^p = x^{p^2} - x^p = f(x).$$

Αλλά από την Πρόταση 4.23, $x^p - x = x(x-1)\cdots(x-(p-1))$. Επομένως η ζητούμενη ανάλυση είναι $f(x) = x^p(x-1)^p \cdots (x-(p-1))^p$.

24. *Λύση.* i) *Πρώτος τρόπος.* Από το Παράδειγμα 4.2 παίρνουμε

$$\begin{aligned} f(x) &= x^{2p} + x^p + 1 - x^2 - x - 1 \\ &= x^{2p} + x^p - x^2 - x \\ &= (x^p - x)(x^p + x) + x^p - x \\ &= (x^p - x)(x^p + x + 1). \end{aligned}$$

Δηλαδή $x^p - x | f(x)$ στο $\mathbb{Z}_p[x]$.

Δεύτερος τρόπος. Από το μικρό θεώρημα του Fermat έχουμε ότι ότι για κάθε $a \in \mathbb{Z}_p$,

$$f(a) = (a^2+a+1)^p - (a^2+a+1) = a^2 + a + 1 - (a^2+a+1) = 0.$$

Συνεπώς $x-a|f(x)$ για κάθε $a\in\mathbb{Z}_p$. Επειδή τα πολυώνυμα $x-a$ είναι ανά δύο σχετικά πρώτα για $a=0,1,...,p-1$, το Λήμμα 4.15(3), δίνει ότι $x(x-1)...(x-(p-1))|f(x)$, δηλαδή $x^p-x|f(x)$.

ii) Έστω $p=2$. Τότε $f(x)=x(x-1)(x^2+x+1)$. Το $x^2+x+1\in\mathbb{Z}_2[x]$ είναι δευτέρου βαθμού και δεν έχει ρίζες στο $\mathbb{Z}_2$, οπότε από την Πρόταση 4.19 είναι ανάγωγο. Επομένως η ζητούμενη ανάλυση είναι $f(x)=x(x-1)(x^2+x+1)$.

Έστω $p=3$. Τότε $f(x)=x(x-1)(x+1)(x^3+x+1)$. Παρατηρούμε ότι $1^3+1+1=3=0$, άρα το $x^3+x+1\in\mathbb{Z}_3[x]$ διαιρείται με το $x-1$ στο $\mathbb{Z}_3[x]$. Από την Ευκλείδεια διαίρεση παίρνουμε,

$$x^3+x+1=(x-1)(x^2+x+2).$$

Το $x^2+x+2\in\mathbb{Z}_3[x]$ είναι δευτέρου βαθμού και δεν έχει ρίζες στο $\mathbb{Z}_3[x]$, επομένως είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Άρα η ζητούμενη ανάλυση είναι στο $\mathbb{Z}_3[x]$ είναι

$$f(x)=x(x-1)^2(x+1)(x^2+x+2).$$

25. *Λύση.* Η συνεπαγωγή "$\Leftarrow$" αποδείχτηκε στην Πρόταση 4.24(1).

Για το ευθύ αρκεί να δειχθεί ότι για κάθε πεπερασμένο σώμα k η ψ δεν είναι 1-1. Έστω λοιπόν $k=\{a_1,...,a_n\}$. Για τα πολυώνυμα

$$f(x)=(x-a_1)(x-a_2)...(x-a_n),\ \ g(x)=0$$

παρατηρούμε ότι $\overline{f}=\overline{g}$ καθώς η συνάρτηση $\overline{f}:k\to k$ είναι η μηδενική.

26. *Υπόδειξη.* Δείξτε ότι από τη δοσμένη σχέση έπεται (πχ με απαλοιφή παρονομαστών και χρήση του θεωρήματος του Wilson) ότι στο $\mathbb{Z}_p$ έχουμε

$$[b]\Big([1]^{-1}+[2]^{-1}+...+[p-1]^{-1}\Big)=[a].$$

Στη συνέχεια δείξτε ότι $[1]^{-1}+[2]^{-1}+...+[p-1]^{-1}=[1]+[2]+...+[p-1]=[0]$.

27. Λύση. Για τη μία κατεύθυνση, έστω $(1-ax)(b_0+...+b_mx^m)=1$. Κάνοντας τις πράξεις στο αριστερό μέλος και εξισώνοντας αντίστοιχους συντελεστές παίρνουμε

$$\begin{aligned} b_0 &= 1\\ -ab_0+b_1 &= 0\\ &\cdots\\ -ab_{m-1}+b_m &= 0\\ -ab_m &= 0. \end{aligned}$$

Εύκολα προκύπτουν διαδοχικά οι σχέσεις

$$b_0=1, b_1=a, ..., b_m=a^m, a^{m+1}=0.$$

Άρα το a είναι μηδενοδύναμο.

Αντίστροφα, έστω ότι $a^n=0$ για κάποιο n, οπότε $(ax)^n=0$. Το ζητούμενο έπεται από τη σχέση

$$\begin{aligned} 1=1-(ax)^n &= (1-ax)(1+ax+(ax)^2+...+(ax)^{n-1})\\ &= (1+ax+(ax)^2+...+(ax)^{n-1})(1-ax). \end{aligned}$$

28. *Υπόδειξη.* Έστω ότι $f(x)g(x)=0, g(x)=b_mx^m+...+b_0$. Μπορούμε να υποθέσουμε ότι $b_0\neq 0$ (δικαιολογήστε το). Χρησιμοποιώντας τις σχέσεις

$$\sum_{i+j=k}a_ib_j=0,\ k=0,...,n+m,$$

δείξτε ότι $b_0^{n+m+1}a_i=0$ για κάθε i.

29.

30. *Λύση.* Στην απόδειξη του κριτηρίου του Euler, Παράδειγμα 4.22(4), είδαμε ότι τα στοιχεία $1^2, 2^2, ..., q^2 \in \mathbb{Z}_p$ είναι διακεκριμένες ρίζες του πολυωνύμου $x^q - 1 \in \mathbb{Z}_p[x]$. Επειδή το πλήθος τους είναι q και το $\mathbb{Z}_p$ είναι σώμα, συμπεραίνουμε ότι υπάρχει $c \in \mathbb{Z}_p$ με

$$x^q - 1 = c(x - 1^2)(x - 2^2)...(x - q^2).$$

Συγκρίνοντας μεγιστοβάθμιους όρους έχουμε $c = 1$.

31. *Υπόδειξη* i) Ύπαρξη: Χρησιμοποιήστε την Ευκλείδεια διαίρεση πολυωνύμων όπως ακριβώς στη λύση της άσκησης 1.14. Δηλαδή, θεωρήστε
$r_0(x), q_0(x)$ το υπόλοιπο και πηλίκο της διαίρεσης του $f(x)$ με το $p(x)$,
$r_1(x), q_1(x)$ το υπόλοιπο και το πηλίκο της διαίρεσης του $q_0(x)$ με το $p(x)$, κοκ.

Ομομορφισμοί και ιδεώδη

Θυμόμαστε από τη Γραμμική Άλγεβρα ότι με τις γραμμικές απεικονίσεις μεταξύ δύο διανυσματικών χώρων U, V μπορούμε να 'συγκρίνουμε' τους U, V.

Έστω R και S δύο δακτύλιοι. Στο κεφάλαιο αυτό θα μελετήσουμε απεικονίσεις $R \to S$ που μας επιτρέπουν να 'συγκρίνουμε' τους R, S. Επίσης εισάγουμε και μελετάμε την έννοια του ιδεώδους δακτυλίου.

Βασικά σημεία

- ομομορφισμοί, ισομορφισμοί
- ιδεώδη (άθροισμα γινόμενο και τομή ιδεωδών)

5.1. Ομομορφισμοί και ισομορφισμοί

Ορισμός 5.1. *Έστω $(R, +, \cdot)$ και $(S, \oplus, \odot)$ δύο δακτύλιοι.*

- *Μια απεικόνιση $\varphi : R \to S$ λέγεται* ***ομομορφισμός δακτυλίων*** *αν*
  (1) $\varphi(r + r') = \varphi(r) \oplus \varphi(r')$ *για κάθε* $r, r' \in R$
  (2) $\varphi(r \cdot r') = \varphi(r) \odot \varphi(r')$ *για κάθε* $r, r' \in R$.
- *Ένας ομομορφισμός δακτυλίων λέγεται*
  (1) ***μονομορφισμός*** *αν είναι 1-1,*
  (2) ***επιμορφισμός*** *αν είναι επί,*
  (3) ***ισομορφισμός*** *αν είναι 1-1 και επί.*
- *Αν υπάρχει ισομορφισμός $R \to S$ θα λέμε ότι οι R και S είναι* ***ισόμορφοι*** *(συμβολικά $R \simeq S$).*

Σημείωση. Τώρα που είναι σαφές ότι γενικά οι πράξεις $+, \cdot$ του R είναι διαφορετικές από τις πράξεις $\oplus, \odot$ του S, θα επανέλθουμε στη συνήθη πρακτική να χρησιμοποιούμε απλούστερους συμβολισμούς. Έτσι, αντί να γράφουμε

$$\varphi(r + r') = \varphi(r) \oplus \varphi(r'), \quad \varphi(r \cdot r') = \varphi(r) \odot \varphi(r')$$

θα γράφουμε αντίστοιχα

$$\varphi(r + r') = \varphi(r) + \varphi(r'), \quad \varphi(rr') = \varphi(r)\varphi(r').$$

Παραδείγματα 5.2.

(1) Για κάθε δακτύλιο R η ταυτοτική απεικόνιση $R \to R, r \mapsto r$, είναι ισομορφισμός δακτυλίων Αν R, S είναι δακτύλιοι, η μηδενική απεικόνιση $R \to S, r \mapsto 0_S$, είναι ομομορφισμός δακτυλίων.

(2) Έστω $R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) : a, b \in \mathbb{R} \right\}$ και $S = \mathbb{C}$. Αφήνουμε ως άσκηση την επαλήθευση ότι το R είναι υποδακτύλιος του $M_2(\mathbb{R})$. Θα δείξουμε ότι η απεικόνιση $\varphi : R \to S$ με $\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$ είναι ισομορφισμός δακτυλίων.

Πράγματι έχουμε,

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} a+a' & b+b' \\ -(b+b') & a+a' \end{pmatrix}\right) \\ &= a + a' + (b+b')i \\ &= (a+bi) + (a'+b'i) \\ &= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) \end{aligned}$$

και

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right) &= \varphi\left(\begin{pmatrix} aa'-bb' & ab'+ba' \\ -(ab'+ba') & aa'-bb' \end{pmatrix}\right) \\ &= aa' - bb' + (ab'+ba')i \\ &= (a+bi)(a'+b'i) \\ &= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}\right). \end{aligned}$$

Προφανώς η φ είναι επί. Είναι και 1-1, γιατί αν $\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \varphi \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$, τότε $a + bi = a' + b'i \Rightarrow a = a'$ και $b = b'$ δηλαδή $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix}$. Άρα η $\varphi : R \to S$ είναι ισομορφισμός δακτυλίων.

(3) Η απεικόνιση $\varphi : \mathbb{C} \to \mathbb{C}$ με $\varphi(z) = \overline{z}$ είναι ισομορφισμός δακτυλίων, όπου $\overline{z}$ είναι ο συζυγής του z.

Πράγματι γνωρίζουμε ότι για κάθε $z_1, z_2 \in \mathbb{C}$, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$, δηλαδή

$$\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2), \quad \varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$$

που σημαίνει ότι η φ είναι ομομορφισμός δακτυλίων. Από την ισότητα μιγαδικών αριθμών είναι σαφές ότι η φ είναι 1-1. Τέλος, αν $z \in \mathbb{C}$, τότε $\varphi(\overline{z}) = \overline{\overline{z}} = z$ που σημαίνει ότι η φ είναι επί.

Σημείωση. Ότι η απεικόνιση φ είναι 1-1 και επί έπεται και από το γεγονός ότι η σύνθεση $\varphi \circ \varphi$ είναι η ταυτοτική απεικόνιση στο $\mathbb{C}$.

(4) Έστω $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Η απεικόνιση $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ με

$$\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$$

είναι ισομορφισμός.

Παρατηρούμε πρώτα ότι κάθε στοιχείο του $\mathbb{Z}[\sqrt{2}]$ γράφεται μοναδικά ως $a + b\sqrt{2}$ με $a, b \in \mathbb{Z}$. Πράγματι, αν $a + b\sqrt{2} = a' + b'\sqrt{2}$ με $a, a', b, b' \in \mathbb{Z}$, αρκεί να δείξουμε ότι $a = a$ και $b = b'$. Έχουμε,

$$a + b\sqrt{2} = a' + b'\sqrt{2} \Rightarrow a - a' = (b' - b)\sqrt{2},$$

οπότε αν $b' - b \neq 0$, τότε $\sqrt{2} = \frac{a-a'}{b-b'} \in \mathbb{Q}$, που είναι άτοπο. Άρα $b' - b = 0$ και συνεπώς $a - a' = 0$.

Από την προηγούμενη παρατήρηση έπεται ότι η απεικόνιση φ είναι καλά ορισμένη.

Έχουμε,

$$\begin{aligned}\varphi\left((a+b\sqrt{2})+(a'+b'\sqrt{2})\right) &= \varphi\left(a+a'+(b+b')\sqrt{2}\right)\\ &= a+a'-(b+b')\sqrt{2}\\ &= a-b\sqrt{2}+a'-b'\sqrt{2}\\ &= \varphi(a+b\sqrt{2})+\varphi(a'+b'\sqrt{2}),\ \text{και}\\ \varphi\left((a+b\sqrt{2})(a'+b'\sqrt{2})\right) &= \varphi\left(aa'+2bb'+(ab'+ba')\sqrt{2}\right)\\ &= aa'+2bb'-(ab'+ba')\sqrt{2}\\ &= (a-b\sqrt{2})(a'-b'\sqrt{2})\\ &= \varphi(a+b\sqrt{2})\varphi(a'+b'\sqrt{2})\end{aligned}$$

που σημαίνει ότι η φ είναι ομομορφισμός δακτυλίων.

Από την αρχική παρατήρηση έπεται άμεσα ότι η φ είναι 1-1.

Από την ισότητα $\varphi(a-b\sqrt{2}) = a+b\sqrt{2}$ έπεται άμεσα ότι η φ είναι επί.

Σημείωση. Ότι η φ είναι 1-1 και επί έπεται και από το γεγονός ότι η σύνθεση $\varphi\circ\varphi$ είναι η ταυτοτική απεικόνιση στο $\mathbb{Z}[\sqrt{2}]$.

(5) Αν $\mu\kappa\delta(m,n)=1$, τότε υπάρχει ισομορφισμός δακτυλίων $\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$.

Ορίζουμε $\varphi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$, με

$$\varphi([a]_{mn}) = ([a]_m,[a]_n).$$

Παρατηρούμε πρώτα ότι η φ είναι καλώς ορισμένη απεικόνιση. Πράγματι, αν $[a]_{mn}=[b]_{mn}$, τότε $mn|a-b$, οπότε $m|a-b$ και $n|a-b$, δηλαδή $[a]_m=[b]_m$ και $[a]_n=[b]_n$. Άρα

$$([a]_m,[a]_n)=([b]_m,[b]_n),$$

δηλαδή $\varphi([a]_{mn})=\varphi([b]_{mn})$.

Η φ είναι ομομορφισμός: Έχουμε

$$\begin{aligned}\varphi([a]_{mn}+[a']_{mn}) &= \varphi([a+a']_{mn}) = ([a+a']_m,[a+a']_n)\\ &= ([a]_m+[a']_m,[a]_n+[a']_n)\\ &= ([a]_m,[a]_n)+([a']_m,[a']_n)\\ &= \varphi([a]_{mn})+\varphi([a']_{mn}).\end{aligned}$$

Ομοίως αποδεικνύεται ότι $\varphi([a]_{mn}[a']_{mn})=\varphi([a]_{mn})\varphi([a']_{mn})$.

Η φ είναι 1-1. Πράγματι, έστω $\varphi([a]_{mn})=\varphi([a']_{mn})$. Τότε

$$([a]_m,[a]_n)=([a']_m,[a']_n).$$

Επομένως $[a]_m=[a']_m$ και $[a]_n=[a']_n$. Άρα $m|a-a'$ και $n|a-a'$. Επειδή όμως $\mu\kappa\delta(m,n)=1$, έχουμε $mn|a-a'$. Άρα $[a]_{mn}=[b]_{mn}$.

Η φ είναι επί. Πράγματι η $\varphi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ είναι 1-1 και $|\mathbb{Z}_{mn}|=|\mathbb{Z}_m\times\mathbb{Z}_n|=mn<\infty$. Επομένως η φ είναι επί.

Σημειώσεις. (1) Ως πόρισμα από το γεγονός ότι η παραπάνω απεικόνιση $\varphi:\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$ είναι 1-1 και επί, παίρνουμε το κλασσικό **Κινέζικο θεώρημα υπολοίπων**:

Έστω $n_1,...,n_t\in\mathbb{Z}$ σχετικά πρώτοι ανά δύο και έστω $a_1,...,a_t\in\mathbb{Z}$. Τότε υπάρχει ακέραιος $x\in\mathbb{Z}$ έτσι ώστε για κάθε i,

$$x\equiv a_i \mod n_i.$$

Επιπλέον, αν x,x' είναι δύο τέτοιοι ακέραιοι, τότε $x\equiv x' \mod (n_1...n_t)$. Μια γενίκευση αυτού θα δούμε στην Παράγραφο 6.5.

(2) Την απεικόνιση του παραδείγματος και μερικά από τα επιχειρήματα τα είδαμε στην απόδειξη του θεωρήματος 2.22.

(6) Η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, με $\varphi(a) = [a]$ είναι επιμορφισμός.
Πράγματι είναι σαφές ότι η φ είναι ομομορφισμός δακτυλίων, αφού

$$[a + a'] = [a] + [a'] \text{ και } [aa'] = [a][a'].$$

Επίσης είναι σαφές ότι η φ είναι επί.

(7) Έστω R μεταθετικός δακτύλιος ώστε $pr = 0$ για κάθε $r \in R$ και για κάποιο πρώτο p. Τότε η απεικόνιση $\varphi : R \to R$, $\varphi(r) = r^p$ είναι ομομορφισμός.
Πράγματι από το Παράδειγμα 3.17 αν $r, s \in R$ τότε $(r + s)^p = r^p + s^p$. Δηλαδή, $\varphi(r + s) = \varphi(r) + \varphi(s)$. Επίσης, $\varphi(rs) = (rs)^p = r^p s^p$ αφού ο R είναι μεταθετικός.
Για παράδειγμα, η απεικόνιση

$$\mathbb{Z}_p[x] \to \mathbb{Z}_p[x],\ f(x) \mapsto f(x)^p,$$

όπου p πρώτος, είναι ομομορφισμός δακτυλίων.

(8) Η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(a) = 2a$, δεν είναι ομομορφισμός δακτυλίων.
Για παράδειγμα, ενώ $\varphi(1 \cdot 1) = \varphi(1) = 2$, έχουμε $\varphi(1)\varphi(1) = 2 \cdot 2 = 4 \neq 2$.

Ακολουθούν μερικές άμεσες συνέπειες του ορισμού που θα χρησιμοποιούμε παρακάτω χωρίς ιδιαίτερη μνεία.

Πρόταση 5.3. *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε ισχύουν τα ακόλουθα.*

(1) $\varphi(0_R) = 0_S$.
(2) *Για κάθε $r \in R$ έχουμε $\varphi(-r) = -\varphi(r)$.*
(3) *Για κάθε $r_1, \ldots, r_n \in R$,*

$$\varphi(r_1 + \cdots + r_n) = \varphi(r_1) + \cdots + \varphi(r_n) \quad \text{και} \quad \varphi(r_1 \cdots r_n) = \varphi(r_1) \cdots \varphi(r_n).$$

Ειδικά για κάθε $n \in \mathbb{Z}$ και για κάθε $r \in R$ ισχύει $\varphi(nr) = n\varphi(r)$. Επίσης για κάθε $n \in \mathbb{Z}_{>0}$ και για κάθε $r \in R$ ισχύει $\varphi(r^n) = \varphi(r)^n$.

Απόδειξη. (1) Παρατηρούμε ότι

$$0_R + 0_R = 0_R \Rightarrow \varphi(0_R + 0_R) = \varphi(0_R) \Rightarrow \varphi(0_R) + \varphi(0_R) = \varphi(0_R) \Rightarrow \varphi(0_R) = 0_S$$

σύμφωνα με το νόμο διαγραφής της πρόσθεσης στον S)
(2) Παρατηρούμε ότι

$$r + (-r) = 0_R \Rightarrow \varphi(r + (-r)) = \varphi(0_R) \Rightarrow$$
$$\varphi(r) + \varphi(-r) = \varphi(0_R) = 0_S \Rightarrow \varphi(-r) = -\varphi(r).$$

(3) Για $n \in \mathbb{Z}_{>0}$ έπεται άμεσα με επαγωγή. Για αρνητικό n παρατηρήστε ότι $\varphi(nr) = \varphi((-n)(-r)) = -n\varphi(-r) = -n(-\varphi(r)) = n\varphi(r)$, όπου στην τρίτη ισότητα χρησιμοποιήσαμε το (2). □

Μια χρήσιμη παρατήρηση για τη συμπεριφορά ομομορφισμών στα μοναδιαία στοιχεία (αν υπάρχουν) είναι η ακόλουθη.

Πρόταση 5.4. *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Αν η φ είναι επί και ο R έχει μοναδιαίο στοιχείο 1_R, τότε ο S έχει μοναδιαίο στοιχείο το $\varphi(1_R)$. Ειδικά, αν ο φ είναι ισομορφισμός και οι R, S έχουν μοναδιαία στοιχεία, τότε $\varphi(1_R) = 1_S$.*

Απόδειξη. Έστω ότι η $\varphi : R \to S$ είναι επί και $s \in S$. Τότε υπάρχει $r \in R$ ώστε $\varphi(r) = s$. Επομένως

$$\varphi(1_R)s = \varphi(1_R)\varphi(r) = \varphi(1_R r) = \varphi(r) = s.$$

Ομοίως παίρνουμε ότι $s\varphi(1_R) = s$. Επομένως ο S έχει μοναδιαίο στοιχείο το $\varphi(1_R)$.

Ο δεύτερος ισχυρισμός της πρότασης έπεται από τον πρώτο και τη μοναδικότητα του μοναδιαίου στοιχείου του S. □

Πρόταση 5.5. *Έστω $\varphi : R \to S$ και $\psi : S \to T$ ομομορφισμοί δακτυλίων.*

(1) *Η σύνθεση $\psi \circ \varphi : R \to T$ είναι ομομορφισμός δακτυλίων. Ειδικά, αν οι φ, ψ είναι ισομορφισμοί, τότε ο $\psi \circ \varphi$ είναι ισομορφισμός.*

(2) *Αν ο φ είναι ισομορφισμός, τότε η αντίστροφη απεικόνιση $\varphi^{-1} : S \to R$ είναι ισομορφισμός.*

Απόδειξη. (1) Για κάθε $r, r' \in R$ έχουμε

$$(\psi \circ \varphi)(r + r') = \psi(\varphi(r + r')) = \psi(\varphi(r) + \varphi(r')) =$$
$$\psi(\varphi(r)) + \psi(\varphi(r')) = (\psi \circ \varphi)(r) + (\psi \circ \varphi)(r'), \text{ και}$$
$$(\psi \circ \varphi)(rr') = \psi(\varphi(rr')) = \psi(\varphi(r)\varphi(r')) =$$
$$\psi(\varphi(r))\psi(\varphi(r')) = (\psi \circ \varphi)(r)(\psi \circ \varphi)(r').$$

Αν καθεμιά από τις απεικονίσεις φ, ψ είναι 1-1 και επί, ξέρουμε ότι και η σύνθεση $\psi \circ \varphi$ είναι 1-1 και επί.
(2) Επειδή η απεικόνιση φ είναι 1-1 και επί, ξέρουμε ότι ορίζεται η αντίστροφη απεικόνιση $\varphi^{-1} : S \to R$ από

$$\varphi^{-1}(s) = r \Leftrightarrow s = \varphi(r).$$

Για κάθε $s, s' \in S$ έχουμε

$$\varphi(\varphi^{-1}(s) + \varphi^{-1}(s')) = \varphi(\varphi^{-1}(s)) + \varphi(\varphi^{-1}(s')) = s + s' \Rightarrow$$
$$\varphi^{-1}(s) + \varphi^{-1}(s') = \varphi^{-1}(s + s')$$

και όμοια

$$\varphi(\varphi^{-1}(s)\varphi^{-1}(s')) = \varphi(\varphi^{-1}(s))\varphi(\varphi^{-1}(s')) = ss' \Rightarrow$$
$$\varphi^{-1}(s)\varphi^{-1}(s') = \varphi^{-1}(ss').$$

Άρα η φ^{-1} είναι ισομορφισμός δακτυλίων. □

Παρατήρηση. Από την προηγούμενη πρόταση έπεται ότι αν A είναι οποιοδήποτε μη κενό σύνολο τα στοιχεία του οποίου είναι δακτύλιοι, τότε η σχέση στο A που ορίζεται από $R \sim S \Leftrightarrow R \simeq S$ είναι σχέση ισοδυναμίας. Όταν μελετάμε αλγεβρικές ιδιότητες ισόμορφων δακτυλίων, μπορούμε να τους ταυτίζουμε.

Παραδείγματα 5.6.

(1) Οι δακτύλιοι $2\mathbb{Z}$ και $3\mathbb{Z}$ δεν είναι ισόμορφοι.

Πράγματι, έστω $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ ομομορφισμός. Τότε $\varphi(2) = 3m$, για κάποιο $m \in \mathbb{Z}$. Παρατηρούμε ότι

$$\varphi(4) = \varphi(2 + 2) = \varphi(2) + \varphi(2) = 3m + 3m = 6m \text{ και}$$
$$\varphi(4) = \varphi(2^2) = \varphi(2)^2 = (3m)^2 = 9m^2.$$

Άρα $6m = 9m^2 \Rightarrow m(3m - 2) = 0 \Rightarrow m = 0$, αφού $\frac{2}{3} \notin \mathbb{Z}$. Δείξαμε ότι $\varphi(2) = 0$. Επειδή ο φ είναι ομομορφισμός ισχύει $\varphi(0) = 0$. Άρα η απεικόνιση φ δεν είναι 1-1, επομένως δεν είναι ισομορφισμός.

(2) Οι δακτύλιοι $\mathbb{C}$ και $\mathbb{R}$ δεν είναι ισόμορφοι.

Έστω $\varphi : \mathbb{C} \to \mathbb{R}$ ισομορφισμός. Αφού έχουμε $i^2 = -1$ στο $\mathbb{C}$, παίρνουμε

$$\varphi(i^2) = \varphi(-1) \Rightarrow \varphi(i)^2 = -\varphi(1) = -1.$$

(Είναι $\varphi(1) = 1$ από την Πρόταση 5.4). Άρα $\varphi(i) \notin \mathbb{R}$, άτοπο.

(3) Οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{Q}[x]$ δεν είναι ισόμορφοι.
Έστω $\varphi : \mathbb{Q}[x] \to \mathbb{Z}$ ισομορφισμός και $\varphi(x) = m$. Για κάθε ακέραιο n είναι

$$\varphi(n) = n\varphi(1) = n,$$

όπου η τελευταία ισότητα προκύπτει από την Πρόταση 5.4. Άρα $\varphi(x) = \varphi(m)$, δηλαδή η απεικόνιση φ δεν είναι 1-1, άτοπο.

(4) Θα βρούμε όλους τους ομομορφισμούς δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{C}$.
Κάθε ομομορφισμός δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{C}$ καθορίζεται από την εικόνα $\varphi(1)$, γιατί για κάθε $n \in \mathbb{Z}$ έχουμε $\varphi(n) = n\varphi(1)$. Επειδή $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)^2$, έπεται ότι $\varphi(1) \in \{0, 1\}$. Στην πρώτη περίπτωση έχουμε το μηδενικό ομομορφισμό, $\varphi : \mathbb{Z} \to \mathbb{C}$, $n \mapsto 0$, και στη δεύτερη έχουμε το μονομορφισμό $\varphi : \mathbb{Z} \to \mathbb{C}$, $n \mapsto n$.

Πρόταση 5.7. *Έστω $\varphi : R \to S$ ισομορφισμός δακτυλίων.*
(1) *Ο R είναι μεταθετικός αν και μόνο αν ο S είναι μεταθετικός.*
(2) *Ο R είναι περιοχή αν και μόνο αν ο S είναι περιοχή.*
(3) *Ο R είναι σώμα αν και μόνο αν ο S είναι σώμα.*

Απόδειξη. Σε κάθε περίπτωση αρκεί να δείξουμε το ευθύ καθώς το αντίστροφο έπεται από το ευθύ για την απεικόνιση φ^{-1} που ξέρουμε ότι είναι ισομορφισμός από την Πρόταση 5.5.
(1) Έστω $s_1, s_2 \in S$. Επειδή η απεικόνιση φ είναι επί, υπάρχουν $r_i \in R$ με $s_i = \varphi(r_i)$. Έχουμε διαδοχικά

$$s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) = \varphi(r_2 r_1) = \varphi(r_2)\varphi(r_1) = s_2 s_1.$$

(2) Παρατηρούμε τα εξής.

- Ως περιοχή, ο R έχει μονάδα και $1_R \neq 0_R$. Επειδή η απεικόνιση φ είναι 1-1 παίρνουμε $\varphi(1_R) \neq \varphi(0_R)$. Επειδή ο ομομορφισμός φ είναι επί, το $\varphi(1_R)$ είναι μονάδα του S, σύμφωνα με την Πρόταση 5.4. Συνεπώς έχουμε $1_S \neq 0_S$.
- Ο S είναι μεταθετικός από το (1).
- Έστω $s_1, s_2 \in S$. Επειδή η απεικόνιση φ είναι επί, υπάρχουν $r_i \in R$ με $s_i = \varphi(r_i)$. Αν $s_1 s_2 = 0_S$, τότε

$$\varphi(0_R) = 0_S = s_1 s_2 = \varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2).$$

Επειδή η φ είναι 1-1 παίρνουμε $0_R = r_1 r_2$. Επειδή ο R είναι περιοχή έπεται ότι $r_1 = 0_R$ ή $r_2 = 0_R$. Τότε $s_1 = \varphi(0_R) = 0_S$ ή $s_2 = \varphi(0_R) = 0_S$ Άρα ο S είναι περιοχή.

(3) Λόγω των δύο πρώτων συμπερασμάτων του (2), αρκεί να δειχθεί ότι κάθε μη μηδενικό στοιχείο του S είναι αντιστρέψιμο. Έστω $s \in S$ με $s \neq 0$. Αφού η φ είναι επί υπάρχει $r \in R$ με $\varphi(r) = s$. Παρατηρούμε ότι αν $r = 0_R$, τότε $s = \varphi(0_R) = 0_S$. Άρα $r \neq 0_R$. Επειδή το R είναι σώμα, υπάρχει $r' \in R$ ώστε $rr' = 1_R$ και $r'r = 1_R$. Τότε

$$s\varphi(r') = \varphi(r)\varphi(r') = \varphi(rr') = \varphi(1_R) = 1_S, \text{ και}$$

$$\varphi(r')s = \varphi(r')\varphi(r) = \varphi(r'r) = \varphi(1_R) = 1_S,$$

που σημαίνει ότι το s είναι αντιστρέψιμο. □

Παράδειγμα 5.8. Στα Παραδείγματα 3.12 είδαμε ότι ο δακτύλιος $\mathbb{Q}[\sqrt{2}]$ είναι σώμα και ο δακτύλιος $\mathbb{Z}[\sqrt{2}]$ δεν είναι σώμα. Άρα οι δακτύλιοι αυτοί δεν είναι ισόμορφοι.

Εφαρμογή (Ένα κριτήριο για ανάγωγα πολυώνυμα)

(1) Έστω $\varphi : R \to S$ ένας ομομορφισμός μεταθετικών δακτυλίων που έχουν μοναδιαία στοιχεία, τέτοιος ώστε $\varphi(1_R) = 1_S$. Τότε η απεικόνιση

$$\tilde{\varphi} : R[x] \to S[x], \quad \tilde{\varphi}(r_m x^m + \cdots + r_0) = \varphi(r_m)x^m + \cdots + \varphi(r_0)$$

είναι ένας ομομορφισμός δακτυλίων τέτοιος ώστε $\tilde{\varphi}(1_R) = 1_S$.
Πράγματι, με εύκολους υπολογισμούς επαληθεύεται ότι

$$\tilde{\varphi}(f(x) + g(x)) = \tilde{\varphi}(f(x)) + \tilde{\varphi}(g(x)), \quad \text{και}$$
$$\tilde{\varphi}(f(x)g(x)) = \tilde{\varphi}(f(x))\tilde{\varphi}(g(x))$$

για κάθε $f(x), g(x) \in R[x]$. Η $\tilde{\varphi}$ ονομάζεται η **επέκταση** της φ στο $R[x]$

(2) Έστω $f(x) \in \mathbb{Z}[x]$ ένα μονικό πολυώνυμο. Τότε το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$ αν υπάρχει $m > 0$ τέτοιο ώστε το $\tilde{\varphi}(f(x))$ είναι ανάγωγο στο $\mathbb{Z}_m[x]$, όπου $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ είναι η επέκταση του φυσικού επιμορφισμού $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ στο $\mathbb{Z}[x]$.
Πράγματι, έστω ότι υπάρχουν θετικού βαθμού πολυώνυμα $g(x), h(x) \in \mathbb{Z}[x]$ με $f(x) = g(x)h(x)$. Μπορούμε να υποθέσουμε ότι τα $g(x), h(x)$ είναι μονικά. Τότε τα $\tilde{\varphi}(g(x)), \tilde{\varphi}(h(x))$ είναι μονικά και

$$\deg \tilde{\varphi}(g(x)) = \deg g(x), \quad \deg \tilde{\varphi}(h(x)) = \deg h(x).$$

Από το (1) έχουμε επίσης ότι $\tilde{\varphi}(f(x)) = \tilde{\varphi}(g(x))\tilde{\varphi}(h(x))$. Επειδή το $\tilde{\varphi}(f(x))$ είναι ανάγωγο καταλήγουμε σε άτοπο.

(3) Το $f(x) = x^3 + 10x^2 + 30x - 1027 \in \mathbb{Z}[x]$ είναι ανάγωγο.
Πράγματι, έστω $m = 3$. Τότε $\tilde{\varphi}(f(x)) = x^3 + x^2 - 1$. Παρατηρούμε ότι στο $\mathbb{Z}_3$, το $x^3 + x^2 - 1$ δεν έχει ρίζα και επειδή ο βαθμός του είναι 3 συμπεραίνουμε ότι αυτό είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Από το (2) έπεται ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$.
Σημείωση. Αν επιλέγαμε $m = 5$, τότε το $\tilde{\varphi}(f(x)) = x^3 - 2$ δεν είναι ανάγωγο στο $\mathbb{Z}_5[x]$ αφού έχει μια ρίζα στο $\mathbb{Z}_5$, την 3. Συνεπώς για αυτόν τον m το κριτήριο δεν μπορεί να εφαρμοστεί.

5.2. Πυρήνας και εικόνα ομομορφισμού

Ορισμός 5.9. *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Ο **πυρήνας** του φ είναι το σύνολο*

$$\ker \varphi = \{r \in R : \varphi(r) = 0_S\}$$

*και η **εικόνα** του φ είναι το σύνολο*

$$\mathrm{Im}\varphi = \{\varphi(r) \in S : r \in R\}.$$

Παραδείγματα 5.10.

(1) Η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(m) = [m]$, είναι ομομορφισμός δακτυλίων και

$$\ker \varphi = \{m \in \mathbb{Z} : [m] = [0]\} = \{m \in \mathbb{Z} : n|m\} = n\mathbb{Z},$$
$$Im\varphi = \mathbb{Z}_n.$$

(2) **Ομομορφισμός εκτίμησης** Έστω F σώμα και $a \in F$. Η απεικόνιση $\epsilon_a : F[x] \to F$ με $\epsilon_a(f(x)) = f(a)$ είναι ομομορφισμός δακτυλίων και

$$\ker \epsilon_a = \{f(x) \in F[x] : f(a) = 0\} = \{(x-a)g(x) : g(x) \in F[x]\},$$
$$Im\epsilon_a = F.$$

(3) Έστω F σώμα. Η απεικόνιση $\varphi : F[x] \to F \times F$ με $\varphi(f(x)) = (f(0), f(1))$ είναι ομομορφισμός δακτυλίων και

$$\ker \varphi = \{f(x) \in F[x] : f(0) = f(1) = 0\} = \{x(x-1)g(x) : g(x) \in F[x]\},$$

όπου η δεύτερη ισότητα προκύπτει ως εξής.

$$\begin{aligned} f(0) = f(1) = 0 &\Leftrightarrow x|f(x) \quad \text{και} \quad x-1|f(x) \\ &\Leftrightarrow x(x-1)|f(x) \quad (\text{αφού} \quad \mu\kappa\delta(x, x-1) = 1) \\ &\Leftrightarrow f(x) = x(x-1)g(x), \ \ g(x) \in F[x]. \end{aligned}$$

Η απεικόνιση φ είναι επί, δηλαδή $Im\varphi = F \times F$, διότι δοσμένου του $(a, b) \in F \times F$, το πολυώνυμο $f(x) = (b-a)x + a$ ικανοποιεί $f(0) = a, \ f(1) = b$.

(4) Έστω $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\}$. Είναι υπόθεση ρουτίνας να επαληθευθεί ότι η απεικόνιση $\varphi : R \to \mathbb{Z},\ \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = c$ είναι επιμορφισμός δακτυλίων και $\ker \varphi = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$.

(5) Έστω $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$, $m \in \mathbb{N}$, η επέκταση του φυσικού επιμορφισμού $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, $a \mapsto [a]$. Τότε $\ker \tilde{\varphi} = \{a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] | m | a_i \text{ για κάθε } i\}$. Πιο γενικά, αν $\varphi : R \to S$ είναι ένας ομομορφισμός μεταξύ δύο δακτυλίων που έχουν μοναδιαία στοιχεία τέτοιος ώστε $\varphi(1_R) = 1_S$, τότε για τον πυρήνα της επέκτασης $\tilde{\varphi} : R[x] \to S[x]$ έχουμε $\ker \tilde{\varphi} = \{a_n x^n + \cdots + a_1 x + a_0 \in R[x] | a_i \in \ker \varphi \text{ για κάθε } i\}$.

Πρόταση 5.11. *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε η φ είναι 1-1 αν και μόνο αν $\ker \varphi = \{0_R\}$.*

Απόδειξη. Έστω φ 1-1 και έστω $a \in \ker \varphi$. Τότε $\varphi(a) = 0_S = \varphi(0_R) \Rightarrow a = 0_R$, αφού η φ είναι 1-1. Επομένως $\ker \varphi = \{0_R\}$.

Αντίστροφα, έστω $\ker \varphi = \{0_R\}$ και έστω ότι $\varphi(a) = \varphi(b),\ a, b \in R$. Τότε

$$\varphi(a) - \varphi(b) = 0_S \Rightarrow \varphi(a - b) = 0_S \overset{\ker \varphi = \{0_R\}}{\Longrightarrow} a - b = 0_R \Rightarrow a = b.$$

□

Πρόταση 5.12. *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε ισχύουν οι ακόλουθες ιδιότητες.*
(1) $\ker \varphi \neq \emptyset$.
(2) *Αν $a, b \in \ker \varphi$ τότε $a - b \in \ker \varphi$.*
(3) *Αν $a \in \ker \varphi$ και $r \in R$, τότε $ra \in \ker \varphi$ και $ar \in \ker \varphi$.*

Απόδειξη. (1) Επειδή $\varphi(0_R) = 0_S$, έχουμε $0_R \in \ker \varphi$.

(2) Έστω $\varphi(a) = \varphi(b) = 0_S$. Τότε

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0_S \Rightarrow a - b \in \ker \varphi.$$

(3) Έστω $\varphi(a) = 0_S$. Τότε

$$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S \Rightarrow ra \in \ker \varphi.$$

Ομοίως αποδεικνύεται ότι $ar \in \ker \varphi$. □

Σημείωση. Από την προηγούμενη πρόταση έπεται άμεσα ότι ο $\ker \varphi$ είναι υποδακτύλιος του R. Αφήνουμε ως άσκηση την επαλήθευση ότι η εικόνα $Im\varphi$ είναι υποδακτύλιος του S.

5.3. Ιδεώδη

Ορισμός 5.13. *Έστω R δακτύλιος και $I \subseteq R$. Το I καλείται* **ιδεώδες** *του R (συμβολικά $I \trianglelefteq R$) αν ισχύουν τα ακόλουθα.*
(1) $I \neq \emptyset$.
(2) *Για κάθε $a, b \in I,\ a - b \in I$.*
(3) *Για κάθε $r \in R$ και για κάθε $a \in I$, $ra \in I$ και $ar \in I$.*

Παρατηρήσεις.

(1) Παρατηρούμε ότι στην περίπτωση που ο R είναι μεταθετικός, η ιδιότητα (3) του παραπάνω ορισμού ισοδυναμεί με την ιδιότητα
(3′) Για κάθε $r \in R$ και για κάθε $a \in I$, $ra \in I$.

(2) Στην Πρόταση 5.12 είδαμε ότι ο πυρήνας κάθε ομομορφισμού δακτυλίων $R \to S$ είναι ιδεώδες του R.

Παραδείγματα 5.14.

(1) Αν R δακτύλιος, τότε τα σύνολα R και $\{0_R\}$ είναι ιδεώδη του R. Θα καλούμε το $\{0_R\}$ το **τετριμμένο** (ή **μηδενικό**) ιδεώδες του R.

(2) Από την παραπάνω Παρατήρηση και τα Παραδείγματα 5.10 έχουμε τα ακόλουθα παραδείγματα ιδεωδών:
   i) $n\mathbb{Z}$ ιδεώδες του $\mathbb{Z}$.
   ii) $\{f(x) \in F[x] : f(a) = 0\} = \{(x-a)g(x) : g(x) \in F[x]\}$ ιδεώδες του $F[x]$.
   iii) $\{f(x) \in F[x] : f(0) = f(1) = 0\} = \{x(x-1)g(x) : g(x) \in F[x]\}$ ιδεώδες του $F[x]$.
   iv) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$ είναι ιδεώδες του

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\}.$$

(3) Το υποσύνολο I του $R = \mathbb{Z}[x]$ που αποτελείται από όλα τα πολυώνυμα βαθμού το πολύ 2 δεν είναι ιδεώδες του $\mathbb{Z}[x]$ διότι δεν ικανοποιείται η ιδιότητα (3) του Ορισμού 5.11. Για παράδειγμα έχουμε $x \in R$, $x^2 \in I$ αλλά $xx^2 = x^3 \notin I$.

(4) Έστω

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a, b, c \in \mathbb{Z} \right\} \quad \text{και} \quad I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \mathbb{Z} \right\}.$$

Τότε το I είναι ιδεώδες του R.

Πράγματι, $I \neq \emptyset$, αφού για παράδειγμα $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in I$.

Έστω $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I$. Τότε

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b-b' \\ 0 & 0 \end{pmatrix} \in I.$$

Τέλος έστω $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$ και $\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \in I$. Τότε

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ab' \\ 0 & 0 \end{pmatrix} \in I, \text{ και}$$
$$\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & b'c \\ 0 & 0 \end{pmatrix} \in I.$$

2ος τρόπος. Εναλλακτικά, για να δείξουμε ότι το I είναι ιδεώδες του R θεωρούμε την απεικόνιση

$$\varphi : R \to \mathbb{Z} \times \mathbb{Z}, \text{ με } \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c).$$

Τότε

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \right) &= \varphi \begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix} \\ &= (a+a', c+c') \\ &= (a, c) + (a', c') \\ &= \varphi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \varphi \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \end{aligned}$$

και

$$\begin{aligned}\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) &= \varphi\begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix} \\ &= (aa', cc') \\ &= (a,c)(a',c') \\ &= \varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\varphi\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}.\end{aligned}$$

Επομένως ο φ είναι ομομορφισμός δακτυλίων. Επίσης,

$$\ker\varphi = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : (a,c) = 0\right\} = \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})\right\} = I.$$

Το I ως πυρήνας ομομορφισμού είναι ιδεώδες του R.

(5) Από τον ορισμό του ιδεώδους προκύπτει άμεσα ότι κάθε ιδεώδες του R είναι υποδακτύλιος του R. Το αντίστροφο δεν αληθεύει γενικά. Για παράδειγμα ο υποδακτύλιος $\mathbb{Z}$ του $\mathbb{Q}$ δεν είναι ιδεώδες του $\mathbb{Q}$ καθώς $\frac{1}{2} \in \mathbb{Q}$, $1 \in \mathbb{Z} \Rightarrow \frac{1}{2}1 = \frac{1}{2} \notin \mathbb{Z}$. Για μια άλλη δικαιολόγηση βλ. επόμενη πρόταση.

Πρόταση 5.15. *Έστω R δακτύλιος με μονάδα και I ιδεώδες του R.*
(1) *Ισχύει $I = R$ αν και μόνο αν το I περιέχει αντιστρέψιμο στοιχείο του R.*
(2) *Αν ο R είναι σώμα, τότε $I = R$ ή $I = \{0_R\}$.*

Απόδειξη. (1) Πράγματι, αν $a \in I$ και $a \in U(R)$, τότε από την ιδιότητα (3) του Ορισμού 5.13 έχουμε $a^{-1}a \in I \Rightarrow 1_R \in I$. Άρα για κάθε $r \in R$ έχουμε $r = r1_R \in I$, δηλαδή $R \subseteq I$ οπότε $I = R$. Αντίστροφα, αν $I = R$, τότε $1_R \in I$.
(2) Άμεσο από το (1) καθώς κάθε μη μηδενικό στοιχείο σώματος είναι αντιστρέψιμο. □

Παράδειγμα 5.16. Έστω F σώμα με 16 στοιχεία και R δακτύλιος με 4 στοιχεία. Βρείτε όλους τους ομομορφισμούς δακτυλίων $F \to R$.

Έστω $\varphi : F \to R$ ομομορφισμός δακτυλίων. Το $\ker\varphi$ είναι ιδεώδες του F που είναι σώμα. Από την Πρόταση 5.15 έχουμε ότι $\ker\varphi = \{0\}$ ή $\ker\varphi = F$. Στην πρώτη περίπτωση έπεται ότι η απεικόνιση φ είναι 1-1 σύμφωνα με την Πρόταση 5.11. Αυτό είναι αδύνατο καθώς $|F| > |R|$. Άρα $\ker\varphi = F$ και ο φ είναι ο μηδενικός ομομορφισμός.

Κύρια ιδεώδη

Τα ακόλουθα ιδεώδη έχουν ιδιαίτερα απλή μορφή.

Ορισμός 5.17. *Έστω R μεταθετικός δακτύλιος με μονάδα 1_R και έστω $a \in R$. Το σύνολο $< a >= \{ra : r \in R\}$ καλείται το **κύριο ιδεώδες** του R που παράγεται από το a.*

Παρατηρήσεις.

(1) Έχουμε $0_R \in < a >$ (αφού $0_R = 0_R a$) και $a \in < a >$ (αφού $a = 1_R a$).
(2) Το $< a >$ είναι πράγματι ιδεώδες καθώς:
  i) $< a > \neq \emptyset$.
  ii) Αν $ra, sa \in < a >$ $(r, s \in R)$, τότε $ra - sa = (r-s)a \in < a >$.
  iii) Ο R είναι μεταθετικός και αν $ra \in < a >$ και $r' \in R$, τότε $r'(ra) = (r'r)a \in < a >$.
(3) Έστω $a, b \in R$. Τότε $< a > \subseteq < b > \Leftrightarrow$ υπάρχει $r \in R$ με $a = rb$.
  Πράγματι, αν $< a > \subseteq < b >$, τότε $a \in < a > = < b >$, οπότε $a = rb$ για κάποιο $r \in R$. Αντίστροφα, αν $a = rb$ για κάποιο $r \in R$, τότε κάθε στοιχείο του $< a >$ είναι της μορφής της μορφής $r'a = r'(rb) = (r'r)b \in < b >$.

Παραδείγματα 5.18.

(1) Έστω $R = \mathbb{Z}$ και $a \in \mathbb{Z}$. Τότε

$$< a >= \{ra \in \mathbb{Z} : r \in \mathbb{Z}\} = \{\cdots, -2a, -a, 0, a, 2a, \cdots\}.$$

Σημειώνουμε ότι αν $a, b \in \mathbb{Z}$, τότε $< a > \subseteq < b > \Leftrightarrow b|a$.

(2) Έστω F σώμα και $f(x) \in F[x]$. Τότε

$$< f(x) >= \{g(x)f(x) : g(x) \in F[x]\}.$$

Σημειώνουμε ότι αν $f(x), g(x) \in F[x]$, τότε $< f(x) > \subseteq < g(x) > \Leftrightarrow g(x)|f(x)$.

(3) Έστω $R = \mathbb{Z}_8$ και $a, b, c, d \in \mathbb{Z}_8$, όπου $a = [2], b = [3], c = [4], d = [6]$. Τότε

$$< a >= \{[0], [2], [4], [6]\},$$
$$< b >= \{[0], [3], [6], [9], [12], [15], [18], [21]\} = \mathbb{Z}_8,$$
$$< c >= \{[0], [4]\},$$
$$< d >= \{[0], [6], [12], [18]\} =< a > .$$

Θεώρημα 5.19. *Κάθε ιδεώδες του $\mathbb{Z}$ και κάθε ιδεώδες του $F[x]$, όπου F σώμα, είναι κύριο.*

Απόδειξη. Ας δούμε πρώτα την περίπτωση του δακτυλίου $F[x]$. Έστω I ιδεώδες του $F[x]$. Αν $I = \{0\}$, τότε $I =< 0 >$. Έστω $I \neq \{0\}$. Τότε υπάρχει $f(x) \in I$, ώστε $f(x) \neq 0$. Θεωρούμε ένα τέτοιο $f(x)$ με $\deg f(x)$ ελάχιστο. Θα δείξουμε ότι $I =< f(x) >$.

Πράγματι ο εγκλεισμός $< f(x) > \subseteq I$ είναι σαφής, αφού $g(x)f(x) \in I$ για κάθε $g(x) \in F[x]$, γιατί το I είναι ιδεώδες και $f(x) \in I$.

Έστω $g(x) \in I$. Από τον Ευκλείδεια διαίρεση υπάρχουν $q(x), r(x) \in F[x]$ ώστε

$$g(x) = q(x)f(x) + r(x), \ \ \deg r(x) < \deg f(x).$$

Τότε

$$r(x) = g(x) - q(x)f(x) \in I,$$

διότι χρησιμοποιώντας ότι το I είναι ιδεώδες έχουμε

$$g(x), f(x) \in I \Rightarrow g(x), q(x)f(x) \in I \Rightarrow g(x) - q(x)f(x) \in I.$$

Αν $r(x) \neq 0$ τότε αφού $\deg r(x) < \deg f(x)$ και $r(x) \in I$ έχουμε άτοπο. Άρα

$$g(x) = q(x)f(x) \in I.$$

Άρα $I \subseteq < f(x) >$ και $I =< f(x) >$.

Έστω τώρα I ιδεώδες του $\mathbb{Z}$. Αν $I = \{0\}$, τότε $I =< 0 >= 0\mathbb{Z}$ κύριο ιδεώδες. Έστω $I \neq \{0\}$ και $a \neq 0$, $a \in I$. Παρατηρούμε ότι $0 - a = -a \in I$. Επομένως $a, -a \in I$, άρα το I περιέχει κάποιον θετικό ακέραιο. Έστω b ο ελάχιστος θετικός ακέραιος στο I. Θα δείξουμε ότι $I =< b >$.

Πράγματι ο εγκλεισμός $< b > \subseteq I$ είναι σαφής, αφού $rb \in I$ για κάθε $r \in \mathbb{Z}$, γιατί το I είναι ιδεώδες και $b \in I$.

Έστω $c \in I$. Από τον Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ ώστε

$$c = bq + r, \ 0 \leq r < b.$$

Τότε $r = c - bq \in I$, διότι χρησιμοποιώντας ότι το I είναι ιδεώδες έχουμε $c, b \in I \Rightarrow c, bq \in I \Rightarrow c - bq \in I$. Επειδή όμως $r < b$ και ο b είναι ο ελάχιστος θετικός ακέραιος στο I, έπεται ότι $r = 0$. Άρα $c = bq \in I$. Άρα $I \subseteq < b >$ και $I =< b >$. □

Ας δούμε ένα παράδειγμα ιδεώδους μεταθετικού δακτυλίου που δεν είναι κύριο.

Παράδειγμα 5.20. Θεωρούμε το υποσύνολο I του $\mathbb{Z}[x]$ που αποτελείται από τα πολυώνυμα που έχουν άρτιο σταθερό όρο, $I = \{f(x) \in \mathbb{Z}[x] : f(0) \in 2\mathbb{Z}\}$. Το I είναι πράγματι ιδεώδες καθώς:

(1) $0 \in I \Rightarrow I \neq \emptyset$.

(2) $f(x), g(x) \in I \Rightarrow (f-g)(0) = f(0) - g(0) \in 2\mathbb{Z} \Rightarrow f(x) - g(x) \in I$.

(3) $r(x) \in \mathbb{Z}[x], f(x) \in I \Rightarrow (rf)(0) = r(0)f(0) \in 2\mathbb{Z} \Rightarrow r(x)f(x) \in 2\mathbb{Z}$.

Ας υποθέσουμε, για άτοπο, ότι υπάρχει $f(x) \in I$ με $I =< f(x) >$. Επειδή $2 \in I$, υπάρχει $g(x) \in \mathbb{Z}[x]$ με $2 = g(x)f(x)$. Καθώς $g(x), f(x) \in \mathbb{Z}[x]$, συμπεραίνουμε ότι $f(x) = \pm 1$ ή $f(x) = \pm 2$.

Η περίπτωση $f(x) = \pm 1$ δεν ισχύει καθώς $f(0) \notin 2\mathbb{Z}$. Άρα $I =< \pm 2 >$. Από $x \in I =< \pm 2 >$ έπεται ότι υπάρχει $g(x) \in \mathbb{Z}[x]$ με $x = 2g(x)$. Αυτό είναι αδύνατο.

5.4. Κατασκευάζοντας νέα ιδεώδη

Θα ασχοληθούμε εδώ με την τομή, το άθροισμα και το γινόμενο ιδεωδών.

Πρόταση 5.21. *Έστω (J_i) οικογένεια ιδεωδών του δακτυλίου R. Τότε η τομή $\cap_i J_i$ είναι ιδεώδες του R.*

Απόδειξη. Πράγματι, για κάθε i έχουμε $0_R \in J_i$ γιατί το J_i είναι ιδεώδες του R και επομένως $0_R \in \cap_i J_i$. Δηλαδή $\cap_i J_i \neq \emptyset$.

Έστω $a, b \in \cap_i J_i$. Τότε για κάθε i έχουμε $a, b \in J_i$ και άρα $a - b \in J_i$ γιατί το J_i είναι ιδεώδες του R. Συνεπώς $a - b \in \cap_i J_i$.

Έστω τώρα $a \in \cap_i J_i$ και $r \in R$. Τότε αφού J_i ιδεώδες του R για κάθε i, έχουμε $ar, ra \in J_i$. Συνεπώς $ar, ra \in \cap_i J_i$. □

Για παράδειγμα, στο $\mathbb{Z}$ έχουμε $< 4 > \cap < 6 >=< 12 >$ καθώς τα κοινά πολλαπλάσια των 4 και 6 είναι τα πολλαπλάσια του 12.

Έστω R μεταθετικός δακτύλιος με μονάδα και X μη κενό υποσύνολο του R. Θέτουμε

$$< X >= \{r_1x_1 + ... + r_nx_n : n \in \mathbb{Z}_{>0}, r_i \in R, x_i \in X\}$$

Δηλαδή κάθε στοιχείο του συνόλου $< X >$ είναι ένα άθροισμα, με οποιοδήποτε πεπερασμένο πλήθος παραγόντων, στοιχείων της μορφής r_ix_i, όπου $r_i \in R, x_i \in X$. Χρησιμοποιώντας τον Ορισμό 5.13, εύκολα επαληθεύεται ότι το $< X >$ είναι πράγματι ιδεώδες του R (άσκηση).

Στην ειδική περίπτωση που το X έχει ένα στοιχείο $X = \{a\}$, τότε το $< X >$ είναι το κύριο ιδεώδες $< a >$. Αν το $X = \{x_1, ..., x_m\}$ είναι πεπερασμένο σύνολο, μπορούμε να χρησιμοποιούμε το συμβολισμό $< x_1, ..., x_m >=< X >$.

Πρόταση 5.22. *Έστω R μεταθετικός δακτύλιος με μονάδα και $X \subseteq R, X \neq \emptyset$. Τότε*

$$< X >= \bigcap_{X \subseteq J \trianglelefteq R} J$$

όπου το J διατρέχει τα ιδεώδη του R που περιέχουν το X.

Απόδειξη. Για κάθε J στο δεξί μέλος έχουμε $X \subseteq J$ και άρα $< X >\subseteq J$, γιατί το J είναι ιδεώδες. Άρα το $< X >$ περιέχεται στο δεξί μέλος.
Αντίστροφα, ένα από τα J στο δεξί μέλος είναι το $< X >$. Άρα το δεξί μέλος περιέχεται στο $< X >$. □

Σύμφωνα με την προηγούμενη Πρόταση, το $< X >$ είναι το μικρότερο ιδεώδες του R που περιέχει το σύνολο X.

Είδαμε πριν ότι η τομή ιδεωδών του R είναι ιδεώδες του R. Γενικά η ένωση ιδεωδών δεν είναι ιδεώδες. Για παράδειγμα, στο δακτύλιο $\mathbb{Z}$ το σύνολο $< 2 > \cup < 3 >$ δεν είναι ιδεώδες καθώς περιέχει τα $2, 3$ αλλά δεν περιέχει το $3 - 2 = 1$.

Ορισμός 5.23. *Έστω I, J ιδεώδη ενός δακτυλίου R. Το ιδεώδες $I + J =< I \cup J >$ του R καλείται το* ***άθροισμα*** *των I και J.*

Σημειώνουμε ότι $I \subseteq I + J$ και $J \subseteq I + J$. Μάλιστα, το $I + J$ είναι το μικρότερο ιδεώδες που R που περιέχει τα ιδεώδη I και J.

Πρόταση 5.24. *Έστω R δακτύλιος και I, J ιδεώδη του R. Τότε*

$$I + J = \{a + b \in R : a \in I, b \in J\}.$$

Απόδειξη. Αποδεικνύουμε αρχικά ότι το δεξιό μέλος, έστω K, είναι ιδεώδες του R. Έχουμε $K \neq \emptyset$ αφού $0_R = 0_R + 0_R \in K$. Έστω $a, a' \in I$ και $b, b' \in J$. Τότε

$$a + b - (a' + b') = (a - a') + (b - b') \in I + J,$$

αφού I, J ιδεώδη και συνεπώς $a - a' \in I,\ b - b' \in J$. Έστω $r \in R, a \in I$ και $b \in I$. Επειδή I, J ιδεώδη έχουμε $ra \in I$ και $rb \in J$. Άρα

$$r(a + b) = ra + rb \in I + J.$$

Ομοίως αποδεικνύεται ότι $(a + b)r \in I + J$.

Έχοντας αποδείξει ότι το K είναι ιδεώδες (που περιέχει το $I \cup J$), από τον ορισμό του $I + J$ έπεται ότι $I + J \subseteq K$. Επειδή το K περιέχεται σε κάθε ιδεώδες του R που περιέχει το σύνολο $I \cup J$, έχουμε $I + J \supseteq K$. Άρα $I + J = K$. □

Ορισμός 5.25. *Έστω I, J ιδεώδη δακτυλίου R. Το* ***γινόμενο*** *των I και J είναι το ιδεώδες*

$$IJ = \{a_1b_1 + ... + a_nb_n : n \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J\}.$$

Το IJ είναι πράγματι ιδεώδες καθώς:

(1) $0 = 0 \cdot 0 \in IJ$.

(2) Έστω $x, y \in I$, οπότε $x = a_1b_1 + ... + a_nb_n,\ y = a'_1b'_1 + ... + a'_mb'_m$, όπου $a_i, a'_j \in I$ και $b_i, b'_j \in J$. Τότε

$$x - y = a_1b_1 + ... + a_nb_n + (-a'_1)b'_1 + ... + (-a'_m)b'_m \in IJ.$$

(3) Για κάθε $r \in R$ έχουμε

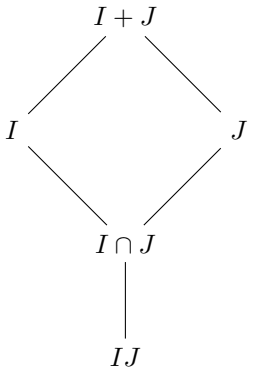
$$rx = r(a_1b_1 + ... + a_nb_n) = (ra_1)b_1 + ... + (ra_n)b_n \in IJ$$

και επίσης $xr = a_1(b_1r) + ... + a_n(b_nr) \in IJ$, αφού $ra_i \in I$ και $b_jr \in J$ καθώς τα I, J είναι ιδεώδη.

Παρατηρήσεις.

(1) Σχετικά με τον Ορισμό 5.25, τονίζουμε ότι αν I, J είναι ιδεώδη του R, τότε γενικά το σύνολο $\{ab : a \in I, b \in J\}$ δεν είναι ιδεώδες του R. Ένα συγκεκριμένο παράδειγμα είναι το ιδεώδες I του $\mathbb{Z}[x]$ στο Παράδειγμα 5.20. Βλ. σχετικά την άσκηση 5.5.6. Στο παράδειγμα αυτό θα αναφερθούμε αρκετές φορές παρακάτω - όλοι έχουμε τις αδυναμίες μας.

(2) Στο ακόλουθο διάγραμμα φαίνονται οι σχέσεις περιέχεσθαι μεταξύ των διαφόρων ιδεωδών που ορίσαμε: Όταν δύο κορυφές του διαγράμματος συνδέονται με μια ακμή, το κάτω ιδεώδες περιέχεται στο πάνω. Για παράδειγμα έχουμε $IJ \subseteq I \cap J$ και $I \cap J \subseteq I$.



Παραδείγματα 5.26.

(1) Έστω $m,n\in\mathbb{Z}$, $d=\mu\kappa\delta(m,n)$ και $e=\varepsilon\kappa\pi(m,n)$. Τότε
i) $< m > \cap < n >=< e >$,
ii) $< m > + < n >=< d >$,
iii) $< m >< n >=< mn >$.

Απόδειξη. i) Επειδή $m|e$ και $n|e$ έχουμε $< e >\subseteq< m >$ και $< e >\subseteq< n >$. Άρα $< e >\subseteq< m > \cap < n >$. Επειδή κάθε στοιχείο του $< m > \cap < n >$ είναι πολλαπλάσιο και του m και του n, θα είναι πολλαπλάσιο του e, δηλαδή θα ανήκει στο $< e >$. Άρα $< m > \cap < n >\subseteq< e >$. Συνεπώς $< m > \cap < n >=< e >$.

ii) Επειδή $d|m$ και $d|n$ έχουμε $< m >\subseteq< d >$ και $< n >\subseteq< d >$. Καθώς το $< d >$ είναι ιδεώδες, παίρνουμε

$$< m > + < n >\subseteq< d > .$$

Από το Θεώρημα 1.9 υπάρχουν ακέραιοι a,b με $d=am+bn$, οπότε από την Πρόταση 5.24 (ή 5.23) παίρνουμε $d\in< m > + < n >$. Από αυτό έπεται ότι

$$< d >\subseteq< m > + < n >$$

γιατί το $< m > + < n >$ είναι ιδεώδες. Άρα έχουμε ισότητα.

iii) Από τον ορισμό του γινομένου ιδεωδών, έπεται ότι κάθε στοιχείο του $< m >< n >$ είναι πολλαπλάσιο του mn, οπότε $< m >< n >\subseteq< mn >$. Αντίστροφα, κάθε στοιχείο του $< mn >$ είναι της μορφής

$$r(mn)=(rm)n\in< m >< n >,$$

οπότε $< mn >\subseteq< m >< n >$ και έχουμε ισότητα. □

(2) Έστω F σώμα, $f(x),g(x)\in F[x]$, $d(x)=\mu\kappa\delta(f(x),g(x))$ και $e(x)=\varepsilon\kappa\pi(f(x),g(x))$. Τότε
i) $< f(x) > \cap < g(x) >=< e(x) >$,
ii) $< f(x) > + < g(x) >=< d(x) >$.
iii) $< f(x) >< g(x) >=< f(x)g(x) >$.
Η απόδειξη είναι παρόμοια με το (1) και παραλείπεται.

(3) Έστω $X=\{2,x\}\subseteq\mathbb{Z}[x]$. Τότε $< 2,x >=\{2a(x)+xb(x) : a(x),b(x)\in\mathbb{Z}[x]\}$. Αφήνουμε ως άσκηση την επαλήθευση ότι $< 2,x >=\{f(x)\in\mathbb{Z}[x] : f(0)\in 2\mathbb{Z}\}$, που είναι το μη κύριο ιδεώδες που είδαμε στο Παράδειγμα 5.17.

Κοινές ιδιότητες των δακτυλίων $\mathbb{Z}$ και $F[x]$, όπου F σώμα.

Στα κεφάλαια 1,4,5 είδαμε ότι οι δακτύλιοι των ακεραίων και των πολυωνύμων με συντελεστές από σώμα έχουν αρκετές κοινές ιδιότητες που φαίνονται συνοπτικά στον ακόλουθο πίνακα. Καλό είναι να συγκρίνετε, αν δεν το έχετε κάνει ήδη, τις αποδείξεις αντίστοιχων αποτελεσμάτων.

	$\mathbb{Z}$	$F[x]$
Ευκλείδεια διαίρεση	Θεώρημα 1.6	Θεώρημα 4.11
Μέγιστος κοινός διαιρέτης	Θεώρημα 1.9	Θεώρημα 4.14
Ευκλείδειος αλγόριθμος	Παράγραφος 1.3	Παράγραφος 4.3
Λήμμα του Ευκλείδη	Λήμμα 1.11	Λήμμα 4.15
Αναλύσεις σε γινόμενα	Θεώρημα 1.12	Θεώρημα 4.16
Ιδεώδη	Θεώρημα 5.19	Θεώρημα 5.19
Πράξεις ιδεωδών	Παράδειγμα 5.26(1)	Παράδειγμα 5.26(2)

Ακολουθεί διαφήμιση. Η αιτία των κοινών ιδιοτήτων στους $\mathbb{Z}$ και $F[x]$ είναι η ύπαρξη Ευκλείδειας διαίρεσης. Περιοχές που είναι εφοδιασμένες με μια Ευκλείδεια διαίρεση΄ είναι γνωστές ως Ευκλείδειες περιοχές. Για παράδειγμα αποδεικνύεται ότι ο δακτύλιος των ακεραίων του Gauss $\mathbb{Z}[i]$ είναι Ευκλείδεια περιοχή. Περισσότερα για αυτές μπορείτε να δείτε στο μάθημα Δακτύλιοι και Πρότυπα.

Ασκήσεις Κεφαλαίου 5

Ομάδα1: 1-5, 22, 23.
Ομάδα2: 6-17, 19-21, 24-28, 30, 33.
Ομάδα3: 18, 29,31, 32.

1. Αποδείξτε ότι η αντιστοιχία $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_4$, $\varphi([a]_{12}) = [a]_4$ είναι απεικόνιση και μάλιστα επιμορφισμός δακτυλίων. Να βρεθεί ο $\ker \varphi$.
2. Για ποια $n > 1$ η απεικόνιση
$$\varphi : \mathbb{Z}_n \to \mathbb{Z}_n, \varphi(a) = 2a$$
είναι ομομορφισμός δακτυλίων; Ίδιο ερώτημα για την απεικόνιση
$$\psi : \mathbb{Z}_n \to \mathbb{Z}_n, \psi(a) = a^3.$$
3. Θεωρούμε το δακτύλιο $R = M_2(\mathbb{R})$.
   i) Δείξτε ότι η απεικόνιση $\varphi : R \to R, \varphi(A) = A^t$ (ο ανάστροφος του A), δεν είναι ομομορφισμός δακτυλίων.
   ii) Έστω αντιστρέψιμος $P \in R$. Δείξτε ότι η απεικόνιση $\psi : R \to R, \psi(A) = P^{-1}AP$ είναι ισομορφισμός δακτυλίων.
4. Θεωρούμε το δακτύλιο $T_2(\mathbb{Z})$ των 2×2 άνω τριγωνικών πινάκων με στοιχεία από το $\mathbb{Z}$ και το υποσύνολο $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$. Δείξτε ότι R είναι υποδακτύλιος του $T_2(\mathbb{Z})$ αλλά όχι ιδεώδες. Στη συνέχεια δείξτε ότι $R \simeq \mathbb{Z} \times \mathbb{Z}$.
5. Εξετάστε ποια από τα παρακάτω σύνολα είναι ιδεώδη του $R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$.
   i) $\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in R \right\}$.
   ii) $\left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \in R \right\}$.
   iii) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R \right\}$.
   iv) $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R | b \in 2\mathbb{Z} \right\}$.
6. Στο δακτύλιο $\mathbb{Z}[x]$ θεωρούμε τα ιδεώδη $I = \{f(x) \in \mathbb{Z}[x] : f(0) \in 2\mathbb{Z}\}$ και $J =< 2, x >$.
   i) Δείξτε ότι $I = J$.
   ii) Για το γινόμενο ιδεωδών II δείξτε ότι $II \neq \{ab \in R : a, b \in I\}$.
   iii) Βρείτε όλα τα κύρια ιδεώδη K του $\mathbb{Z}[x]$ με $I \subseteq K$.
7. Δείξτε ότι οι δακτύλιοι $R = \mathbb{Z}[\sqrt{2}]$ και $S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$ είναι ισόμορφοι.
8. Να εξετάσετε αν στα ακόλουθα ζεύγη οι δακτύλιοι είναι ισόμορφοι.
   i) $2\mathbb{Z}$ και $\mathbb{Z}$.
   ii) $\mathbb{C}$ και $\mathbb{R} \times \mathbb{R}$.
   iii) $R = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : a \in \mathbb{Z} \right\}$ και $\mathbb{Z}$.
   iv) $R = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \mathbb{Z} \right\}$ και $\mathbb{Z}$.
   v) $R = \mathbb{Z}[\sqrt{2}]$ και $S = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\}$.
9. Βρείτε όλους τους ισομορφισμούς δακτυλίων $R \to R$ στις ακόλουθες περιπτώσεις.
   i) $R = \mathbb{Q}$.

ii) $R = \mathbb{Q}[\sqrt{2}]$.
iii) $R = \mathbb{Z}[i]$.

10. Βρείτε όλα τα ιδεώδη I του $\mathbb{Z}$ ώστε $20\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$.

11. Βρείτε ένα $f(x) \in \mathbb{R}[x]$ ώστε $< f(x) >= \{g(x) \in \mathbb{R}[x] : g(0) = g(3-4i) = 0\}$.

12. Υπάρχει δακτύλιος R και ομομορφισμός δακτυλίων $\mathbb{R} \to R$ με πυρήνα το $\mathbb{Z}$;

13. $\star$ Έστω R μεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$. Δείξτε ότι ο R είναι σώμα αν και μόνο αν τα μόνα ιδεώδη του R είναι τα R και $\{0_R\}$.

14. $\star$ Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Δείξτε ότι για κάθε ιδεώδες J του S, το $\varphi^{-1}(J)$ είναι ιδεώδες του R. Ως εφαρμογή αυτού, δείξτε ότι κάθε ιδεώδες του $\mathbb{Z}_n$ είναι κύριο.

15. Έστω R δακτύλιος με μονάδα. Το κέντρο του R είναι το σύνολο

$$C(R) = \{a \in R : ra = ar \ \forall r \in R\}.$$

i) Δείξτε ότι το $C(R)$ είναι μεταθετικός υποδακτύλιος του R.
ii) Βρείτε το $C(T_2(\mathbb{Z}))$.
iii) Αληθεύει ότι $C(T_2(R)) \simeq C(R)$;
iv) Δείξτε ότι αν S είναι δακτύλιος με $S \simeq R$, τότε $C(S) \simeq C(R)$

16. Έστω R ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. Αποδείξτε ότι το σύνολο $nil(R)$ των μηδενοδύναμων στοιχείων του R (βλ. άσκηση 3.20) αποτελεί ιδεώδες του R.

17. Έστω R ένας μεταθετικός δακτύλιος και I ένα ιδεώδες του R. Το ριζικό του I είναι το σύνολο $\sqrt{I} = \{r \in R | r^n \in I \text{ για κάποιο } n \geq 1\}$.
i) Αποδείξτε ότι το $\sqrt{I}$ είναι ένα ιδεώδες του R που περιέχει το I.
ii) Έστω $R = \mathbb{Z}$. Να προσδιορίσετε τα $\sqrt{< 3 >}$, $\sqrt{< 12 >}$.
iii) Έστω $R = \mathbb{Z}_n$. Αποδείξτε ότι $\sqrt{< 0 >} =< [p_1 \dots p_r] >$, όπου $n = p_1^{a_1} \dots p_r^{a_r}$ είναι η ανάλυση του n σε γινόμενο διακεκριμένων πρώτων.

18. $\star$ Έστω R, S δακτύλιοι.
i) Δείξτε ότι αν I, J είναι ιδεώδη των R, S αντίστοιχα, τότε το $I \times J$ είναι ιδεώδες του $R \times S$.
ii) Έστω ότι οι R, S έχουν μοναδιαία στοιχεία. Δείξτε ότι κάθε ιδεώδες του $R \times S$ είναι της μορφής $I \times J$, όπου I, J είναι ιδεώδη των R, S αντίστοιχα.

19. Αληθεύει ότι κάθε ιδεώδες του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$ είναι κύριο;

20. Ξέρουμε ότι κάθε υποδακτύλιος του $\mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z}$. Βρείτε υποδακτύλιο του $\mathbb{Z} \times \mathbb{Z}$ που δεν είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$.

21. Δίνονται τα πολυώνυμα $f(x), g(x) \in \mathbb{Z}_3[x], f(x) = x^2 + x + 1, g(x) = x^3 - x$ και το σύνολο

$$I = \{f(x)a(x) + g(x)b(x) \in \mathbb{Z}_3[x] : a(x), b(x) \in \mathbb{Z}_3[x]\}.$$

i) Δείξτε ότι το I είναι ιδεώδες του $\mathbb{Z}_3[x]$ και βρείτε $h(x)$ με $I =< h(x) >$.
ii) Πόσα τέτοια $h(x)$ υπάρχουν;

22. Αποδείξτε με πληρότητα τους ισχυρισμούς στο Παράδειγμα 5.26(2).

23. Αληθεύει ότι κάθε μη μηδενικό ιδεώδες του δακτυλίου $\mathbb{Z}[i]$ περιέχει θετικό ακέραιο;

24. Δείξτε ότι $IJ \subseteq I \cap J$, όπου I, J ιδεώδη δακτυλίου R. Δώστε παράδειγμα που δείχνει ότι δεν ισχύει γενικά η ισότητα.

25. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν. Δικαιολογήστε τις απαντήσεις σας. Έστω I, J, K ιδεώδη δακτυλίου R.
i) $I + J = I \Leftrightarrow J \subseteq I$.
ii) $(I + J)K = IK + JK$.

26. Έστω R, S δακτύλιοι με μονάδες. Δείξτε ότι αν οι R, S είναι ισόμορφοι, τότε οι $R[x], S[x]$ είναι ισόμορφοι.

27. Δίνεται το σύνολο I των πολυωνύμων του $\mathbb{Z}_3[x]$ που έχουν την ιδιότητα
$$\mu\kappa\delta(f(x), x^{18}+1) \neq 1.$$
Αληθεύει ότι το I είναι ιδεώδες του $\mathbb{Z}_3[x]$; Να βρεθεί μη μηδενικό $f(x) \in I$ ελαχίστου βαθμού.

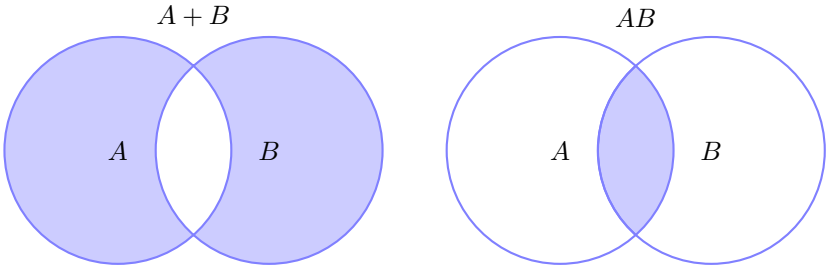
28. Δείξτε ότι αν $\varphi : F \to S$ είναι επιμορφισμός δακτυλίων, όπου F σώμα και S μη μηδενικός δακτύλιος, τότε ο S είναι σώμα.

29. Αληθεύει ότι οι δακτύλιοι $\mathbb{Z} \times \mathbb{Z}$ και $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ είναι ισόμορφοι;

30. Έστω $n > 1$. Συμπληρώστε και αποδείξτε την πρόταση: Όλα τα μη αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$ αποτελούν ιδεώδες του $\mathbb{Z}_n$ αν και μόνο αν ο n είναι ....

31. ≀ Δείξτε ότι τα μόνα ιδεώδη του δακτυλίου $M_2(\mathbb{Q})$ είναι το μηδενικό και το $M_2(\mathbb{Q})$.

32. *Δακτύλιος του Boole* Έστω X μη κενό σύνολο και $P(X)$ σύνολο των υποσυνόλων του X. Θεωρούμε τις πράξεις στο $P(X)$ που ορίζονται από
$$A + B = A \cup B - A \cap B,$$
$$AB = A \cap B.$$



   i) Δείξτε ότι το σύνολο $P(X)$ με τις παραπάνω πράξεις είναι μεταθετικός δακτύλιος με μονάδα τέτοιος ώστε $2A = 0_{P(X)}$ για κάθε $A \in P(X)$.
   ii) ≀ Δείξτε ότι αν το σύνολο X είναι πεπερασμένο με n στοιχεία, τότε ο δακτύλιος $P(X)$ είναι ισόμορφος με το $\underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n \text{ φορές}}$.

33. Έστω m, n σχετικά πρώτοι ακέραιοι.
   i) Έστω R δακτύλιος τέτοιος ώστε υπάρχουν $a, b \in R$ με $ma = nb = 0$. Δείξτε ότι $ab = 0$.
   ii) Αληθεύει ότι υπάρχει περιοχή που περιέχει υποδακτύλιους R_1, R_2 με $R_1 \simeq \mathbb{Z}_m, R_2 \simeq \mathbb{Z}_n$;

34. Σε ποιον από τους δακτυλίους (rings)
$$\mathbb{Z},\ \mathbb{Z}_n,\ \mathbb{Z}[i],\ \mathbb{Z}[\sqrt{2}],\ \mathbb{Q},\ \mathbb{Q}[\sqrt{2}],\ \mathbb{R},\ \mathbb{C},\ \mathbb{C}[x],\ M_n(\mathbb{Z})$$
θα δίνατε τον τίτλο του Lord ; Δείτε την επιλογή ενός πρωτεργάτη μαθηματικού στο σύνδεσμο Kronecker.

Υποδείξεις Ασκήσεων Κεφαλαίου 5

1. *Λύση.* Αν $[a]_{12} = [b]_{12}$, τότε $12|a-b$, οπότε $4|a-b$ και επομένως $[a]_4 = [b]_4$. Συνεπώς η φ είναι απεικόνιση. Για κάθε $[a]_{12}, [b]_{12} \in \mathbb{Z}_{12}$ είναι
   - $\varphi([a]_{12} + [b]_{12}) = \varphi([a+b]_{12}) = [a+b]_4 = [a]_4 + [b]_4 = \varphi([a]_{12}) + \varphi([b]_{12})$,
   - $\varphi([a]_{12}[b]_{12}) = \varphi([ab]_{12}) = [ab]_4 = [a]_4[b]_4 = \varphi([a]_{12})\varphi([b]_{12})$.

   Έχουμε
   $$\varphi([a]_{12}) = [0]_4 \Leftrightarrow [a]_4 = [0]_4 \Leftrightarrow 4|a \Leftrightarrow [a]_{12} \in < [4]_{12} > .$$
   Άρα $\ker\varphi = < [4]_{12} >$, το κύριο ιδεώδες του $\mathbb{Z}_{12}$ που παράγεται από το $[4]_{12}$.

2. *Λύση.* Είναι σαφές ότι $\varphi(a+b) = 2(a+b) = \varphi(a) + \varphi(b)$ για κάθε $a, b \in \mathbb{Z}_n$. Παρατηρούμε ότι
   $$\varphi([1][1]) = \varphi([1])\varphi([1]) \Rightarrow [2] = [4] \Rightarrow n|2 \Rightarrow n = 2.$$
   Από τα παραπάνω συνάγεται ότι αναγκαία συνθήκη για να είναι η φ ομομορφισμός δακτυλίων, είναι $n = 2$. Άμεσα επαληθεύεται ότι για $n = 2$ η φ είναι ομομορφισμός.

   Για την ψ έχουμε $\psi(ab) = (ab)^3 = a^3b^3 = \psi(a)\psi(b)$ για κάθε $a, b \in \mathbb{Z}_n$, όπου στη δεύτερη ισότητα χρησιμοποιήσαμε ότι ο $\mathbb{Z}_n$ είναι μεταθετικός. Παρατηρούμε ότι
   $$\psi([1] + [1]) = \psi([1]) + \psi([1]) \Rightarrow [8] = [2] \Rightarrow n|6 \Rightarrow n = 2, 3, 6.$$
   Για καθεμία από τις περιπτώσεις $n = 2, 3, 6$ εύκολα επαληθεύεται με πράξεις ότι η ψ είναι ομομορφισμός.

   Σημείωση. Σε περίπτωση που δεν το έχετε προσέξει, η περίπτωση $n = 6$ για την απεικόνιση ψ προκύπτει από το Παράδειγμα 4.21(1) [και η περίπτωση $n = 3$ είναι ένα από τα όνειρα του πρωτοετή].

3. *Λύση.* i) Έστω $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ και $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Τότε έχουμε
   $$\varphi(AB) = (AB)^t = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^t = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \text{ και}$$
   $$\varphi(A)\varphi(B) = A^tB^t = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$
   Άρα $\varphi(AB) \neq \varphi(A)\psi(B)$ και η φ δεν είναι ομομορφισμός δακτυλίων.

   ii) Έστω $A, B \in R$. Υπολογίζουμε
   $$\psi(A+B) = P^{-1}(A+B)P = P^{-1}AP + P^{-1}BP = \psi(A) + \psi(B), \text{ και}$$
   $$\psi(AB) = P^{-1}ABP = P^{-1}APP^{-1}BP = \psi(A)\psi(B).$$
   Παρατηρούμε ότι ο ομομορφισμός ψ έχει τετριμμένο πυρήνα γιατί αν $\psi(A) = 0$, τότε $P^{-1}AP = 0 \Rightarrow A = P0P^{-1} = 0$. Άρα ο ψ είναι 1-1. Η ψ είναι επί γιατί αν $B \in R$, τότε
   $$\psi(PBP^{-1}) = P^{-1}PBP^{-1}P = B.$$

4. *Λύση.* Έχουμε $R \neq \emptyset$. Παρατηρούμε ότι αν $a, b, x, y \in \mathbb{Z}$, τότε
   $$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} - \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} a-x & 0 \\ 0 & b-y \end{pmatrix} \in R, \text{ και}$$
   $$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} ax & 0 \\ 0 & by \end{pmatrix} \in R.$$
   Επομένως ο R είναι υποδακτύλιος του $T_2(\mathbb{Z})$.

   Το σύνολο R δεν είναι ιδεώδες του $T_2(\mathbb{Z})$ γιατί είναι γνήσιο υποσύνολο του $T_2(\mathbb{Z})$ και περιέχει τη μονάδα του $T_2(\mathbb{Z})$. (Αν ένα ιδεώδες περιέχει αντιστρέψιμο στοιχείο του δακτυλίου, τότε ισούται με το δακτύλιο, βλ Πρόταση 5.15).

Ορίζουμε $\varphi : R \to \mathbb{Z} \times \mathbb{Z}$, $\varphi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = (a, b)$. Θα δείξουμε ότι η φ είναι ομομορφισμός. Πράγματι, έστω $A_1 = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \in R$ και $A_2 = \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \in R$. Τότε

$$\begin{aligned}
\varphi(A_1 + A_2) &= \varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}\right) \\
&= \varphi \begin{pmatrix} a_1 + a_2 & 0 \\ 0 & b_1 + b_2 \end{pmatrix} \\
&= (a_1 + a_2, b_1 + b_2) \\
&= (a_1, b_1) + (a_2, b_2) \\
&= \varphi \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + \varphi \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \\
&= \varphi(A_1) + \varphi(A_2), \text{ και} \\
\varphi(A_1 A_2) &= \varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix}\right) \\
&= \varphi \begin{pmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{pmatrix} \\
&= (a_1 a_2, b_1 b_2) \\
&= (a, b_1)(a_2, b_2) \\
&= \varphi \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \varphi \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} \\
&= \varphi(A_1)\varphi(A_2).
\end{aligned}$$

Θα δείξουμε τώρα ότι η φ είναι 1-1. Έχουμε

$$\varphi(A_1) = \varphi(A_2) \Rightarrow (a_1, b_1) = (a_2, b_2) \Rightarrow a_1 = a_2, b_1 = b_2 \Rightarrow A_1 = A_2.$$

Τέλος, η φ είναι επί καθώς αν $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, τότε $\varphi \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = (x, y)$. Τελικά $R \simeq \mathbb{Z} \times \mathbb{Z}$.

5. *Λύση.* (i) Είδαμε στο Παράδειγμα 5.14(4) ότι το J_1 είναι ιδεώδες του R.

(ii) Είναι φανερό ότι το J_2 είναι μη κενό.Για κάθε $a, b, x, y, z \in \mathbb{Z}$ έχουμε

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a - x & b - y \\ 0 & 0 \end{pmatrix} \in J_2,$$

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & 0 \end{pmatrix} \in J_2, \text{ και}$$

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ax & bx \\ 0 & 0 \end{pmatrix} \in J_2.$$

Άρα το J_2 είναι ιδεώδες του R.

(iii) Είναι ιδεώδες και η απόδειξη είναι παρόμοια με το (ii) .

(iv) Το υποσύνολο J_4 του R είναι γνήσιο, για παράδειγμα $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin R$. Περιέχει τη μονάδα $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ του R, οπότε αν το J_4 ήταν ιδεώδες του R, θα ήταν $J_4 = R$, αδύνατο.

6. *Λύση.* i) Επειδή $2, x \in I$ και το I είναι ιδεώδες, ισχύει ότι $J =< 2, x > \subseteq I$. Αντίστροφα, αν $f(x) \in I$, τότε από τον ορισμό του I υπάρχουν ακέραιοι a_i με

$$f(x) = a_n x^n + ... + a_1 x + 2a_0 = (a_n x^{n-1} + ... + a_1)x + 2a_0 \in < x, 2 >= J.$$

ii) Θεωρούμε το πολυώνυμο $f(x) = x^2 + 4$. Είναι σαφές ότι $f(x) \in II$. Θα δείξουμε ότι

$$f(x) \notin \{ab \in \mathbb{Z}[x] : a, b \in I\}.$$

Έστω $f(x) = ab$ με $a, b \in \mathbb{Z}[x]$. Επειδή τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[x]$ είναι τα ± 1 και το $f(x)$ είναι μονικό, μπορούνε να υποθέσουμε ότι τα a, b είναι μονικά και επιπλέουν είναι θετικού βαθμού. Άρα το $f(x)$ δεν θα ήταν ανάγωγο στο $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, πράγμα αδύνατο καθώς είναι βαθμού 2 και δεν έχει ρίζα στο σώμα $\mathbb{Q}$. Βλέπε Πρόταση 5.19(2).

7. *Λύση.* Ορίζουμε $\varphi : \mathbb{Z}[\sqrt{2}] \to S$ με $\varphi(a + b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$. Έστω $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Τότε έχουμε,

$$\begin{aligned} \varphi\Big((a + b\sqrt{2}) + (c + d\sqrt{2})\Big) &= \varphi\Big((a + c) + (b + d\sqrt{2})\Big) \\ &= \begin{pmatrix} a + c & b + d \\ 2(b + d) & a + c \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} c & d \\ 2d & c \end{pmatrix} \\ &= \varphi(a + b\sqrt{2}) + \varphi(c + d\sqrt{2}). \end{aligned}$$

Επίσης,

$$\begin{aligned} \varphi\Big((a + b\sqrt{2})(c + d\sqrt{2})\Big) &= \varphi\Big((ac + 2bd) + (ad + bc)\sqrt{2}\Big) \\ &= \begin{pmatrix} ac + 2bd & ad + bc \\ 2(ad + bc) & ac + 2bd \end{pmatrix}, \text{ και} \end{aligned}$$

$$\varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\begin{pmatrix} c & d \\ 2d & c \end{pmatrix} = \begin{pmatrix} ac + 2bd & ad + bc \\ 2(ad + bc) & ac + 2bd \end{pmatrix}.$$

Επομένως $\varphi\big((a + b\sqrt{2})(c + d\sqrt{2})\big) = \varphi(a + b\sqrt{2})\varphi(c + d\sqrt{2})$. Παρατηρούμε ότι

$$\begin{aligned} \ker\varphi &= \left\{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\} \\ &= \Big\{a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a = 0,\ b = 0\Big\} = \{0\}. \end{aligned}$$

Επομένως η φ είναι 1-1. Τέλος είναι σαφές ότι η φ είναι επί.

8. *Λύση.* i) Έστω $\varphi : \mathbb{Z} \to 2\mathbb{Z}$ ισομορφισμός. Αφού ο $\mathbb{Z}$ έχει μονάδα και ο φ είναι επιμορφισμός, τότε και ο $2\mathbb{Z}$ έχει μονάδα, άτοπο. Επομένως $\mathbb{Z} \ncong 2\mathbb{Z}$.

ii) Το $\mathbb{C}$ είναι περιοχή, ενώ το $\mathbb{R} \times \mathbb{R}$ δεν είναι. Πράγματι,

$$(1, 0)(0, 1) = (0, 0),$$

όπου $(1, 0) \neq (0, 0)$ και $(0, 1) \neq (0, 0)$. Άρα $\mathbb{C} \ncong \mathbb{R} \times \mathbb{R}$.

iii) Θα δείξουμε ότι $R \simeq \mathbb{Z}$. Ορίζουμε $\varphi : R \to \mathbb{Z}$ με $\varphi\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$. Παρατηρούμε ότι

$$\begin{aligned} \varphi\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right) &= \varphi\begin{pmatrix} a + b & 0 \\ 0 & 0 \end{pmatrix} \\ &= a + b = \varphi\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \varphi\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}, \text{ και} \end{aligned}$$

$$\varphi\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right) = \varphi\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = ab = \varphi\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\varphi\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}.$$

Άρα η φ είναι ομομορφισμός δακτυλίων. Είναι σαφές ότι είναι 1-1 και επί.

iv) Ο $\mathbb{Z}$ είναι περιοχή, ενώ το R δεν είναι αφού $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Επομένως $R \ncong \mathbb{Z}$.

v) Οι δακτύλιοι R και S δεν είναι ισόμορφοι καθώς ο πρώτος είναι περιοχή ενώ ο δεύτερος δεν είναι αφού $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,και οι δύο πίνακες στο αριστερό μέλος είναι μη μηδενικοί.

9. Λύση. i) Επειδή ο φ είναι ισομορφισμός, $\varphi(1)=1$. Έχουμε
$$\varphi(\frac{m}{n})=\varphi(m\frac{1}{n})=m\varphi(\frac{1}{n})=\frac{m}{n}n\varphi(\frac{1}{n})=\frac{m}{n}\varphi(n\frac{1}{n})=\frac{m}{n}\varphi(1)=\frac{m}{n},$$
για κάθε $m,n\in\mathbb{Z}, n\neq 0$. Συνεπώς ο μόνος ισομορφισμός $\mathbb{Q}\to\mathbb{Q}$ είναι ο ταυτοτικός.

ii) Έστω $\varphi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}[\sqrt{2}]$ ισομορφισμός. Ακριβώς με το επιχείρημα της προηγούμενης περίπτωσης έπεται ότι $\varphi(a)=a$ για κάθε $a\in\mathbb{Q}$. Επειδή κάθε στοιχείο του $\mathbb{Q}[\sqrt{2}]$ είναι της μορφής $a+b\sqrt{2}$, όπου $a,b\in\mathbb{Q}$, και ισχύει ότι
$$\varphi(a+b\sqrt{2})=\varphi(a)+\varphi(b)\varphi(\sqrt{2})=a+b\varphi(\sqrt{2}),$$
συμπεραίνουμε ότι ο ισομορφισμός φ καθορίζεται από την εικόνα $\varphi(\sqrt{2})$ του $\sqrt{2}$. Από τη σχέση $(\sqrt{2})^2=2$ έχουμε
$$\varphi((\sqrt{2})^2)=\varphi(2)\Rightarrow(\varphi(\sqrt{2}))^2=2\Rightarrow\varphi(\sqrt{2})=\pm\sqrt{2}.$$
• Αν $\varphi(\sqrt{2})=\sqrt{2}$, τότε η απεικόνιση φ είναι η ταυτοτική
$$\varphi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}[\sqrt{2}], a+b\sqrt{2}\mapsto a+b\sqrt{2},$$
που προφανώς είναι ισομορφισμός.

• Αν $\varphi(\sqrt{2})=-\sqrt{2}$, τότε η απεικόνιση φ είναι
$$\varphi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}[\sqrt{2}], a+b\sqrt{2}\mapsto a-b\sqrt{2}.$$
Εύκολα αποδεικνύεται ότι η απεικόνιση αυτή είναι ισομορφισμός, όπως στο Παράδειγμα 5.2(4).

iii) Έστω $\varphi:\mathbb{Z}[i]\to\mathbb{Z}[i]$ ισομορφισμός. Έχουμε $\varphi(a)=\varphi(a1)=a\varphi(1)=a1=a$ για κάθε $a\in\mathbb{Z}$. Επειδή κάθε στοιχείο του $\mathbb{Z}[i]$ είναι της μορφής $a+bi$, όπου $a,b\in\mathbb{Z}$, και ισχύει ότι
$$\varphi(a+bi)=\varphi(a)+\varphi(b)\varphi(i)=a+b\varphi(i),$$
συμπεραίνουμε ότι ο ισομορφισμός φ καθορίζεται από την εικόνα $\varphi(i)$ του i. Από τη σχέση $i^2=-1$ έχουμε
$$\varphi(i^2)=\varphi(-1)\Rightarrow(\varphi(i))^2=-1\Rightarrow\varphi(i)=\pm i.$$
• Αν $\varphi(i)=i$, τότε η απεικόνιση φ είναι η ταυτοτική $\varphi:\mathbb{Z}[i]\to\mathbb{Z}[i], a+bi\mapsto a+bi$, που προφανώς είναι ισομορφισμός.

• Αν $\varphi(i)=-i$, τότε η απεικόνιση φ είναι $\varphi:\mathbb{Z}[i]\to\mathbb{Z}[i], a+bi\mapsto a-bi$. Εύκολα αποδεικνύεται ότι η απεικόνιση αυτή είναι ισομορφισμός, όπως στο Παράδειγμα 5.2(4).

10. *Λύση.* Από το Θεώρημα 5.19, κάθε ιδεώδες I του $\mathbb{Z}$ είναι κύριο, δηλαδή της μορφής $I=<m>, m\in\mathbb{Z}$. Έχουμε
$$\begin{aligned}20\mathbb{Z}\subseteq I\subseteq 2\mathbb{Z} &\Leftrightarrow <20>\subseteq<m>\subseteq<2>\\ &\Leftrightarrow <20>\subseteq<m> \quad \text{και} \quad <m>\subseteq<2>\\ &\Leftrightarrow m|20 \quad \text{και} \quad 2|m.\end{aligned}$$
Επομένως ζητάμε τους άρτιους διαιρέτες του 20, άρα $m=\pm2,\pm4,\pm10,\pm20$. Επειδή για κάθε ακέραιο m έχουμε $<m>=<-m>$, τα ζητούμενα ιδεώδη είναι τα
$$I=<2>,<4>,<10>,<20>.$$

11. *Λύση.* Έστω $g(x)\in\mathbb{R}[x]$ τέτοιο ώστε $g(0)=g(3-4i)=0$. Τότε $g(0)=0\Rightarrow x|g(x)$ και
$$\begin{aligned}g(3-4i)=0\Rightarrow g(3+4i)=0 &\quad (\text{αφού έχουμε πραγματικούς συντελεστές})\\ &\Rightarrow x-(3-4i)|g(x) \quad \text{και} \quad x-(3+4i)|g(x) \ \text{ στο } \ \mathbb{C}[x].\end{aligned}$$
Όμως επειδή $\text{μκδ}(x-3+4i, x-3-4i)=1$, έπεται ότι
$$(x-(3-4i))(x-(3+4i))|g(x) \ \text{ στο } \ \mathbb{C}[x]\Rightarrow x^2-6x+25|g(x) \ \text{ στο } \ \mathbb{C}[x].$$
Αλλά $x^2-6x+25, g(x)\in\mathbb{R}[x]$, οπότε από το Λήμμα 4.28 έπεται ότι
$$x^2-6x+25|g(x) \ \text{ στο } \ \mathbb{R}[x].$$

Επειδή μκδ$(x, x^2 - 6x + 25) = 1$, έπεται ότι

$$x(x^2 - 6x + 25) | g(x) \text{ στο } \mathbb{R}[x]$$

Επομένως $g(x) \in < f(x) >$, όπου $f(x) = x(x^2 - 6x + 25)$, που σημαίνει ότι

$$\{g(x) \in \mathbb{R}[x] : g(0) = g(3 - 4i) = 0\} \subseteq < f(x) > .$$

Η σχέση $< f(x) > \subseteq \{g(x) \in \mathbb{R}[x] : g(0) = g(3 - 4i) = 0\}$ είναι σαφής καθώς $f(0) = f(3 - 4i) = 0$. Συνεπώς έχουμε ισότητα.

12. *Λύση.* Όχι γιατί το $\mathbb{Z}$ δεν είναι ιδεώδες του $\mathbb{C}$.

13. *Λύση.* Η μία κατεύθυνση έχει αποδειχθεί στην Πρόταση 5.15(2). Έστω R μεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$ τέτοιος ώστε τα μόνα ιδεώδη του R είναι το R και το μηδενικό. Για να δείξουμε ότι το R είναι σώμα, αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο. Έστω λοιπόν $a \in R, a \neq 0_R$. Από την υπόθεση έχουμε $< a >= R$. Άρα υπάρχει $r \in R$ με $ra = 1_R$. Επειδή ο R είναι μεταθετικός, αυτό σημαίνει ότι το a είναι αντιστρέψιμο.

14. *Λύση.* Έχουμε $0_R \in \varphi^{-1}(J)$ αφού $\varphi(0_R) = 0_S \in J$. Έστω $a_1, a_2 \in \varphi^{-1}(J)$ και $r \in R$. Τότε

$$\varphi(a_1), \varphi(a_2) \in J \Rightarrow \varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) \in J,$$

γιατί το J είναι ιδεώδες. Άρα $a_1 - a_2 \in \varphi^{-1}(J)$. Και πάλι επειδή το J είναι ιδεώδες έχουμε

$$\varphi(ra_1) = \varphi(r)\varphi(a_1) \in J, \quad \varphi(a_1 r) = \varphi(a_1)\varphi(r) \in J.$$

Άρα το $\varphi^{-1}(J)$ είναι ιδεώδες του R.

Για το δεύτερο ερώτημα θεωρούμε πιο γενικά ένα επιμορφισμό δακτυλίων $\varphi : R \to S$ και υποθέτουμε ότι κάθε ιδεώδες του R είναι κύριο. Θα δείξουμε ότι κάθε ιδεώδες του S είναι κύριο.

Πράγματι, έστω ιδεώδες J του S. Από το πρώτο ερώτημα, το $\varphi^{-1}(J)$ είναι ιδεώδες του R και άρα κύριο, $\varphi^{-1}(J) =< a >$, $a \in R$. Επειδή η απεικόνιση φ είναι επί έχουμε $J = \varphi(\varphi^{-1}(J))$ και επομένως

$$J = \varphi(< a >) = \{\varphi(r)\varphi(a) : r \in R\}.$$

Και πάλι επειδή η φ είναι επί παίρνουμε

$$\{\varphi(r)\varphi(a) : r \in R\} = \{s\varphi(a) : s \in R\} =< \varphi(a) >$$

και έχουμε το ζητούμενο.

Η ειδική περίπτωση της άσκησης προκύπτει θεωρώντας το φυσικό επιμορφισμό $\mathbb{Z} \to \mathbb{Z}_n$, $m \mapsto [m]$, και επικαλώντας το Θεώρημα 5.19 που λέει ότι κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο.

15. *Λύση* των ii) και iii). Αρχικά θα προσδιορίσουμε το σύνολο $C(A)$. Έστω $A, X \in T_2(R)$, $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, X = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$. Τότε $A \in C(T_2(R)) \Leftrightarrow AX = XA$ για κάθε $x, y, z \in R$. Κάνοντας τις πράξεις πινάκων, αυτό ισοδυναμεί με

$$\begin{aligned} ax &= xa, \\ ay + bz &= xb + yc, \\ cz &= zc, \end{aligned}$$

για κάθε $x, y, z \in R$. Ισοδύναμα, έχουμε τις σχέσεις

$$\begin{aligned} a &\in C(R), \\ ay + bz &= xb + yc, \\ c &\in C(R), \end{aligned}$$

για κάθε $x, y, z \in R$. Θέτοντας στην παραπάνω ισότητα $x = y = 0_R$ και $z = 1_R$, παίρνουμε $b = 0_R$. Επίσης θέτοντας στην παραπάνω ισότητα $x = z = 0_R$ και $y = 1_R$, παίρνουμε $a = c$.

Άρα

$$C(T_2(R)) \subseteq \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in C(R)\}.$$

Αντίστροφα, είναι σαφές ότι κάθε A της μορφής $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a \in C(T_2(R))$, ικανοποιεί τις παραπάνω σχέσεις και άρα έχουμε ισότητα $C(T_2(R)) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in C(R)\}$. Θεωρούμε τώρα την απεικόνιση

$$\psi : C(T_2(R)) \to C(R),\ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mapsto a.$$

Είναι υπόθεση ρουτίνας η επαλήθευση ότι η ψ είναι ισομορφισμός δακτυλίων.

Υπόδειξη για το iv). Έστω $\varphi : S \to R$ ισομορφισμός δακτυλίων και $\psi : C(S) \to R$ ο περιορισμός της φ στο υποσύνολο $C(S)$ του S. Ως περιορισμός μονομορφισμού σε υποδακτύλιο, είναι σαφές ότι η ψ είναι μονομορφισμός. Δείξτε ότι $Im\psi = C(R)$. Από αυτό έπεται ότι $C(S) \simeq C(R)$.

16. *Υπόδειξη.* Η απόδειξη είναι παρόμοια με εκείνη της άσκησης 3.20 iii).

17. i) *Λύση.* Η σχέση $I \subseteq \sqrt{I}$ είναι σαφής. Έστω $a, b \in \sqrt{I}$ και $r \in R$. Τότε υπάρχουν φυσικοί αριθμοί n, m, με $a^n, b^m \in I$. Επειδή $(ra)^n = r^n a^n \in I$, έχουμε $ra \in \sqrt{I}$. Χρησιμοποιώντας το διωνυμικό ανάπτυγμα, έπεται ότι το $(a-b)^{n+m}$ είναι ένα άθροισμα στοιχείων της μορφής

$$c_i a^i b^{n+m-i}$$

με $c_i \in \mathbb{Z}$, $i \in \{0, 1, \ldots, n+m\}$. Θα δείξουμε ότι κάθε τέτοιο στοιχείο ανήκει στο I. Πράγματι, για $i \geq n$ έχουμε

$$c_i a^i b^{n+m-i} = a^n c_i a^{i-n} b^{n+m-i} \in I,$$

ενώ για $i < n$, έχουμε $i+1 \leq n$ και άρα

$$c_i a^i b^{n+m-i} = c_i a^i b^{n+i} \cdot b^m \in I.$$

Συνεπώς $(a-b)^{n+m} \in I$ και άρα $a - b \in \sqrt{I}$. Έχουμε δείξει ότι το $\sqrt{I}$ είναι ένα ιδεώδες του R.

ii)*Απάντηση.* $\sqrt{<3>} = <3>$, $\sqrt{<12>} = <6>$

iii) *Λύση.* Για να δείξουμε ότι $\sqrt{<0>} \subseteq <[p_1 \ldots p_r]>$, έστω $[m] \in \sqrt{<0>}$. Τότε υπάρχει φυσικός αριθμός $k \geq 1$, τέτοιος ώστε $[m^k] = [m]^k = [0] \in \mathbb{Z}_n$ και άρα $n | m^k$. Καθώς είναι $n = p_1^{a_1} \ldots p_r^{a_r}$ και $a_i > 0$ για κάθε i, συμπεραίνουμε ότι είναι $p_i | m^k$ και άρα $p_i | m$ για κάθε i. Όμως, οι πρώτοι $p_1, \ldots, p_r$ είναι διακεκριμένοι και άρα θα πρέπει να είναι $p_1 \ldots p_r | m$. Άρα $[m] \in <[p_1 \ldots p_r]> \subseteq \mathbb{Z}_n$.

Αντίστροφα, έστω $[m] \in <[p_1 \ldots p_r]>$. Μπορούμε να υποθέσουμε ότι $m = s p_1 \ldots p_r$, για κάποιο $s \in \mathbb{Z}$. Αν $a = \max\{a_1, \ldots, a_r\}$, τότε ο ακέραιος $m^a = s^a p_1^a \ldots p_r^a$ είναι πολλαπλάσιο του $n = p_1^{a_1} \ldots p_r^{a_r}$ (καθώς $a \geq a_i$ για κάθε $i = 1, \ldots, r$). Συνεπώς $[m]^a = [m^a] = [0] \in \mathbb{Z}_n$ και άρα $[m] \in \sqrt{<0>}$. Έτσι, έχουμε δείξει ότι $<[p_1 \ldots p_r]> \subseteq \sqrt{<0>}$ και συνεπώς έχουμε ισότητα.

18. ii) Υπόδειξη. Έστω K ιδεώδες του $R \times S$. Θεωρούμε τα σύνολα

$$I = \{a \in R : \exists s \in S,\ (a, s) \in K\}$$
$$J = \{b \in S : \exists r \in R,\ (r, b) \in K\}.$$

Δείξτε ότι τα I, J είναι ιδεώδη των R, S αντίστοιχα και ότι $K = I \times J$.

19. *Υπόδειξη.* Αληθεύει. Χρησιμοποιώντας την προηγούμενη άσκηση και το γεγονός ότι κάθε ιδεώδες του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$, έπεται ότι κάθε ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ είναι της μορφής $m\mathbb{Z} \times n\mathbb{Z}$. Δείξτε ότι ως ιδεώδη του $\mathbb{Z} \times \mathbb{Z}$, ισχύει ότι

$$m\mathbb{Z} \times n\mathbb{Z} = <(m, n)>.$$

20. *Λύση.* Ένα παράδειγμα είναι το σύνολο $S = \{(a, a) \in \mathbb{Z} \times \mathbb{Z} : a \in \mathbb{Z}\}$. Εύκολα αποδεικνύεται ότι είναι υποδακτύλιος του $\mathbb{Z} \times \mathbb{Z}$ (άσκηση). Δεν είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ καθώς $(1, 0)(1, 1) = (1, 0) \notin S$.

21. *Λύση.* Είναι σαφές ότι το σύνολο I είναι μη κενό. Αν $u(x), v(x) \in I$, τότε
$$u(x) = f(a)a(x) + g(x)b(x),\ v(x) = f(a)a'(x) + g(x)b'(x)$$
για κάποια $a(x), a'(x), b(x), b'(x) \in \mathbb{Z}_3[x]$. Έχουμε
$$u(x) - v(x) = f(x)(a(x) - a'(x)) + g(x)(b(x) - b'(x)) \in I.$$
Επίσης έχουμε
$$u(x)r(x) = f(a)(a(x)r(x)) + g(x)(b(x)r(x)) \in I$$
για κάθε $r(x) \in \mathbb{Z}_3[x]$. Επειδή ο δακτύλιος $\mathbb{Z}_3[x]$ είναι μεταθετικός, τα παραπάνω δείχνουν ότι το I είναι ιδεώδες του $\mathbb{Z}_3[x]$.
Εναλλακτικά θα μπορούσαμε απλά να παρατηρήσουμε ότι $I =< f(x), g(x) >$ που είναι ιδεώδες (βλ. Παράγραφο 5.4).
Θα δείξουμε ότι $I =< d(x) >$, όπου $d(x)$ είναι ο μκδ των $f(x), g(x)$. Επειδή $d(x)|f(x)$ και $d(x)|g(x)$, έπεται ότι $d(x)|f(x)a(x)+g(x)b(x)$ για κάθε $a(x), b(x) \in \mathbb{Z}_3[x]$. Συνεπώς $I \subseteq < d(x) >$. Από το Θεώρημα 4.13 υπάρχουν $a(x), b(x) \in \mathbb{Z}_3[x]$ με $d(x) = f(x)a(x)+g(x)b(x)$. Άρα $d(x) \in I$ και επειδή το I είναι ιδεώδες, έχουμε $< d(x) > \subseteq I$. Άρα $I =< d(x) >$.
Κατά τα γνωστά βρίσκουμε (πχ με τον Ευκλείδειο αλγόριθμο) $d(x) = x - 1$, οπότε $I =< x - 1 >$.
Εναλλακτικά, το ζητούμενο έπεται άμεσα από το Παράδειγμα 5.26(2iii), αλλά προτιμήσαμε να δώσουμε μια αυτοτελή και αναλυτική απόδειξη.
Τέλος, έστω $h(x) \in \mathbb{Z}_3[x]$ με $< d(x) >=< h(x) >$. Τότε $h(x)|d(x)$ και $d(x)|h(x)$. Επειδή ο δακτύλιος $\mathbb{Z}_3$ είναι σώμα, από την Πρόταση 4.8(4) έπεται ότι υπάρχει μη μηδενικό $c \in \mathbb{Z}_3$, με $h(x) = cd(x)$. Αντίστροφα, αν $h(x) = cd(x)$ για κάποιο μη μηδενικό $c \in \mathbb{Z}_3$, τότε $< h(x) > \subseteq < d(x) >$. Επειδή το c είναι αντιστρέψιμο, έχουμε τη σχέση $d(x) = c^{-1}h(x)$ και άρα $< d(x) > \subseteq < h(x) >$, οπότε $< h(x) >=< d(x) >$. Καθώς $c \in \mathbb{Z}_3 - \{0\}$, έχουμε $3 - 1 = 2$ δυνατότητες για το c, πράγμα που σημαίνει ότι το πλήθος των $h(x)$ με $< h(x) >= I$ είναι 2.

22.

23. *Απάντηση.* Αληθεύει καθώς αν I ιδεώδες του $\mathbb{Z}[i]$, τότε $a + bi \in I \Rightarrow a^2 + b^2 = (a - bi)(a + bi) \in I$.

24. *Λύση.* Παρατηρούμε ότι για κάθε $a \in I, b \in J$ έχουμε $ab \in I$ και $ab \in J$ από τον ορισμό του ιδεώδους. Άρα $ab \in I \cap J$. Από τον Ορισμό 5.25 και το γεγονός ότι το $I \cap J$ είναι ιδεώδες, έπεται ότι $IJ \in I \cap J$.

    Ένα παράδειγμα όπου δεν ισχύει η ισότητα είναι $R = \mathbb{Z}, I =< 4 >, J =< 6 >$, καθώς $IJ =< 24 > \subsetneq I \cap J =< 12 >$.

25. *Απάντηση.* Σ, Λ, Σ.

26. *Υπόδειξη.* Δείξτε ότι η επέκταση (βλ. Εφαρμογή στην Παράγραφο 5.1) ισομορφισμού δακτυλίων είναι ισομορφισμός.

27. *Λύση.* Παρατηρούμε ότι στο $\mathbb{Z}_3[x]$ έχουμε $x^{18} + 1 = (x^2)^{3^2} + 1 = (x^2 + 1)^{3^2}$ σύμφωνα με Παράδειγμα 4.2. Το πολυώνυμο $x^2 + 1$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$ γιατί είναι δευτέρου βαθμού και δεν έχει ρίζα στο $\mathbb{Z}_3$. Συνεπώς το $x^{18} + 1$ διαιρείται από μοναδικό ανάγωγο παράγοντα, το $x^2 + 1$. Από αυτό έπεται ότι $\mu\kappa\delta(f(x), x^{18} + 1) \neq 1 \Leftrightarrow x^2 + 1 | f(x)$. Άρα $I =< x^2 + 1 >$. Συνεπώς ένα μη μηδενικό πολυώνυμο ελαχίστου βαθμού στο I είναι το $x^2 + 1$.

28. *Λύση.* Ως γνήσιο ιδεώδες σώματος, ο $\ker\varphi$ είναι το μηδενικό ιδεώδες. Άρα ο φ είναι ισομορφισμός και ο R ισόμορφος με το F, οπότε ο R είναι σώμα.

29. *Υπόδειξη.* Μετρήστε το πλήθος των στοιχείων e που ικανοποιούν $e^2 = e$.

30. *Απάντηση.* n είναι δύναμη πρώτου.

31.

32. Υπόδειξη για το ii. Έστω $X = \{x_1, ..., x_n\}$. Θεωρήστε τη συνάρτηση

$$\chi : P(X) \to \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2,\ A \mapsto (a_1, ..., a_n),$$

όπου $a_i = [0]$ αν $x_i \notin A$ και $a_i = [1]$ αν $x_i \in A$. Δείξτε ότι η χ είναι ισομορφισμός δακτυλίων.
Σημείωση. Η χ είναι γνωστή ως η *χαρακτηριστική συνάρτηση*.

33.

Δακτύλιος πηλίκο

Έστω R δακτύλιος και I ιδεώδες του R. Ο σκοπός μας είναι να κατασκευάσουμε τον *δακτύλιο πηλίκο* R/I και να εξετάσουμε βασικές ιδιότητές και εφαρμογές του. Δίνουμε έμφαση σε πηλίκα πολυωνυμικών δακτυλίων. Μεταξύ των άλλων αποδεικνύουμε το κινέζικο θεώρημα υπολοίπων για δακτυλίους με μονάδα.

Βασικά σημεία

- δακτύλιος πηλίκο
- πηλίκα πολυωνυμικών δακτυλίων
- πρώτο θεώρημα ισομορφισμών
- κινέζικο θεώρημα υπολοίπων
- πεπερασμένα σώματα

6.1. Ο δακτύλιος πηλίκο

Ορισμός 6.1. *Έστω R δακτύλιος και I ιδεώδες του R. Ορίζουμε στο R την εξής σχέση ισοδυναμίας.*

$$a \equiv b \mod I \Leftrightarrow a - b \in I.$$

Η παραπάνω σχέση είναι πράγματι σχέση ισοδυναμίας:

(1) $a \equiv a \mod I$, για κάθε $a \in R$ αφού $a - a = 0_R \in I$.

(2) Αν $a \equiv b \mod I$, τότε $a - b \in I$ και επειδή το I είναι ιδεώδες έπεται ότι $-(a-b) \in I$. Επομένως $b - a \in I \Rightarrow b \equiv a \mod I$.

(3) Αν $a \equiv b \mod I$ και $b \equiv c \mod I$, τότε $a - b \in I$ και $b - c \in I$. Επειδή το I είναι ιδεώδες, έπεται ότι $(a - b) + (b - c) = a - c \in I$.

Η κλάση ισοδυναμίας του $a \in R$ είναι εξ ορισμού $[a] = \{b \in R : b \equiv a \mod I\}$. Παρατηρούμε ότι

$$b \equiv a \mod I \Leftrightarrow b - a \in I \Leftrightarrow b = a + c, \ \ c \in I.$$

Δηλαδή, $[a] = \{a + c \in R : c \in I\}$. Συμβολικά γράφουμε $[a] = a + I$.

Ορισμός 6.2. *Το σύνολο των κλάσεων ισοδυναμίας της παραπάνω σχέσης ισοδυναμίας θα συμβολίζεται με R/I, δηλαδή*

$$R/I = \{a + I : a \in R\}.$$

Τονίζουμε ότι δύο κλάσεις $a+I, b+I \in R/I$ είναι ίσες αν και μόνο αν $a-b \in I$, ισοδύναμα υπάρχει $c \in I$ με $b = a + c$.

Παρατήρηση. Στην ειδική περίπτωση που $R = \mathbb{Z}$ και $I =< n >$, ο Ορισμός 6.1 είναι απλά ο ορισμός της ισοτιμίας δύο ακεραίων modulo n που είδαμε στην Παράγραφο 2.1. Επομένως στην περίπτωση αυτή έχουμε

$$a + I = a + n\mathbb{Z} = \{a + kn : k \in \mathbb{Z}\} = [a]_n \quad \text{και} \quad \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Στη συνέχεια θα ορίσουμε με φυσικό τρόπο δύο πράξεις στο σύνολο R/I και θα δούμε ότι έχουμε τη δομή δακτυλίου.

Θεώρημα 6.3. *Έστω R δακτύλιος και I ιδεώδες του R. Το σύνολο R/I με τις ακόλουθες πράξεις είναι δακτύλιος.*

$$+ : R/I \times R/I \to R/I, \quad (a + I) + (b + I) = (a + b) + I,$$
$$\cdot : R/I \times R/I \to R/I, \quad (a + I)(b + I) = ab + I.$$

Επιπλέον,

- *αν ο R είναι μεταθετικός, τότε και ο R/I είναι μεταθετικός, και*
- *αν ο R έχει μονάδα (το 1_R), τότε και ο R/I έχει μονάδα (το $1_R + I$).*

Απόδειξη. Πρώτα θα δείξουμε ότι οι παραπάνω πράξεις είναι καλώς ορισμένες. Πράγματι, έστω $a + I = a' + I$ και $b + I = b' + I$. Τότε $a - a' \in I$ και $b - b' \in I$. Επομένως

$$(a - a') + (b - b') \in I \Rightarrow (a + b) - (a' + b') \in I \Rightarrow a + b + I = a' + b' + I.$$

Άρα η πρόσθεση είναι καλώς ορισμένη. Θα δείξουμε το ίδιο και για τον πολλαπλασιασμό. Πράγματι, έστω $a + I = a' + I$ και $b + I = b' + I$. Τότε ομοίως με πριν παίρνουμε $a - a' \in I$ και $b - b' \in I$. Παρατηρούμε ότι

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' \in I,$$

αφού το I είναι ιδεώδες. Επομένως

$$ab + I = a'b' + I.$$

Ας δείξουμε την προσεταιριστικότητα του πολλαπλασιασμού. Πράγματι για κάθε $a, b, c \in R$ έχουμε,

$$\begin{aligned} ((a + I)(b + I))\,(c + I) &= (ab + I)(c + I) \\ &= (ab)c + I \\ &= a(bc) + I \\ &= (a + I)\,((b + I)(c + I)), \end{aligned}$$

όπου η τρίτη ισότητα έπεται από την προσεταιριστικότητα του πολλαπλασιασμού στο R. Για το μηδενικό στοιχείο, παρατηρούμε ότι για κάθε $a \in R$ έχουμε

$$(a + I) + (0_R + I) = a + I = (0_R + I) + (a + I).$$

Δηλαδή το μηδενικό στοιχείο του R/I είναι το

$$0_{R/I} = 0_R + I = I.$$

Εύκολα επαληθεύεται ότι το αντίθετο του $a + I$ είναι το

$$-(a + I) = -a + I.$$

Για τη μία επιμεριστική ιδιότητα έχουμε

$$\begin{aligned}(a+I+b+I)\,(c+I) &= (a+b+I)(c+I)\\ &= (a+b)c+I\\ &= ac+bc+I\\ &= ac+I+bc+I,\end{aligned}$$

όπου στην τρίτη ισότητα χρησιμοποιήσαμε την αντίστοιχη επιμεριστική ιδιότητα στο R. Οι αποδείξεις των άλλων ιδιοτήτων του ορισμού του δακτυλίου είναι εξίσου άμεσες και παραλείπονται.

Επομένως ο R/I με τις δοσμένες πράξεις είναι δακτύλιος.

Έστω τώρα $a, b \in R$ με $ab = ba$. Τότε

$$(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I).$$

Άρα αν ο R είναι μεταθετικός, τότε και ο R/I είναι μεταθετικός. Τέλος αν $1_R \in R$, τότε ο R/I έχει μοναδιαίο στοιχείο το $1_R + I$ αφού για κάθε $a \in R$ έχουμε

$$(1_R+I)(a+I) = 1_R a+I = a+I = a1_R+I = (a+I)(1_R+I).$$

□

Ο δακτύλιος R/I του προηγούμενου θεωρήματος καλείται ο **δακτύλιος πηλίκο** του R modulo I. Εύκολα επαληθεύεται ότι η απεικόνιση

$$R \to R/I,\ r \mapsto r+I$$

είναι επιμορφισμός δακτυλίων. Θα τον καλούμε το **φυσικό επιμορφισμό** από το R στο R/I.

Παραδείγματα 6.4. Στα παρακάτω, R θα είναι δακτύλιος και I ιδεώδες του R.

(1) Αν $I = \{0_R\}$, τότε για κάθε $a \in R$ είναι

$$a+I = \{a+0_R\} = \{a\} \ \text{ και } \ R/I = \{\{a\} : a \in R\}.$$

Εύκολα επαληθεύεται ότι η απεικόνιση $R \to R/I, a \mapsto \{a\}$ είναι ισομορφισμός δακτυλίων.

(2) Αν $I = R$, τότε για κάθε $a \in R$ είναι

$$a+I = \{a+r : r \in R\} = R \ \text{ και } \ R/I = \{R\} = \{0_{R/I}\}.$$

Δηλαδή εδώ έχουμε ότι ο δακτύλιος R/I είναι ο μηδενικός.

(3) Σημειώσαμε πιο πάνω ότι αν $R = \mathbb{Z}$ και $I =< n >$, τότε

$$a+I = [a]_n \ \text{ και } \ R/I = \mathbb{Z}_n.$$

(4) Έστω $R = \mathbb{Z}_2[x]$ και $I =< x^3+1 >= \{g(x)(x^3+1) : g(x) \in \mathbb{Z}_2[x]\}$. Θα σχολιάσουμε την αριθμητική του R/I.

- Στο R/I έχουμε $x^4+x^3+I = x+1+I$.
  Πράγματι, από την Ευκλείδεια διαίρεση έχουμε
  $$x^4+x^3 = (x+1)(x^3+1)+x+1 \Rightarrow x^4+x^3-(x+1) \in I.$$
  Η τελευταία σχέση σημαίνει ότι οι κλάσεις x^4+x^3+I και $x+1+I$ είναι ίσες.
  Είναι σαφές ότι η προηγούμενη παρατήρηση γενικεύεται, δηλαδή αν στο R έχουμε
  $$f(x) = q(x)(x^3+1)+r(x),$$
  τότε στο δακτύλιο πηλίκο έχουμε
  $$f(x)+I = r(x)+I.$$
  Επειδή το υπόλοιπο της Ευκλείδειας διαίρεσης με το x^3+1 έχει βαθμό το πολύ 2, συμπεραίνουμε ότι:
- Κάθε στοιχείο του R/I γράφεται στη μορφή $ax^2+bx+c+I$, όπου $a, b, c \in \mathbb{Z}_2$.

- Η προηγούμενη παράσταση είναι μοναδική.
  Αυτό έπεται άμεσα από την Ευκλείδεια διαίρεση που λέει (μεταξύ των άλλων) ότι για κάθε $f(x) \in R$ υπάρχει μοναδικό $r(x) \in R$ με $f(x) - r(x) \in < x^3 + 1 >$ και $\deg r(x) < 3$.
- Το πλήθος των στοιχείων του R/I είναι $|R/I| = 8$.
  Πράγματι, από τα παραπάνω έπεται ότι το $|R/I|$ ισούται με το πλήθος των πολυωνύμων του $\mathbb{Z}_2[x]$ βαθμού το πολύ 2, δηλαδή με το πλήθος των $ax^2 + bx + c$, όπου $a, b, c \in \mathbb{Z}_2$. Είναι σαφές ότι το πλήθος αυτό είναι $2^3 = 8$.
- Ο δακτύλιος R/I είναι μεταθετικός με μονάδα σύμφωνα με το Θεώρημα 6.3, αλλά:
- Ο R/I δεν είναι περιοχή.
  Πράγματι, από την ταυτότητα πολυωνύμων $x^3 + 1 = (x + 1)(x^2 + x + 1)$ στο $R = \mathbb{Z}_2[x]$ έπεται ότι στο πηλίκο R/I έχουμε

  $$(x + 1 + I)(x^2 + x + 1 + I) = x^3 + 1 + I = I = 0_{R/I}.$$

  Οι παράγοντες αυτού του γινομένου είναι μη μηδενικοί,

  $$x + 1 + I \neq 0_{R/I} \quad \text{και} \quad x^2 + x + 1 + I \neq 0_{R/I}$$

  από τη μοναδικότητα που είπαμε πριν. (Εναλλακτική δικαιολόγηση: οι παράγοντες αυτοί είναι μη μηδενικοί γιατί $x + 1 \notin I$ και $x^2 + x + 1 \notin I$ αφού το $x^3 + 1$ δεν διαιρεί το $x + 1$ και δεν διαιρεί το $x^2 + x + 1$.)
- Το στοιχείο $x + I \in R/I$ είναι αντιστρέψιμο.
  Πράγματι,

  $$x^3 - 1 = x^3 + 1 \in I \Rightarrow x^3 + I = 1 + I \Rightarrow (x + I)(x^2 + I) = 1_{R/I}.$$

- Το στοιχείο $x + 1 + I \in R/I$ δεν είναι αντιστρέψιμο.
  Πράγματι, αν υπήρχε $g(x) \in R[x]$ με $(x + 1 + I)(g(x) + I) = 1 + I$, τότε

  $$(x + 1)g(x) + I = 1 + I \Rightarrow (x + 1)g(x) - 1 \in I \Rightarrow$$

  $$1 = (x + 1)g(x) + (x^3 + 1)q(x),$$

  για κάποιο $q(x) \in R$. Καθώς $x + 1 | x^3 + 1$, παίρνουμε $x + 1 | 1$, άτοπο.

6.2. Πηλίκα $F[x]/I$

Στη συνέχεια θα μελετήσουμε δακτυλίους πηλίκα της μορφής $F[x]/I$, όπου F σώμα.

Πρόταση 6.5. *Έστω F σώμα, $f(x) \in F[x]$ μη μηδενικό βαθμού k και I το ιδεώδες $< f(x) >$ του $F[x]$.*

(1) *Για κάθε $g(x) \in F[x]$ υπάρχει μοναδικό $r(x) \in F[x]$ με $degr(x) < k$ και $g(x)+I = r(x) + I$.*
(2) *Αν το F είναι πεπερασμένο σώμα και έχει m στοιχεία, τότε ο δακτύλιος $F[x]/I$ είναι πεπερασμένος και έχει m^k στοιχεία.*

Απόδειξη. i) Από την Ευκλείδεια διαίρεση, για κάθε $g(x) \in F[x]$, υπάρχει μοναδικό $r(x) \in F[x]$ με $g(x) - r(x) \in < f(x) >$ και $degr(x) < k$. Δηλαδή υπάρχει μοναδικό $r(x) \in F[x]$ με $g(x) + I = r(x) + I$ και $degr(x) < k$.

ii) Από το i) έπεται ότι το πλήθος των στοιχείων του συνόλου $F[x]/I$ ισούται με το πλήθος των πολυωνύμων του $F[x]$ της μορφής

$$r(x) = a_{k-1}x^{k-1} + ... + a_1x + a_0.$$

Καθώς έχουμε m επιλογές για κάθε a_i και η παραπάνω παράσταση του $r(x)$ είναι μοναδική, έπεται ότι το πλήθος των $r(x)$ ισούται με m^k. □

Θα δούμε τώρα πότε ένα στοιχείο του $F[x]/I$ είναι αντιστρέψιμο.

Θεώρημα 6.6. *Έστω F σώμα, $f(x) \in F[x]$, $I =< f(x) >$ και $g(x) \in F[x]$. Τότε το $g(x)+I$ είναι αντιστρέψιμο αν και μόνο αν τα $f(x), g(x)$ είναι σχετικά πρώτα.*

Απόδειξη. Αν το $g(x)+I$ είναι αντιστρέψιμο, τότε υπάρχει $h(x) \in F[x]$ με

$$(g(x)+I)(h(x)+I) = 1+I \Rightarrow g(x)h(x)+I = 1+I \Rightarrow f(x)|g(x)h(x)-1.$$

Αν τώρα $p(x)$ είναι κοινός διαιρέτης των $f(x)$ και $g(x)$, τότε από την τελευταία σχέση έπεται ότι $p(x)|1$. Άρα τα $f(x), g(x)$ είναι σχετικά πρώτα.
Αντίστροφα, αν τα $f(x), g(x)$ είναι σχετικά πρώτα, τότε υπάρχουν $a(x), b(x) \in F[x]$ με

$$a(x)f(x)+b(x)g(x) = 1.$$

Περνώντας στο πηλίκο $F[x]/I$ έχουμε $a(x)f(x)+b(x)g(x)+I = 1+I$, δηλαδή

$$(a(x)+I)(f(x)+I)+(b(x)+I)(g(x)+I) = 1+I.$$

Επειδή $f(x) \in I$, έχουμε $f(x)+I = I = 0_{F[x]/I}$, οπότε η παραπάνω σχέση δίνει

$$(b(x)+I)(g(x)+I)+I = 1+I,$$

που σημαίνει ότι το $g(x)+I$ είναι αντιστρέψιμο. □

Τονίζουμε ότι η προηγούμενη απόδειξη παρέχει έναν τρόπο με τον οποίο μπορούμε να αποφανθούμε αν ένα στοιχείο του $F[x]/I$ είναι αντιστρέψιμο και, σε περίπτωση που είναι αντιστρέψιμο, να υπολογίσουμε τον αντίστροφό του. (Ο Ευκλείδειος αλγόριθμος ξαναχτυπά.)

Παράδειγμα 6.7. Έστω $f(x) = x^2+x+1 \in \mathbb{Z}_5[x]$ και $I =< f(x) >$. Βρείτε (αν υπάρχει) το αντίστροφο του $g(x)+I \in R/I$, όπου $g(x) = x^3+x+1$.

Σύμφωνα με τον Ευκλείδειο αλγόριθμο έχουμε,

$$\begin{aligned} g(x) &= f(x)(x-1)+x+2 \\ f(x) &= (x+2)(x-1)+3 \end{aligned}$$

και

$$\begin{aligned} 3 &= f(x)-(x+2)(x-1) \\ &= f(x)-[g(x)-f(x)(x-1)](x-1) \\ &= f(x)(1+(x-1)^2)+g(x)(-x+1). \end{aligned}$$

Άρα τα πολυώνυμα $f(x), g(x)$ είναι σχετικά πρώτα. Σύμφωνα με το Θεώρημα 6.6, το $g(x)+I$ είναι αντιστρέψιμο στο R/I. Για να βρούμε τον αντίστροφο του $g(x)+I$ συνεχίζουμε ως εξής. Πολλαπλασιάζοντας με το αντίστροφο του 3 στο $\mathbb{Z}_5$, δηλαδή με το 2, παίρνουμε,

$$1 = 2f(x)(1+(x-1)^2)+g(x)(-2x+2).$$

Τότε στο R/I παίρνουμε,

$$1+I = (g(x)+I)\left((-2x+2)+< f(x) >\right).$$

Επειδή ο R/I είναι μεταθετικός, το αντίστροφο του $g(x)+I$ είναι είναι το $-2x+2+I$.

Θεώρημα 6.8. *Έστω F σώμα, $p(x) \in F[x]$ και $I =< p(x) >$. Τότε ο δακτύλιος $F[x]/I$ είναι σώμα αν και μόνο αν το $p(x) \in F[x]$ είναι ανάγωγο.*

Απόδειξη. Έστω ότι ο δακτύλιος $F[x]/I$ είναι σώμα. Θα δείξουμε ότι το $p(x) \in F[x]$ είναι ανάγωγο. Αρχικά παρατηρούμε ότι το $p(x)$ έχει θετικό βαθμό, γιατί αν $p(x) = c \in F$ με $c \neq 0$, τότε το c είναι αντιστρέψιμο στο $F[x]$ που σημαίνει ότι $I = F[x]$, δηλαδή $F[x]/I = 0$, αδύνατο.

Αν $p(x) = 0$, τότε $I = 0$ και ο δακτύλιος $F[x]/I$ είναι ισόμορφος με το $F[x]$ που δεν είναι σώμα. Έστω ότι

$$p(x) = a(x)b(x), \quad a(x), b(x) \in F[x].$$

Έχουμε $a(x)b(x) + I = I$ αφού $a(x)b(x) = p(x) \in I$. Επομένως $(a(x) + I)(b(x) + I) = I = 0_{F[x]/I}$. Επειδή ο $F[x]/I$ είναι σώμα παίρνουμε ότι

$$a(x) + I = I \quad \text{ή} \quad b(x) + I = I.$$

Δηλαδή, $a(x) \in I =< p(x) >$ ή $b(x) \in I =< p(x) >$. Επομένως έχουμε $p(x)|a(x)$ ή $p(x)|b(x)$. Άρα $\deg p(x) \leq \deg a(x)$ ή $\deg p(x) \leq \deg b(x)$. Συνεπώς το $p(x)$ είναι ανάγωγο.

Αντίστροφα, έστω $p(x) \in F[x]$ ανάγωγο. Ο $F[x]/I$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο το $1_F[x] + I$. Παρατηρούμε ότι

$$1_{F[x]} + I \neq 0_{F[x]} + I \ \ (\text{δηλαδή} \ \ 1_{F[x]/I} \neq 0_{F[x]/I}).$$

Πράγματι, αλλιώς θα είχαμε $1_{F[x]} \in I =< p(x) >$. Δηλαδή, $p(x)|1_{F[x]} \Rightarrow \deg p(x) = 0$, άτοπο αφού $p(x)$ ανάγωγο. Έστω $f(x) + I \in F[x]/I$ με $f(x) + I \neq 0_{F[x]/I}$. Τότε $f(x) \notin I$, δηλαδή $p(x) \nmid f(x)$. Επειδή το $p(x)$ είναι ανάγωγο, έχουμε $\mu\kappa\delta(f(x), p(x)) = 1$. Από το προηγούμενο θεώρημα παίρνουμε ότι το $f(x) + I$ είναι αντιστρέψιμο. □

Παρατήρηση. Καλό είναι να συγκριθούν τα θεωρήματα 6.6 και 6.8 με τις προτάσεις 2.18 και 3.13 αντίστοιχα ώστε να είναι σαφής η αναλογία.

6.3. Τα ιδεώδη του R/I

Θα περιγράψουμε εδώ τα ιδεώδη του δακτυλίου πηλίκου R/I συναρτήσει των ιδεωδών του R.

Αν $I \subseteq J$ είναι ιδεώδη του R, τότε το J είναι δακτύλιος (ως υποδακτύλιος του R) και έπεται άμεσα από τον ορισμό του ιδεώδους, ότι το I είναι ιδεώδες του δακτυλίου J. Συνεπώς έχουμε το δακτύλιο πηλίκο

$$J/I = \{a + I : a \in J\}.$$

Εύκολα επαληθεύεται ότι το J/I είναι ιδεώδες του R/I. Πράγματι, έχουμε $0_R \in J \Rightarrow 0_R + I \in J/I$. Αν $a, b \in J$ και $r \in R$, τότε επειδή το J είναι ιδεώδες του R έχουμε $a - b,\ ra,\ ar \in J$. Συνεπώς

$$\begin{aligned} a + I - (b + I) &= a - b + I \in J/I, \\ (r + I)(a + I) &= ra + I \in J/I, \\ (a + I)(r + I) &= ar + I \in J/I. \end{aligned}$$

Πρόταση 6.9. *Έστω I ιδεώδες του δακτυλίου R. Ισχύουν τα εξής.*

(1) *Αν J είναι ιδεώδες του R που περιέχει το I, τότε το J/I είναι ιδεώδες του R/I.*
(2) *Κάθε ιδεώδες K του R/I είναι της μορφής $K = J/I$, όπου J ιδεώδες του R που περιέχει το I. Επιπλέον, για κάθε K υπάρχει μοναδικό τέτοιο J.*

Απόδειξη. i) Αποδείχθηκε πριν.

ii)Θεωρούμε το φυσικό επιμορφισμό $\pi : R \to R/I,\ \pi(r) = r + I$. Έστω K ιδεώδες του R/I. Ορίζουμε το υποσύνολο του R,

$$J = \pi^{-1}(K) = \{r \in R : r + I \in K\}$$

Από την άσκηση 5.14, το J είναι ιδεώδες του R. Ισχύει $I \subseteq J$ καθώς για κάθε $r \in I$ είναι $\pi(r) = I = 0_{R/I} \in K$. Είναι σαφές ότι $J/I = K$. Για τη μοναδικότητα, έστω J, J' ιδεώδη του R που περιέχουν το I τέτοια ώστε

$$J/I = J'/I = K.$$

Για κάθε $a \in J$ έχουμε $a + I \in J/I = J'/I$ και συνεπώς

$$\exists a' \in J',\ a + I = a' + I \Rightarrow a - a' \in I \subseteq J' \Rightarrow a \in J'.$$

Άρα $J \subseteq J'$. Όμοια αποδεικνύεται η σχέση $J' \subseteq J$ και άρα έχουμε ισότητα. □

Η προηγούμενη πρόταση λέει ότι υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ των ιδεωδών J του R που περιέχουν το I και των ιδεωδών του R/I που δίνεται από $J \mapsto J/I$.

Πριν δούμε παραδείγματα να σημειώσουμε μερικές παρατηρήσεις σχετικά με κύρια ιδεώδη.Έστω R περιοχή και $a, b \in R$. Τότε

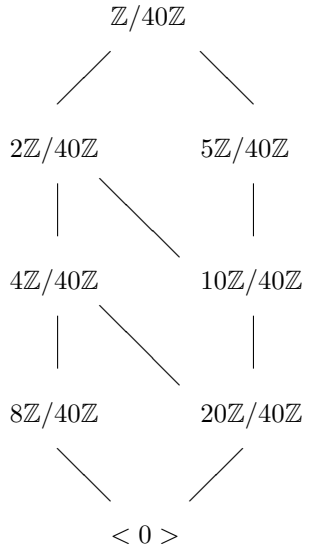
$$< a >=< b > \Leftrightarrow \exists u \in U(R),\ b = ua.$$

Πράγματι, αν $b = 0_R$, τότε $a = b = 0_R$. Έστω ότι $b \neq 0_R$. Από $b \in < b >=< a >$ παίρνουμε ότι $b = ua$ για κάποιο $u \in R$. Όμοια από $a \in < b >$ παίρνουμε ότι $a = vb$ για κάποιο $v \in R$. Αντικαθιστώντας έχουμε $b = uvb$ και επειδή ο R είναι περιοχή και το $b \in R$ είναι μη μηδενικό, παίρνουμε $uv = 1_R$. Δηλαδή $u \in U(R)$.

Ξέρουμε ότι κάθε ιδεώδες I του $R = \mathbb{Z}$ ή $F[x]$ είναι κύριο, $I =< a >$. Σημειώνουμε ότι
• αν $R = \mathbb{Z}$, τότε $< a >=< -a >$ και μπορούμε να υποθέσουμε ότι ο ακέραιος a είναι μη αρνητικός,
• αν $R = F[x]$, όπου F σώμα, τότε $< a >=< ca >$ για κάθε μη μηδενικό $c \in F$ και μπορούμε να υποθέσουμε ότι το πολυώνυμο a είναι μονικό.

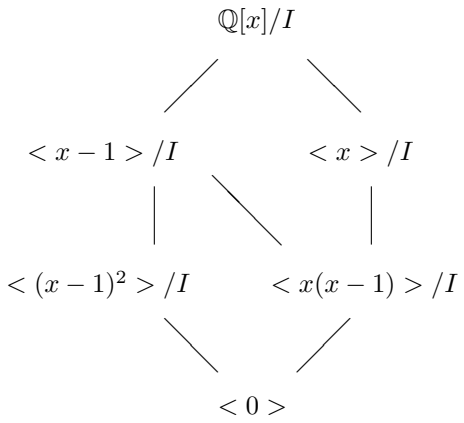
Παραδείγματα 6.10.

(1) Έστω $m \in \mathbb{N}$. Τα ιδεώδη του $\mathbb{Z}$ που περιέχουν το $< m >$ είναι ακριβώς τα $< d >$ καθώς το d διατρέχει τους θετικούς διαιρέτες του m. Από την Πρόταση 6.9 συμπεραίνουμε ότι κάθε ιδεώδες του $\mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}$, είναι της μορφής $d\mathbb{Z}/m\mathbb{Z}$ για μοναδικό θετικό $d \in \mathbb{N}$ που είναι διαιρέτης του m. Για να έχουμε εικόνα για τις διάφορες σχέσεις εγκλεισμού μεταξύ των ιδεωδών του $R = \mathbb{Z}/40\mathbb{Z}$, μπορούμε να κατασκευάσουμε το *γράφημα των ιδεωδών* του R: Οι κορυφές του γραφήματος αντιστοιχούν στα ιδεώδη του R. Δύο ιδεώδη I, J του R συνδέονται με μία ακμή αν ισχύει $I \subseteq J$ ή $J \subseteq I$ και δεν υπάρχει ιδεώδες K με $I \subsetneqq K \subsetneqq J$ ή $J \subsetneqq K \subsetneqq I$. Στην περίπτωση αυτή, το ιδεώδες που αντιστοιχεί στο άνω άκρο της ακμής περιέχει το ιδεώδες που αντιστοιχεί στο κάτω άκρο.
Για τον δακτύλιο $R = \mathbb{Z}/40\mathbb{Z}$ το διάγραμμα ιδεωδών είναι το εξής.



(2) Έστω $n = p_1^{n_1}...p_s^{n_s}$ η ανάλυση του n σε γινόμενο πρώτων. Τότε το πλήθος των ιδεωδών του δακτυλίου $\mathbb{Z}_n$ ισούται με $(n_1 + 1)...(n_s + 1)$.
Πράγματι, το πλήθος των ιδεωδών του $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ισούται με το πλήθος των θετικών διαιρετών m του $n = p_1^{n_1}...p_s^{n_s}$. Επειδή κάθε τέτοιο m έχει μοναδική παράσταση της μορφής $m = p_1^{m_1}...p_s^{m_s}$ με $m_i \leq n_i$ για κάθε i, έπεται άμεσα ότι το πλήθος των m ισούται με $(n_1 + 1)...(n_s + 1)$.

(3) Έστω $R = \mathbb{Q}[x]/ < x^3 - 2x^2 + x >$. Θα ταξινομήσουμε τα ιδεώδη του R. Για συντομία, έστω $f(x) = x^3 - 2x^2 + x \in \mathbb{Q}[x]$. Όπως στο πρώτο παράδειγμα, συμπεραίνουμε ότι κάθε ιδεώδες του R είναι της μορφής $< g(x) > / < f(x) >$, για μοναδικό μονικό $g(x) \in \mathbb{Q}[x]$ τέτοιο ώστε $g(x)|f(x)$. Έχουμε $f(x) = x(x-1)^2$. Επομένως το διάγραμμα των ιδεωδών του R είναι το ακόλουθο, όπου με I συμβολίζουμε το ιδεώδες $< f(x) >$ του $\mathbb{Q}[x]$.



(4) Έστω F σώμα και $f(x) = p_1(x)^{n_1}...p_s(x)^{n_s}$, όπου $p_i(x)^{n_i} \in F[x]$ διακεκριμένα μονικά ανάγωγα πολυώνυμα. Τότε το πλήθος των ιδεωδών του δακτυλίου $F[x]/ < f(x) >$ ισούται με $(n_1 + 1)...(n_s + 1)$.

6.4. Πρώτο θεώρημα ισομορφισμών

Έστω $\varphi : R \to S$ επιμορφισμός δακτυλίων. Τότε ο $\ker \varphi$ είναι ιδεώδες του R. Άρα ο $R/\ker \varphi$ είναι δακτύλιος. Ποια είναι η σχέση των $R/\ker \varphi$ και S; Σύμφωνα με το επόμενο θεώρημα οι δακτύλιοι $R/\ker \varphi$ και S είναι ισόμορφοι.

Θεώρημα 6.11 (Πρώτο θεώρημα ισομορφισμών δακτυλίων). *Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων. Τότε η απεικόνιση*

$$\psi : R/\ker \varphi \to S,\ r + \ker \varphi = \varphi(r),$$

είναι μονομορφισμός και η ακόλουθη απεικόνιση είναι ισομορφισμός

$$\psi : R/\ker \varphi \to Im\varphi,\ r + \ker \varphi = \varphi(r).$$

Απόδειξη. Ορίζουμε την αντιστοιχία

$$\psi : R/\ker \varphi \to \mathrm{Im}\varphi,\ \ \psi(r + \ker \varphi) = \varphi(r).$$

Θα δείξουμε πρώτα ότι η αντιστοιχία αυτή είναι μια καλώς ορισμένη απεικόνιση. Πράγματι, έστω $r + \ker \varphi = r' + \ker \varphi$. Τότε $r - r' \in \ker \varphi$, άρα

$$\varphi(r) - \varphi(r') = \varphi(r - r') = 0_S \Rightarrow \varphi(r) = \varphi(r') \Rightarrow \psi(r + \ker \varphi) = \psi(r' + \ker \varphi).$$

Τώρα θα δείξουμε ότι η ψ είναι ομομορφισμός. Πράγματι, έστω $r_1 + \ker \varphi,\ r_2 + \ker \varphi \in R/\ker \varphi$. Τότε

$$\begin{aligned} \psi\left((r_1 + \ker \varphi) + (r_2 + \ker \varphi)\right) &= \psi(r_1 + r_2 + \ker \varphi) \\ &= \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \\ &= \psi(r_1 + \ker \varphi) + \psi(r_2 + \ker \varphi). \end{aligned}$$

Ομοίως αποδεικνύεται ότι

$$\psi\left((r_1 + \ker \varphi)(r_2 + \ker \varphi)\right) = \psi(r_1 + \ker \varphi)\psi(r_2 + \ker \varphi).$$

Τέλος θα δείξουμε ότι η ψ είναι ισομορφισμός. Πράγματι, έστω $r+\ker\varphi \in \ker\psi$. Τότε

$$\psi(r+\ker\varphi)=0_S \Leftrightarrow \varphi(r)=0_S \Leftrightarrow r\in\ker\varphi \Leftrightarrow r+\ker\varphi = 0_{R/\ker\varphi}.$$

Άρα $\ker\psi=\{0_{R/\ker\varphi}\}$, δηλαδή η ψ είναι 1-1. Είναι σαφές από τον ορισμό ότι η ψ είναι επί. Η απόδειξη είναι πλήρης. □

Το προηγούμενο θεώρημα μας επιτρέπει πολλές φορές να ΄ταυτοποιήσουμε΄ ένα δακτύλιο πηλίκο.

Παραδείγματα 6.12.

(1) Έστω F ένα σώμα $I=<x-a>$ το κύριο ιδεώδες του $F[x]$ που παράγεται από το $x-a$. Ισχυριζόμαστε ότι $F[x]/I\simeq F$. Πράγματι, θεωρούμε τον επιμορφισμό εκτίμησης

$$\epsilon_a : F[x]\to F,$$

$\epsilon_a(f(x))=f(a)$. Έχουμε $\ker\epsilon_a=<x-a>$ σύμφωνα με το Παράδειγμα 5.10(2). Το Θεώρημα 6.11 δίνει το ζητούμενο.

(2) Τα σώματα $\mathbb{R}[x]/<x^2+1>$ και $\mathbb{C}$ είναι ισόμορφα.
Πράγματι, η απεικόνιση $\varphi:\mathbb{R}[x]\to\mathbb{C}$, $f(x)\mapsto f(i)$ είναι ένας επιμορφισμός δακτυλίων. Αν $f(x)\in\ker\varphi$, τότε $x-i|f(x)$ στο $\mathbb{C}[x]$ σύμφωνα με την Πρόταση 9. Από το Λήμμα 4.30 συμπεραίνουμε ότι $x+i|f(x)$. Άρα $x^2+1|f(x)$ στο $\mathbb{C}[x]$, αφού τα $x-i, x+i$ είναι σχετικά πρώτα πολυώνυμα. Άρα $x^2+1|f(x)$ στο $\mathbb{R}[x]$. Άρα $\ker\varphi\subseteq<x^2+1>$. Προφανώς έχουμε $<x^2+1>\subseteq\ker\varphi$, οπότε $<x^2+1>=\ker\varphi$. Από το Θεώρημα 6.11 έχουμε ότι $\mathbb{R}[x]/<x^2+1>\simeq\mathbb{C}$.

(3) Θεωρούμε το δακτύλιο R και το ιδεώδες I του Παραδείγματος 5.14(4).
Ισχυριζόμαστε ότι $R/I\simeq\mathbb{R}$. Πράγματι, θεωρούμε την απεικόνιση

$$\phi: R\to\mathbb{R},\ \phi\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}=a.$$

Η φ είναι επιμορφισμός δακτυλίων επειδή

$$\phi\left(\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}+\begin{pmatrix} c & d\\ 0 & c\end{pmatrix}\right)=\phi\begin{pmatrix} a+c & b+d\\ 0 & a+c\end{pmatrix}$$
$$=a+c=\phi\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}+\phi\begin{pmatrix} c & d\\ 0 & c\end{pmatrix}$$

και

$$\phi\left(\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}\begin{pmatrix} c & d\\ 0 & c\end{pmatrix}\right)=\phi\begin{pmatrix} ac & ad+bc\\ 0 & ac\end{pmatrix}$$
$$=ac=\phi\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}\phi\begin{pmatrix} c & d\\ 0 & c\end{pmatrix}$$

για κάθε $a,b,c,d\in\mathbb{R}$. Επιπλέον, ο πυρήνας είναι

$$\ker\varphi=\left\{\begin{pmatrix} a & b\\ 0 & a\end{pmatrix}\middle| a=0\right\}=I.$$

Άρα $R/I\simeq\mathbb{R}$.

(4) Το υποσύνολο $M_n(2\mathbb{Z})$ του $M_n(\mathbb{Z})$ είναι ιδεώδες του $M_n(\mathbb{Z})$ και

$$M_n(\mathbb{Z})/M_n(2\mathbb{Z})\simeq M_n(\mathbb{Z}_2).$$

Πράγματι, εύκολα επαληθεύεται ότι η απεικόνιση

$$\varphi: M_n(\mathbb{Z})\to M_n(\mathbb{Z}_2),\ (a_{ij})\mapsto([a_{ij}])$$

είναι επιμορφισμός δακτυλίων με πυρήνα το $M_n(2\mathbb{Z})$. Το ζητούμενο έπεται από το Θεώρημα 6.11.

6.5. Κινέζικο θεώρημα υπολοίπων

Θυμίζουμε ότι αν I, J είναι ιδεώδη δακτυλίου R, τότε

$$I + J = \{a + b \in R : a \in I,\ b \in J\}.$$

Ορισμός 6.13. *Δύο ιδεώδη I, J δακτυλίου R θα λέγονται* ***σχετικά πρώτα*** *αν $I + J = R$.*

Σημειώνουμε ότι αν ο R έχει μονάδα, τότε τα ιδεώδη I, J είναι σχετικά πρώτα αν και μόνο αν υπάρχουν $a \in I$ και $b \in J$ με

$$a + b = 1.$$

Πράγματι, αν $I + J = R$, τότε $1 \in R = I + J$ και άρα υπάρχουν $a \in I$ και $b \in J$ με $a + b = 1$. Αντίστροφα, αν υπάρχουν $a \in I$ και $b \in J$ με $a + b = 1$, τότε για κάθε $r \in R$ έχουμε $r = r1 = ra + rb \in I + J$ καθώς $ra \in I$ και $rb \in J$.

Για παράδειγμα, τα ιδεώδη $< m >, < n >$ του $\mathbb{Z}$ είναι σχετικά πρώτα αν και μόνο αν $\mu\kappa\delta(m, n) = 1$.

Λήμμα 6.14. *Έστω R δακτύλιος με μονάδα και $I, I_1, ..., I_n$ ιδεώδη του R τέτοια ώστε για κάθε t, τα I και I_t είναι σχετικά πρώτα. Τότε τα I και $I_1 \cap I_2 \cap ... \cap I_n$ είναι σχετικά πρώτα.*

Απόδειξη. Από την υπόθεση υπάρχουν στοιχεία $a_t \in I$ και $b_t \in I_t$, όπου $t = 1, ..., n$ με

$$a_i + b_i = 1.$$

Πολλαπλασιάζοντας κατά μέλη τις ισότητες αυτές, παίρνουμε ισότητα της μορφής

$$x + b_1 b_2 ... b_n = 1.$$

Είναι σαφές ότι $b_1 b_2 ... b_n = b_1 b_2 ... b_t ... b_n \in I_t$ για κάθε t αφού το I_t είναι ιδεώδες. Επειδή το x είναι άθροισμα γινομένων καθένα από τα οποία περιλαμβάνει έναν τουλάχιστον παράγοντα $x_i \in I$ και επειδή το I είναι ιδεώδες, έχουμε $x \in I$. □

Θεώρημα 6.15 (Κινέζικο θεώρημα υπολοίπων)**.** *Έστω R δακτύλιος και $I_1, ..., I_n$ ιδεώδη του R. Θεωρούμε την απεικόνιση*

$$\psi : R/I_1 \cap ... \cap I_n \to R/I_1 \times \cdots R/I_n,$$
$$r + I_1 \cap ... \cap I_n \mapsto (r + I_1, ..., r + I_n).$$

(1) *Η ψ είναι μονομορφισμός δακτυλίων.*
(2) *Αν ο R έχει μονάδα και τα ιδεώδη $I_1, ..., I_n$ είναι ανά δύο σχετικά πρώτα, τότε η ψ είναι ισομορφισμός δακτυλίων.*

Απόδειξη. (1) Θεωρούμε την απεικόνιση

$$\varphi : R \to R/I_1 \times ...R/I_n,$$
$$r \mapsto (r + I_1, ..., r + I_n).$$

Η φ είναι ομομορφισμός δακτυλίων, καθώς για κάθε $r, r' \in R$ είναι

$$\begin{aligned} \varphi(r + r') &= ((r + r') + I_1, ..., (r + r') + I_n) \\ &= ((r + I_1) + (r' + I_1), ..., (r + I_n) + (r' + I_n)) \\ &= (r + I_1, .., r + I_n) + (r' + I_1, ..., r' + I_n) \\ &= \varphi I_1(r) + \varphi I_1(r'), \end{aligned}$$

και

$$\begin{aligned} \varphi(rr') &= (rr' + I_1, ..., rr' + I_n) \\ &= ((r + I_1)(r' + I_1), ..., (r + I_n)(r' + I_n)) \\ &= (r + I_1, ..., r + I_n)(r' + I_1, ..., r' + I_n) \\ &= \varphi(r)\varphi(r'). \end{aligned}$$

Ένα $r \in R$ ανήκει στον πυρήνα της φ αν και μόνο αν $(r + I_1, ..., r + I_n) = (0 + I_1, ..., 0 + I_n)$, ισοδύναμα, αν για κάθε t,

$$r + I_t = 0 + I_t \Leftrightarrow r \in I_t \Leftrightarrow r \in I_1 \cap ... \cap I_n.$$

Άρα $\ker \varphi = I_1 \cap ... \cap I_n$. Συνεπώς από το πρώτο θεώρημα ισομορφισμών, έπεται ότι η απεικόνιση ψ είναι μονομορφισμός δακτυλίων.

Θα δείξουμε τώρα ότι, αν ο R διαθέτει μονάδα και τα ιδεώδη $I_1, ..., I_n$ είναι ανά δύο σχετικά πρώτα, τότε ο ομομορφισμός ψ είναι ισομορφισμός. Λόγω του (1), αρκεί να δείξουμε ότι ο ψ είναι επί. Η απόδειξη θα γίνει με επαγωγή στο n.

Έστω ότι $n = 2$. Καθώς $I_1 + I_2 = R$, υπάρχουν $a \in I_1$ και $b \in I_2$ με $1 = a + b$. Έστω $(r_1 + I_1, r_2 + I_2) \in R/I_1 \times R/I_2$. Θέτουμε

$$r = br_1 + ar_2 \in R$$

και παρατηρούμε ότι

$$r + I_1 = br_1 + I_1 = (1 - a)r_1 + I_1 = r_1 + I_1$$

και όμοια

$$r + I_2 = ar_2 + I_2 = (1 - b)r_2 + I_2 = r_2 + I_2.$$

Άρα $\varphi(r) = (r_1 + I_1, r_2 + I_2)$ και ο φ είναι επί. Συνεπώς έχουμε ότι και ο ψ είναι επί.

Έστω ότι $n \geq 3$ και ότι το ζητούμενο ισχύει για $n - 1$ το πλήθος σχετικά πρώτα ιδεώδη. Από το Λήμμα 6.14, τα ιδεώδη I_1 και $J = I_2 \cap ... \cap I_n$ είναι σχετικά πρώτα. Από την περίπτωση $n = 2$, η απεικόνιση

$$\psi_1 : R/(I_1 \cap J) \to R/I_1 \times R/J, r \mapsto (x + I_1, x + J)$$

είναι ισομορφισμός. Από την υπόθεση της επαγωγής, η απεικόνιση

$$\psi_2 : R/(I_2 \cap ... \cap I_n) \to R/I_2 \times ... \times R/I_n, y \mapsto (y + I_2, ..., y + I_n)$$

είναι ισομορφισμός. Παρατηρούμε ότι η απεικόνιση ψ είναι η εξής σύνθεση,

$$R/(I_1 \cap J) \xrightarrow{\psi_1} R/I_1 \times R/J \xrightarrow{1 \times \psi_2} R/I_1 \times R/I_2 \times ... \times R/I_n,$$

όπου

$$(1 \times \varphi_2)(x + I_1, y + J) = (x + I_1, y + I_2, ..., y + I_n).$$

Επειδή η απεικόνιση ψ_2 είναι επί, και η $1 \times \psi_2$ είναι επί. Τέλος η ψ είναι επί ως σύνθεση δύο επί απεικονίσεων. □

Παρατήρηση. Στην ειδική περίπτωση που $R = \mathbb{Z}, I =< m >$ και $J =< n >$, όπου $\mu\kappa\delta(m, n) = 1$, έχουμε $I \cap J =< mn >$ (Παράδειγμα 5.26) και από το Κινέζικο θεώρημα υπολοίπων παίρνουμε ότι η απεικόνιση

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \ [r]_{mn} \mapsto ([r]_m, [r]_n)$$

είναι ισομορφισμός δακτυλίων. Αυτό το είδαμε στο Παράδειγμα 5.2(5).

Πόρισμα 6.16. *Έστω R δακτύλιος με μονάδα και $I_1, ..., I_n$ ιδεώδη του R που είναι ανά δύο σχετικά πρώτα. Αν $b_1, ..., b_n \in R$, τότε υπάρχει $r \in R$ τέτοιο ώστε για κάθε $i = 1, ..., n$,*

$$r \equiv b_i \mod I_i.$$

Επιπλέον, αν r' ικανοποιεί τις παραπάνω ιδιότητες, τότε

$$r \equiv r' \mod I_1 \cap \cdots \cap I_n.$$

Απόδειξη. Ο πρώτος ισχυρισμός έπεται άμεσα από το γεγονός ότι στο Θεώρημα 6.14(2) η απεικόνιση ψ είναι επί. Ο δεύτερος ισχυρισμός έπεται άμεσα επειδή η ψ είναι 1-1. □

Το θεώρημα παρεμβολής του Lagrange λέει ότι κάθε μη μηδενικό πολυώνυμο βαθμού $n-1$ με συντελεστές από σώμα καθορίζεται από n τιμές του, κατ' αναλογία που μια ευθεία καθορίζεται από δύο σημεία της. Υπάρχουν διάφορες αποδείξεις. Θα δούμε μία ως πόρισμα του Κινέζικου θεωρήματος υπολοίπων.

Πόρισμα 6.17 (Θεώρημα παρεμβολής του Lagrange)**.** *Έστω F σώμα και $a_1, \ldots, a_n$ διακεκριμένα στοιχεία του F, όπου n είναι θετικός ακέραιος. Έστω $b_1, \ldots, b_n$ στοιχεία του F. Τότε υπάρχει πολυώνυμο $f(x) \in F[x]$ βαθμού το πολύ $n-1$ τέτοιο ώστε $f(a_i) = b_i$ για κάθε i. Το $f(x)$ είναι μοναδικό ως προς τις ιδιότητες αυτές.*

Απόδειξη. Θεωρούμε το δακτύλιο $R = F[x]$ και τα ιδεώδη του R,

$$I_t =< x - a_t >, t = 1, ..., n.$$

Αυτά είναι ανά δύο σχετικά πρώτα γιατί τα στοιχεία $a_1, ..., a_n$ του F είναι διακεκριμένα και το F σώμα. Από το προηγούμενο Πόρισμα, υπάρχει $g(x) \in R$ με $x - a_i | f(x) - b_i$ για κάθε i. Αυτό σημαίνει ότι $g(a_i) = b_i$. Αν $f(x)$ είναι το υπόλοιπο της διαίρεσης του $g(x)$ με το γινόμενο $(x-a_1)...(x-a_n)$, τότε για κάθε i έχουμε $f(a_i) = g(a_i) = b_i$. Επίσης, $degf(x) < n$.

Έστω $f_1(x) \in F[x]$ με $f_1(a_i) = f_1 a_i) = b_i$ για κάθε i και $degf(x) < n$. Από το προηγούμενο Πόρισμα έχουμε $f(x) - f_1(x) \in I_1 \cap \cdots \cap I_n$. Επειδή τα $a_1, ..., a_n$, είναι διακεκριμένα έχουμε σύμφωνα με το Παράδειγμα 5.26(2), ότι $I_1 \cap \cdots \cap I_n =< (x-a_1)...(x-a_n) >$, οπότε $(x-a_1)...(x-a_n) | f(x) - f_1(x)$. Λαμβάνοντας βαθμούς έχουμε $n \leq deg(f(x) - f_1(x))$ αν $f(x) - f_1(x) \neq 0$. Επειδή $deg(f(x) - f_1(x)) < n$ παίρνουμε $f(x) = f_1(x)$. □

Σημειώνουμε ότι εδώ δεν θα μας απασχολήσει ο συγκεκριμένος τύπος που υπάρχει για το μοναδικό $f(x)$ του θεωρήματος παρεμβολής του Lagrange.

Παραδείγματα 6.18.

(1) Έστω p πρώτος. Ο δακτύλιος $\mathbb{Z}_p[x]/ < x^p - x >$ είναι ευθύ γινόμενο σωμάτων.

Πράγματι, από την Πρόταση 4.23 έχουμε $x^p - x = x(x-1)...(x-(p-1))$. Επειδή τα στοιχεία $0, 1, ..., p-1 \in \mathbb{Z}_p$ είναι διακεκριμένα και το $\mathbb{Z}_p$ είναι σώμα, τα ιδεώδη $< x >, < x-1 >, ..., < x-(p-1) >$ του $\mathbb{Z}_p[x]$ είναι ανά δύο σχετικά πρώτα. Συνεπώς από το Παράδειγμα 5.26(2),

$$< x^p - x >=< x > \cap < x-1 > \cap ... \cap < x-(p-1) > .$$

Τότε από το Κινέζικο θεώρημα υπολοίπων,

$$\mathbb{Z}_p[x]/ < x^p - x >\simeq$$

$$\mathbb{Z}_p[x]/ < x > \times \mathbb{Z}_p[x]/ < x-1 > \times ... \times \mathbb{Z}_p[x]/ < x-(p-1) > .$$

Όμως για κάθε $a \in \mathbb{Z}_p$ έχουμε ότι $\mathbb{Z}_p[x]/ < x-a >\simeq \mathbb{Z}_p$, σύμφωνα με το Παράδειγμα 6.12(1). Άρα

$$\mathbb{Z}_p[x]/ < x^p - x >\simeq \mathbb{Z}_p \times \mathbb{Z}_p \times ... \times \mathbb{Z}_p,$$

όπου στο δεξί μέλος έχουμε p παράγοντες.

(2) Έστω $f(x), g(x) \in \mathbb{R}[x]$, $I =< f(x) >, J =< g(x) >$, όπου

$$f(x) = x^3 + x^2 + x + 1, \;\; g(x) = (x-5)(x^2 + 3x + 3).$$

Θα δείξουμε ότι $\mathbb{R}[x]/I \simeq \mathbb{R}[x]/J$.

Είναι $f(x) = (x+1)(x^2+1)$ και τα ιδεώδη $< x+1 >, < x^2+1 >$ του $\mathbb{R}[x]$ είναι σχετικά πρώτα. Έχουμε διαδοχικά

$$\begin{aligned} \mathbb{R}[x]/I &= \mathbb{R}[x]/ < x+1 > \cap < x^2+1 > \\ &\simeq \mathbb{R}[x]/ < x+1 > \times \mathbb{R}[x]/ < x^2+1 > \\ &\simeq \mathbb{R} \times \mathbb{C}, \end{aligned}$$

όπου στον πρώτο ισομορφισμό εφαρμόσαμε το Κινέζικο θεώρημα υπολοίπων και στο δεύτερο το Παράδειγμα 6.12(1) και το Παράδειγμα 6.12(2).

Με παρόμοιο τρόπο αποδεικνύεται ότι $\mathbb{R}[x]/J \simeq \mathbb{R} \times \mathbb{C}$, όπου χρησιμοποιούμε την άσκηση 6.7 στη θέση του Παραδείγματος 6.12(2). Συνεπώς καθένας από τους $\mathbb{R}[x]/I, \mathbb{R}[x]/J$ είναι ισόμορφος με τον ίδιο δακτύλιο. Το ζητούμενο έπεται από την Πρόταση 5.5.

6.6. Χαρακτηριστική δακτυλίου, πεπερασμένα σώματα

Έστω R δακτύλιος. Αν υπάρχει θετικός ακέραιος m τέτοιος ώστε $mr = 0_R$ για κάθε $r \in R$, τότε τον ελάχιστο τέτοιο m θα καλούμε **χαρακτηριστική** του δακτυλίου και θα το συμβολίζουμε με χαρ(R). Αν δεν υπάρχει τέτοιος m θα λέμε ότι η **χαρακτηριστική** του R είναι 0. Για παράδειγμα, η χαρακτηριστική των $\mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}[\sqrt{2}], \mathbb{Q}$ είναι 0, η χαρακτηριστική των $\mathbb{Z}_6$ και $\mathbb{Z}_6[x]$ είναι 6 και του $\mathbb{Z}_4 \times \mathbb{Z}_6$ είναι το $12 =$ εκπ(4,6).

Με την ορολογία αυτή, το όνειρο του πρωτοετή, Παράδειγμα 3.17(2), λέει ότι σε κάθε μεταθετικό δακτύλιο R χαρακτηριστικής p, όπου p πρώτος, ισχύει $(a+b)^p = a^p + b^p \ \forall a, b \in R$.

Σημειώνουμε ότι στην περίπτωση που ο R είναι περιοχή, τότε η χαρ(R) είναι 0 ή πρώτος. Πράγματι, αν χαρ$(R) = m > 0$ και $m = m_1 m_2, m_i > 1$, τότε

$$(m_1 1_R)(m_2 1_R) = (m_1 m_2)1_R = m1_R = 0_R \Rightarrow m_1 1_R = 0_R \text{ ή } m_2 1_R = 0_R \Rightarrow$$

$$m_1 r = m_1 1_R = 0_R \text{ ή } m_2 r = m_2 1_R = 0_R \ \forall r \in R,$$

που σημαίνει ότι χαρ$(R) \leq m_1 < m$ ή χαρ$(R) \leq m_2 < m$, άτοπο.

Στην περίπτωση των σωμάτων μπορούμε να πούμε κάτι ισχυρότερο.

Πρόταση 6.19. *Έστω F σώμα.*
(1) *Αν χαρ$(F) = p > 0$, τότε το F περιέχει υποδακτύλιο ισόμορφο με το σώμα $\mathbb{Z}_p$.*
(2) *Αν χαρ$(F) = 0$, τότε το F περιέχει υποδακτύλιο ισόμορφο με το σώμα $\mathbb{Q}$.*

Απόδειξη. Εύκολα αποδεικνύεται ότι η απεικόνιση

$$f : \mathbb{Z} \to F, f(a) = a1_F,$$

είναι ομομορφισμός δακτυλίων. Έστω $I = \ker f$. Ως ιδεώδες του $\mathbb{Z}$, το I είναι κύριο, $I =< m >, m \geq 0$, βλ. Θεώρημα 5.19. Το m είναι η χαρακτηριστική του F (δικαιολογήστε το).
(1) Έστω $m > 0$. Τότε $m = p$ πρώτος, αφού το F είναι περιοχή. Από το πρώτο θεώρημα ισομορφισμών δακτυλίων, έχουμε ότι $Imf \simeq \mathbb{Z}/ < p >= \mathbb{Z}_p$.
(2) Έστω $m = 0$. Τότε έχουμε ότι η f είναι μονομορφισμός. Θεωρούμε την απεικόνιση

$$g : \mathbb{Q} \to F, g(a/b) = (a1_F)(b1_F)^{-1}, a, b \in \mathbb{Z}, b \neq 0.$$

Αφήνουμε ως άσκηση ότι είναι ομομορφισμός δακτυλίων με τετριμμένο πυρήνα. □

Εφαρμογή στα πεπερασμένα σώματα.
Η παραπάνω πρόταση έχει την εξής κομψή εφαρμογή.Έστω F πεπερασμένο σώμα. Από την προηγούμενη πρόταση έπεται ότι η χαρακτηριστική του F είναι θετική και άρα είναι πρώτος αριθμός p. Επιπλέον το F περιέχει ως υποδακτύλιο σώμα F_p ισόμορφο με το $\mathbb{Z}_p$. Το σύνολο F μπορεί να γίνει F_p-διανυσματικός χώρος ορίζοντας ως πρόσθεση την πρόσθεση του δακτυλίου F και ως εξωτερικό πολλαπλασιασμό $F_p \times F \to F$ τον περιορισμό του πολλαπλασιασμού του δακτυλίου F στο $F_p \times F$. Είναι υπόθεση ρουτίνας η επαλήθευση ότι πράγματι έχουμε έτσι τη δομή F_p-διανυσματικού χώρου στο F. Από τη Γραμμική Άλγεβρα, το F θα έχει πεπερασμένη βάση καθώς είναι πεπερασμένο σύνολο. Δηλαδή υπάρχουν $v_1, ..., v_n \in F$ έτσι ώστε κάθε $v \in F$ να γράφεται μοναδικά στη μορφή γραμμικού συνδυασμού των v_i,

$$v = a_1 v_1 + ... + a_n v_n, \ a_i \in F_p.$$

Από την πολλαπλασιαστική αρχή συμπεραίνουμε ότι το πλήθος των v είναι $|F_p|^n = p^n$. Συνεπώς έχουμε αποδείξει το εξής αποτέλεσμα για πεπερασμένα σώματα.

Θεώρημα 6.20. *Το πλήθος των στοιχείων πεπερασμένου σώματος χαρακτηριστικής p είναι p^n.*

Περισσότερα για πεπερασμένα σώματα μπορείτε να δείτε στα μαθήματα Θεωρία Galois και Πεπερασμένα Σώματα και Κρυπτογραφία.

Ασκήσεις Κεφαλαίου 6

Ομάδα1: 1-3, 26, 29.
Ομάδα2: 4-21, 23-25, 28.
Ομάδα3: 22, 27, 30.

1. Έστω R δακτύλιος και I ιδεώδες του R. Δείξετε ότι ο R/I είναι μεταθετικός αν και μόνο αν για κάθε $a, b \in R$ ισχύει $ab - ba \in I$.
2. Πόσα στοιχεία έχει καθένας από τους παρακάτω δακτυλίους; Ποιοι είναι σώματα;
   i) $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$.
   ii) $\mathbb{Z}_3[x]/ < x^3 + x + 1 >$.
   iii) $M_n(\mathbb{Z})/M_n(2\mathbb{Z})$.
3. Έστω $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ και $I =< p(x) >$.
   i) Δείξτε ότι ο δακτύλιος $\mathbb{Z}_3[x]/I$ είναι σώμα με 9 στοιχεία.
   ii) Βρείτε όλα τα ιδεώδη J του $\mathbb{Z}_3[x]$ τέτοια ώστε ο δακτύλιος πηλίκο $\mathbb{Z}_3[x]/J$ είναι σώμα με 9 στοιχεία
   iii) Να εξετάσετε αν τα στοιχεία $x^4 + x + 1 + I$ και $x^4 + 2 + I$ είναι αντιστρέψιμα. Βρείτε τα αντίστροφά τους αν υπάρχουν.
4. Κατασκευάστε ένα σώμα με 8 στοιχεία και ένα σώμα με 25 στοιχεία.
5. Θεωρούμε το δακτύλιο $R = \mathbb{Z}_3[x]/ < x^2 + 2x + 2 >$. Βρείτε όλους τους ομομορφισμούς δακτυλίων στις ακόλουθες περιπτώσεις.
   i) $\mathbb{Q} \to R$.
   ii) $R \to \mathbb{Z}_3$.
   iii) $\mathbb{Z}_3 \to R$.
6. Για ποιους $n \in \mathbb{N}$ ο δακτύλιος $\mathbb{Z}[x]/ < n, x >$ είναι σώμα;
7. Έστω $f(x) \in \mathbb{R}[x]$ μονικό. Δείξτε ότι
$$\mathbb{R}[x]/ < f(x) > \simeq \mathbb{C} \quad \Leftrightarrow \quad f(x) = x^2 + ax + b, \text{ με } a^2 - 4b < 0.$$
8. ⋆ Έστω $\varphi : R \to S$ ισομορφισμός δακτυλίων που έχουν μονάδες. Δείξτε ότι αν $r \in U(R)$, τότε $\varphi(r) \in U(S)$. Στη συνέχεια δείξτε ότι ο περιορισμός της φ στο σύνολο $U(R)$ δίνει μια 1-1 και επί απεικόνιση $U(R) \to U(S)$. Ως εφαρμογή δείξτε ότι οι δακτύλιοι $\mathbb{Z}[x]$ και $\mathbb{Q}[x]$ δεν είναι ισόμορφοι.
9. Αληθεύει ότι ο δακτύλιος R/I του Παραδείγματος 6.4 είναι ισόμορφος με το $\mathbb{Z}_8$;
10. ⋆ Έστω I, J σχετικά πρώτα ιδεώδη μεταθετικού δακτυλίου R που έχει μονάδα. Δείξτε ότι $IJ = I \cap J$.
11. Δείξτε τα εξής.
    i) $\mathbb{Z}[i]/ < 1 + 2i > \simeq \mathbb{Z}_5$.
    ii) $\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$.
12. Δίνεται ο δακτύλιος R και το σύνολο I, όπου
$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in M_2(\mathbb{Z}) : a, b \in \mathbb{Z} \right\} \quad \text{και} \quad I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z}) : b \in \mathbb{Z} \right\}.$$
    i) Βρείτε τα αντιστρέψιμα στοιχεία του R.
    ii) Δείξτε ότι το I είναι ιδεώδες του R και ότι $R/I \simeq \mathbb{Z}$.
    iii) Βρείτε όλους τους ομομορφισμούς δακτυλίων $R \to \mathbb{Z}$.
    iv) Δείξτε ότι $R \simeq \mathbb{Z}[x]/ < x^2 >$.
13. Θεωρούμε τα ιδεώδη $I =< x^2 + 2 >$ και $J =< x^2 + 1 >$ του $\mathbb{Z}_5[x]$ και τα πηλίκα $R = \mathbb{Z}_5[x]/I$, $S = \mathbb{Z}_5[x]/J$.
    i) Δείξτε ότι ο R είναι σώμα και ότι ο S δεν είναι περιοχή.
    ii) Αληθεύει ότι $R \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$; Αληθεύει ότι $S \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$;

iii) Πόσα στοιχεία έχει ο R; Πόσα από τα στοιχεία του S είναι αντιστρέψιμα;

14. Έστω n θετικός ακέραιος και $a \in \mathbb{Z}_5$. Θεωρούμε τους δακτυλίους

$$R = \mathbb{Z}_5[x]/ < x^3 - x > \quad \text{και} \quad S = \mathbb{Z}_5[x]/ < x^n + ax > .$$

i) Πόσα στοιχεία του R είναι αντιστρέψιμα και πόσα ικανοποιούν τη σχέση $r^2 = 1$;
ii) Βρείτε όλα τα n, a ώστε $R \simeq S$.

15. Έστω p πρώτος και $R = \mathbb{Z}_p[x]/ < x^p - x >$.
i) Δείξτε ότι για κάθε $r \in R$ ισχύει ότι $r^p = r$.
ii) Βρείτε όλα τα μονικά $g(x) \in \mathbb{Z}_p[x]$ τέτοια ώστε $R \simeq \mathbb{Z}_p[x]/ < g(x) >$.

16. Έστω $p > 2$ πρώτος. Δείξτε ότι αν $\mathbb{Z}_p[x]/ < x^2 + 1 > \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, τότε $p \equiv 1 \mod 4$.
(Σημείωση. Ισχύει και το αντίστροφο. Μια απόδειξη θα δούμε αργότερα στις ομάδες)

17. Έστω p πρώτος και m, n θετικοί ακέραιοι. Πόσα αντιστρέψιμα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_p[x]/I$, όπου $I =< x^m(x-1)^n >$;

18. Έστω $f(x) \in \mathbb{Q}[x]$ που έχει ρίζα το $a + b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$.
i) Δείξτε ότι έχει ρίζα το $a - b\sqrt{2}$.
ii) Δείξτε ότι υπάρχει ισομορφισμός δακτυλίων $\mathbb{Q}[x]/ < x^2 - 2 > \simeq \mathbb{Q}[\sqrt{2}]$.

19. Δείξτε ότι αν F είναι σώμα χαρακτηριστικής 2 και $|F| > 2$, τότε υπάρχουν $x, y \in F$ με $(x+y)^3 \neq x^3 + y^3$.

20. Έστω R δακτύλιος.
i) Αληθεύει ότι οι $R, M_2(R)$ έχουν την ίδια χαρακτηριστική;
ii) Αληθεύει ότι οι R, S έχουν την ίδια χαρακτηριστική για κάθε μη μηδενικό υποδακτύλιο S του R;
iii) Αληθεύει ότι οι $R, R/I$ έχουν την ίδια χαρακτηριστική για κάθε γνήσιο ιδεώδες I του R;

21. Θεωρούμε το δακτύλιο $R = \mathbb{Z} \times \mathbb{Z}$ και το σύνολο $I = \{(5x, y) \in R : x, y \in \mathbb{Z}\}$. Δείξτε ότι το I είναι ιδεώδες του R και ότι το πηλίκο R/I είναι σώμα.

22. Έστω n θετικός ακέραιος. Βρείτε (ως προς ισομορφισμό) όλους του δακτυλίους R που έχουν τις εξής ιδιότητες.
- Ο R έχει μονάδα.
- $|R| = n$.
- Ο μικρότερος θετικός ακέραιος m τέτοιος ώστε $mr = 0_R$ για κάθε $r \in R$ είναι ο n.

23. Έστω F σώμα και I μη μηδενικό ιδεώδες του $F[x]$. Δείξτε ότι ο δακτύλιος $F[x]/I$ είναι περιοχή αν και μόνο αν είναι σώμα.

24. Έστω F σώμα και S περιοχή που δεν είναι σώμα. Δείξτε ότι κάθε επιμορφισμός δακτυλίων $F[x] \to S$ είναι ισομορφισμός. Στη συνέχεια βρείτε όλους τους ομομορφισμούς δακτυλίων $\mathbb{Q}[x] \to \mathbb{Z}$.

25. Θεωρούμε το δακτύλιο $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z})\}$ και το υποσύνολο του R

$$I = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_2(\mathbb{Z}) : a \equiv 0 \mod 4,\ b \equiv 0 \mod 6\}.$$

i) Ποια είναι τα αντιστρέψιμα στοιχεία του R;.
ii) Δείξτε ότι το I είναι ιδεώδες του R.
iii) Βρείτε επιμορφισμό δακτυλίων $R \to S$ για κατάλληλο S που έχει πυρήνα το I.
iv) Πόσα στοιχεία έχει ο δακτύλιος R/I και πόσα από αυτά είναι αντιστρέψιμα;

26. Τι συμπέρασμα βγάζετε για το θετικό ακέραιο n αν όλες οι κορυφές του διαγράμματος ιδεωδών του $\mathbb{Z}_n$ είναι συνευθειακές;

27. Δείξτε ότι υπάρχουν 1821 διαδοχικοί ακέραιοι καθένας από τους οποίους διαιρείται με την 1453η δύναμη κάποιου πρώτου.

28. Δείξτε ότι οι παρακάτω δακτύλιοι είναι ισόμορφοι

$$\mathbb{R}[x]/ < x^3 > \quad \text{και} \quad \{\begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \in M_3(\mathbb{R}) : a, b, c \in \mathbb{R}\}.$$

29. Αληθεύει ότι υπάρχει περιοχή με 77 στοιχεία;

30. Θεωρούμε τα $f(x) = x^2 + 1 \in \mathbb{Z}_{11}[x]$ και $g(x) = x^2 + x + 4 \in \mathbb{Z}_{11}[x]$.
    i) Δείξτε ότι τα $f(x), g(x)$ είναι ανάγωγα και ότι οι δακτύλιοι
    $$\mathbb{Z}_{11}[x]/ < f(x) >, \mathbb{Z}_{11}[x]/ < g(x) >$$
    είναι σώματα με 121 στοιχεία.
    ii) ≀ Δείξτε απευθείας ότι $\mathbb{Z}_{11}[x]/ < f(x) > \simeq \mathbb{Z}_{11}[x]/ < g(x) >$.

Υποδείξεις Ασκήσεων Κεφαλαίου 6

1. *Λύση.* Παρατηρούμε ότι

$$(a+I)(b+I) = (b+I)(a+I) \Leftrightarrow ab+I = ba+I \Leftrightarrow ab-ba \in I.$$

Επομένως ο R/I είναι μεταθετικός αν και μόνο αν $ab-ba \in I$ για κάθε $a, b \in$.

2. *Λύση.* i) Επειδή το πολυώνυμο $x^3+x+1 \in \mathbb{Z}_2[x]$ είναι τρίτου βαθμού και δεν έχει ρίζα στο $\mathbb{Z}_2$, έπεται ότι είναι ανάγωγο. Άρα ο δακτύλιος $\mathbb{Z}_2[x]/ < x^3+x+1 >$ είναι σώμα. Το πλήθος των στοιχείων του είναι 2^3σύμφωνα με την Πρόταση 6.5.

ii) Επειδή το πολυώνυμο $x^3+x+1 \in \mathbb{Z}_3[x]$ έχει ρίζα στο $\mathbb{Z}_2$ (το $1 \in \mathbb{Z}_3$), έπεται ότι δεν είναι ανάγωγο. Άρα ο δακτύλιος $\mathbb{Z}_3[x]/ < x^3+x+1 >$ δεν είναι σώμα. Το πλήθος των στοιχείων του είναι 2^3 σύμφωνα με την Πρόταση 6.5.

iii) Στο Παράδειγμα 6.12 (4), είδαμε ότι $M_n(\mathbb{Z})/M_n(2\mathbb{Z}) \simeq M_n(\mathbb{Z}_2)$. Άρα το πλήθος των στοιχείων του $M_n(\mathbb{Z})/M_n(2\mathbb{Z})$ είναι 2^{n^2} (έχουμε n^2 θέσεις σε κάθε πίνακα και σε κάθε θέση έχουμε επιλογή 2 στοιχείων). Για $n>1$, ο δακτύλιος $M_n(\mathbb{Z})/M_n(2\mathbb{Z})$ δεν είναι σώμα, για παράδειγμα ο πίνακας $diag(1,0,..,0) \in M_n(\mathbb{Z}_2)$ δεν είναι αντιστρέψιμος. Για $n=1$, έχουμε $M_1(\mathbb{Z})/M_1(2\mathbb{Z}) \simeq M_1(\mathbb{Z}_2) \simeq \mathbb{Z}_2$ που είναι σώμα.

3. *Λύση.* i) Στο $\mathbb{Z}_3$ έχουμε,

$$\begin{aligned} [0]^2+[1] &= [1] \neq [0] \\ [1]^2+[1] &= [2] \neq [0] \\ [2]^2+[1] &= [5] \neq [0] \end{aligned}$$

Άρα το $p(x)$ δεν έχει ρίζα στο $\mathbb{Z}_3$. Επειδή $\deg p(x) = 2$, το $p(x) \in \mathbb{Z}_3[x]$ είναι ανάγωγο, επομένως από το Θεώρημα 6.8, ο δακτύλιος $\mathbb{Z}_3[x]/ < p(x) >$ είναι σώμα. Από την Πρόταση 6.5, $|\mathbb{Z}_3[x]/ < p(x) > | = 3^2$.

ii) Ξέρουμε ότι κάθε ιδεώδες I του $F[x]$, όπου F σώμα, είναι κύριο, $J =< f(x) >$, και επιπλέον, το πηλίκο $F[x]/ < f(x) >$ είναι σώμα αν και μόνο αν το $f(x) \in F[x]$ είναι ανάγωγο. Επίσης ξέρουμε ότι για κάθε μη μηδενικό $c \in F$, έχουμε $< f(x) >=< uf(x) >$, που σημαίνει ότι μπορούμε να θεωρήσουμε μόνο μονικά πολυώνυμα. Τέλος ξέρουμε ότι το πλήθος των στοιχείων του $\mathbb{Z}_3[x]/(f(x))$ ισούται με 3^k, όπου $k = degf(x)$. Άρα αναζητούμε τα μονικά ανάγωγα πολυώνυμα στο $\mathbb{Z}_3[x]$ που έχουν βαθμό 2.

Ένα πολυώνυμο στο $\mathbb{Z}_3[x]$ βαθμού 2 είναι ανάγωγο αν και μόνο αν δεν έχει ρίζα στο $\mathbb{Z}_3$. Με βάση αυτό εξετάζουμε ένα προς ένα όλα τα πολυώνυμα της μορφής $x^2+ax+b \in \mathbb{Z}_3[x]$ και βρίσκουμε ότι τα ανάγωγα από αυτά είναι τα x^2+1, x^2+x+2, x^+2x+2 (οι πράξεις παραλείπονται). Άρα όλα τα ιδεώδη I που έχουν την ιδιότητα το πηλίκο $\mathbb{Z}_3[x]/(f(x))$ είναι σώμα 9 στοιχείων είναι τα

$$< x^2+1 >, < x^2+x+2 >, < x^2+2x+2 > .$$

Τέλος αυτά τα ιδεώδη είναι διακεκριμένα καθώς αν $f(x), g(x) \in \{x^2+1, x^2+x+2, x^2+2x+2\}$ και $f(x) \neq g(x)$, τότε δεν υπάρχει μη μηδενικό $c \in \mathbb{Z}_3$ με $f(x) = ug(x)$.

iii) Ο Ευκλείδειος αλγόριθμος δίνει,

$$\begin{aligned} x^4+x+1 &= (x^2-1)(x^2+1)+x+2 \\ x^2+1 &= (x+1)(x+2)-1 \\ x+2 &= (-(x+2))(-1)+0. \end{aligned}$$

Επομένως $\mu\kappa\delta(x^4+x+1, x^2+1) = 1$. Από το Θεώρημα 6.6, το $x^4+x+1+I$ είναι αντιστρέψιμο. Θα υπολογίσουμε τώρα το αντίστροφό του. Συνεχίζοντας την διαδικασία στον Ευκλείδειο αλγόριθμο βρίσκουμε μετά από πράξεις ότι

$$1 = (x+1)(x^4+x+1) + (-(x+1)(x^2-1)-1)(x^2+1).$$

Άρα $1+I=(x+1)(x^4+x+1)+I$ στο $\mathbb{Z}_3[x]$ (αφού $I=<x^2+1>$). Επομένως

$$1+I=((x+1)+I)(x^4+x+1+I),$$

δηλαδή το αντίστροφο του $x^4+x+1+I$ είναι το $x+1+I$.

Με χρήση του Ευκλείδειου αλγορίθμου βρίσκουμε ότι $x^4+2=(x^2-1)(x^2+1)$. Άρα στο $\mathbb{Z}_3[x]/<x^2+1>$ έχουμε

$$x^4+2+<x^2+1>=<x^2+1>=0_{\mathbb{Z}_3[x]/<x^2+1>}.$$

Επομένως το $x^4+2+<x^2+1>$ δεν είναι αντιστρέψιμο.

4. *Υπόδειξη.* Στην πρώτη περίπτωση, επειδή $8=2^3$, αρκεί αν βρούμε ένα πολυώνυμο $f(x)\in\mathbb{Z}_2[x]$ που να είναι ανάγωγο και βαθμού 3, και να σχηματίσουμε το δακτύλιο πηλίκο $\mathbb{Z}_2[x]/<f(x)>$. Μία επιλογή είναι x^3+x+1.
Στη δεύτερη περίπτωση, επειδή $25=5^2$, αρκεί αν βρούμε ένα πολυώνυμο $g(x)\in\mathbb{Z}_5[x]$ που να είναι ανάγωγο και βαθμού 2, και να σχηματίσουμε το δακτύλιο πηλίκο $\mathbb{Z}_5[x]/<g(x)>$. Μία επιλογή είναι x^2+2.
Βλ. τη λύση της άσκησης 6.3 i) για μια συγκεκριμένη κατασκευή πεπερασμένου σώματος. Επίσης βλ. άσκηση 6.2 i).

5. *Λύση.*
   i) Έστω $\mathbb{Q}\to R$ ομομορφισμός δακτυλίων και I ο πυρήνας του. Το I είναι ιδεώδες του σώματος $\mathbb{Q}$ και επομένως $I=\{0\}$ ή $I=\mathbb{Q}$. Στην πρώτη περίπτωση έχουμε μονομορφισμό $\mathbb{Q}\to R$, πράγμα αδύνατο καθώς το σύνολο $\mathbb{Q}$ είναι άπειρο και το R πεπερασμένο σύμφωνα με την Πρόταση 6.5. Άρα $I=\mathbb{Q}$ που σημαίνει ότι ο μόνος ομομορφισμός δακτυλίων $\mathbb{Q}\to R$ είναι ο μηδενικός.
   ii) Έστω $R\to\mathbb{Z}_3$ ομομορφισμός δακτυλίων και I ο πυρήνας του. Στην προηγούμενη άσκηση είδαμε ότι το R είναι σώμα και έχει 9 στοιχεία. Ως ιδεώδες σώματος, έχουμε $I=\{0\}$ ή $I=R$. Στην πρώτη περίπτωση έχουμε μονομορφισμό $R\to\mathbb{Z}_3$, πράγμα αδύνατο καθώς $|R|=9>3=|R|$. Άρα $I=R$ που σημαίνει ότι ο μόνος ομομορφισμός δακτυλίων $R\to\mathbb{Z}_3$ είναι ο μηδενικός.
   iii) Έστω $\varphi:\mathbb{Z}_3\to R$ ομομορφισμός και $a=\varphi([1])$. Σημειώνουμε ότι ο ομομορφισμός φ καθορίζεται από την τιμή $\varphi([1])$, γιατί για κάθε $[m]\in\mathbb{Z}_3$ είναι

$$\varphi([m])=\varphi(m[1])=m\varphi(1).$$

   Από τη σχέση $\varphi([1])=\varphi([1^2])=(\varphi([1]))^2$ παίρνουμε ότι

$$a^2=a\Rightarrow a(a-1)a=0_R\Rightarrow a=1_R\ \text{ ή }\ a=0_R,$$

   όπου η τελευταία συνεπαγωγή ισχύει επειδή ο δακτύλιος R είναι σώμα. Στη δεύτερη περίπτωση έχουμε το μηδενικό ομομορφισμό. Θα δείξουμε στη συνέχεια ότι υπάρχει ομομορφισμός δακτυλίων $\varphi:\mathbb{Z}_3\to R$ τέτοιος ώστε $\varphi([1])=1_R$. Για το σκοπό αυτό θεωρούμε την απεικόνιση $f:\mathbb{Z}\to R$ που ορίζεται από $m\mapsto m1_R$. Εύκολα επαληθεύεται ότι είναι ομομορφισμός δακτυλίων. Παρατηρούμε ότι

$$m\in\ker f\Leftrightarrow x^2+2x+2|[m]\text{ στο }\mathbb{Z}_3[x]\Leftrightarrow[m]=[0]\Leftrightarrow m\in 3\mathbb{Z}.$$

   Άρα $\ker f=3\mathbb{Z}$, οπότε από το πρώτο θεώρημα ισομορφισμών δακτυλίων παίρνουμε ομομορφισμό (μάλιστα μονομορφισμό) $\psi:\mathbb{Z}_3\to R$. Αποδείξαμε ότι υπάρχουν ακριβώς δύο ομομορφισμοί δακτυλίων $\mathbb{Z}_3\to R$, ο μηδενικός και ο ψ.

6. *Λύση.* Θεωρούμε την απεικόνιση

$$\varphi:\mathbb{Z}[x]\to\mathbb{Z},\ \varphi(f(x))=[f(0)]_n.$$

Για κάθε $f(x),g(x)\in\mathbb{Z}[x]$ είναι

$$\varphi(f(x)+g(x))=[f(0)+g(0)]=[f(0)]+[g(0)]=\varphi(f(x))+\varphi(g(x)),$$

$$\varphi(f(x)g(x))=[f(0)g(0)]=[f(0)][g(0)]=\varphi(f(x))\varphi(g(x)).$$

Άρα η φ είναι ομομορφισμός δακτυλίων. Αν $[a]_n \in \mathbb{Z}_n$, τότε θεωρώντας σταθερό πολυώνυμο της μορφής $f(x) = a$, έχουμε $\varphi(f(x)) = [a]$. Άρα η απεικόνιση φ είναι επί. Για το πυρήνα της φ έχουμε

$$\ker\varphi = \{f(x) \in \mathbb{Z}[x] : [f(0)] = [0]\}.$$

Παρατηρούμε ότι αν $f(x) = a_m x^m + ... + a_1 x + a_0$, τότε

$$[f(0)] = [0] \Leftrightarrow n|a_0 \Leftrightarrow f(x) = (a_m x^{m-1} + ... + a_1)x + an, \;\; a \in \mathbb{Z} \Rightarrow f(x) \in < x, n > .$$

Άρα $\ker\varphi \subseteq < x, n >$. Αντίστροφα, κάθε στοιχείο του συνόλου $< x, n >$ είναι της μορφής $h(x) = f(x)x + g(x)n$, όπου $f(x), g(x) \in \mathbb{Z}[x]$. Τότε

$$h(0) = g(0)n \Rightarrow [h(0)] = [g(0)n] = [0] \Rightarrow < x, n > \subseteq \ker\varphi.$$

Συνεπώς $\ker\varphi =< x, n >$. Από το πρώτο θεώρημα ισομορφισμών,

$$\mathbb{Z}[x]/ < n, x > \simeq \mathbb{Z}_n.$$

Ξέρουμε ότι ο δακτύλιος $\simeq Z_n$ είναι σώμα αν και μόνο αν ο n είναι πρώτος, Πρόταση 3.9. Από την Πρόταση 5.7(3) συμπεραίνουμε ότι ο δακτύλιος $\mathbb{Z}[x]/ < n, x >$ είναι σώμα αν και μόνο αν ο n είναι πρώτος.

7. *Λύση.* Έστω $\mathbb{R}[x]/ < f(x) > \simeq \mathbb{C}$. Σύμφωνα με το Θεώρημα 6.8 έχουμε ότι το $\mathbb{R}[x]/ < f(x) >$ είναι σώμα αν και μόνο αν το $f(x) \in \mathbb{R}[x]$ είναι ανάγωγο. Αλλά τα μονικά ανάγωγα πολυώνυμα $f(x) \in \mathbb{R}[x]$ είναι τα

$$f(x) = \begin{cases} x - a, & a \in \mathbb{R} \\ x^2 + ax + b, & a, b \in \mathbb{R},\ a^2 - 4b < 0. \end{cases}$$

Αν $f(x) = x - a,\ a \in \mathbb{R}$, τότε σύμφωνα με το Παράδειγμα 6.12 (1), έχουμε

$$\mathbb{R}[x]/ < x - a > \simeq \mathbb{R}.$$

Άρα $f(x) = x^2 + ax + b$, με $a^2 - 4b < 0$.

Θα δείξουμε τώρα ότι αν $a^2 - 4b < 0$, τότε $\mathbb{R}[x]/ < x^2 + ax + b > \simeq \mathbb{C}$. Έστω $z \in \mathbb{C}$ ρίζα του $x^2 + ax + b$. Τότε $\overline{z}$ ρίζα του $x^2 + ax + b$ (γιατί $a, b \in \mathbb{R}$) και $z \neq \overline{z}$ γιατί $a^2 - 4b < 0$. Θεωρούμε τον ομομορφισμό δακτυλίων

$$\psi : \mathbb{R}[x] \to \mathbb{C}, \;\; \psi(f(x)) = f(z).$$

Η ψ είναι επί: Πράγματι, για κάθε $y \in \mathbb{C}$, υπάρχουν πραγματικοί a, b με $ax + b = y$. (Θεωρήστε $a = y_2/z_2, b = y_1 - z_1 y_2/z_2$, όπου $z = z_1 + iz_2, z_2 \neq 0, y = y_1 + iy_2$.)

Θα δείξουμε τώρα ότι $\ker\psi =< x^2 + ax + b >$. Έστω $f(x) \in \mathbb{R}[x]$. Τότε

$$f(x) \in \ker\psi \Leftrightarrow f(z) = 0 \Leftrightarrow f(z) = f(\overline{z}) = 0.$$

Στην τελευταία ισοδυναμία χρησιμοποιήσαμε το Λήμμα 4.30. Επομένως παίρνουμε ισοδύναμα

$$x - z | f(x) \;\text{ στο }\; \mathbb{C}[x] \quad \text{και} \quad x - \overline{z} | f(x) \;\text{ στο }\; \mathbb{C}[x].$$

Επειδή $z \neq \overline{z}$ παίρνουμε,

$$\begin{array}{rcl} (x - z)(x - \overline{z}) & | & f(x) \;\text{ στο }\; \mathbb{C}[x] \Leftrightarrow \\ x^2 + ax + b & | & f(x) \;\text{ στο }\; \mathbb{C}[x] \Leftrightarrow \\ x^2 + ax + b & | & f(x) \;\text{ στο }\; \mathbb{R}[x] \;\; (\text{αφού } \; x^2 + ax + b, f(x) \in \mathbb{R}[x]). \end{array}$$

Η τελευταία ισοδυναμία έπεται από το Λήμμα 4.29. Άρα $\ker\psi =< x^2 + ax + b >$. Τότε από το πρώτο θεώρημα ισομορφισμών δακτυλίων έχουμε ότι

$$\mathbb{R}[x]/ < x^2 + ax + b > \simeq \mathbb{C}.$$

8. *Λύση.*Επειδή η φ είναι επιμορφισμός, ξέρουμε ότι $\varphi(1_R) = 1_S$. Αν $r \in U(R)$, τότε υπάρχει $r' \in R$ με
$$rr' = r'r = 1_R \Rightarrow \varphi(rr') = \varphi(r'r) = \varphi(1_R) \Rightarrow$$
$$\varphi(r)\varphi('r) = \varphi(r')\varphi(r) = 1_S \Rightarrow \varphi(r) \in U(S).$$
Συνεπώς ο περιορισμός της φ στο υποσύνολο $U(R)$, έστω ψ, δίνει απεικόνιση της μορφής
$$\psi : U(R) \to U(S).$$
Ως περιορισμός μιας 1-1 απεικόνισης, η ψ είναι επίσης 1-1. Τέλος θα δείξουμε ότι η ψ είναι επί. Έστω $s \in U(S)$. Τότε υπάρχει $s' \in U(S)$ με $ss' = s's = 1_S$. Επειδή η φ είναι επί, υπάρχουν $r, r' \in R$ με $s = \varphi(r)$ και $s' = \varphi(r')$. Άρα αντικαθιστώντας έχουμε
$$\varphi(r)\varphi('r) = \varphi(r')\varphi(r) = 1_S \Rightarrow \varphi(r'r) = \varphi(r'r) = \varphi(1_R).$$
Επειδή η φ είναι 1-1, έπεται ότι $rr' = r'r = 1_R$. Ειδικά έχουμε $r \in U(R)$, που σημαίνει ότι η ψ είναι επί απεικόνιση.

Για την εφαρμογή παρατηρούμε ότι $U(\mathbb{Z}[x]) = U(\mathbb{Z}) = \{1, -1\}$ και $U(\mathbb{Q}[x]) = U(\mathbb{Q}) = \mathbb{Q} - \{0\}$, σύμφωνα με την Πρόταση 4.5(3). Δεν υπάρχει 1-1 και επί αντιστοιχία μεταξύ των δύο αυτών συνόλων και επομένως οι δακτύλιοι $\mathbb{Z}[x]$ και $\mathbb{Q}[x]$ δεν είναι ισόμορφοι.

9. Υπόδειξη. Δείξτε ότι $|U(R/I)| = 3$ και $|U(\mathbb{Z}_8)| = 4$. Τότε από την προηγούμενη άσκηση έπεται ότι οι δακτύλιοι R/I και $\mathbb{Z}_8$ δεν είναι ισόμορφοι.

10. Ξέρουμε ότι γενικά (χωρίς την υπόθεση περί σχετικών πρώτων ιδεωδών, μεταθετικότητας και μονάδας) ισχύει $IJ \subseteq I \cap J$. Τώρα από την υπόθεση ότι τα I, J είναι σχετικά πρώτα και ο R έχει μονάδα, υπάρχουν $a \in I$ και $b \in J$ με $a + b = 1$. Άρα για κάθε $r \in I \cap J$ έχουμε
$$r = 1r = ar + br = ar + rb,$$
όπου στην τελευταία ισότητα χρησιμοποιήσαμε ότι ο R είναι μεταθετικός. Επειδή $a \in I$ και $r \in J$ έχουμε $ar \in IJ$. Επειδή $r \in I$ και $b \in J$ έχουμε $rb \in IJ$. Τέλος, επειδή το IJ είναι ιδεώδες του R έπεται ότι $r = ar + rb \in IJ$. Δείξαμε ότι $I \cap J \subseteq IJ$ και άρα $I \cap J = IJ$.

11. i) Θεωρούμε την απεικόνιση
$$\varphi : \mathbb{Z}[i] \to \mathbb{Z}_5,\ a + bi \mapsto [a + 2b].$$
Για κάθε $r_1 = a_1 + b_1 i, r_2 = a_2 + b_2 i$, όπου $a_i, b_i \in \mathbb{Z}$ έχουμε
$$\varphi(r_1 + r_2) = [a_1 + a_2 + 2(b_1 + b_2)] = [a_1 + 2b_1] + [a_2 + 2b_2] = \varphi(r_1) + \varphi(r_2).$$
Για τον πολλαπλασιασμό έχουμε
$$\varphi(r_1 r_2) = [a_1 a_2 - b_1 b_2 + 2(a_1 b_2 + a_2 b_1)] = [a_1 a_2] - [b_1 b_2] + [2a_1 b_2] + [2a_2 b_1],$$
και επίσης
$$\varphi(r_1)\varphi(r_2) = [a_1 + 2b_1][a_2 + 2b_2] = [a_1 a_2] + [4b_1 b_2] + [2a_1 b_2] + [2a_2 b_1].$$
Συνεπώς $\varphi(r_1 r_2) - \varphi(r_1)\varphi(r_2) = -[5b_1 b_2] = [0]$.
Είναι σαφές ότι η φ είναι επί. Επίσης είναι σαφές ότι $< 1 + 2i > \subseteq \ker \varphi$ γιατί για κάθε $r \in \mathbb{Z}[i]$, είναι
$$\varphi(r(1 + 2i)) = \varphi(r)\varphi(1 + 2i) = \varphi(r)[5] = [0].$$
Τέλος, αν $r = a + bi \in \ker \varphi$, τότε $[a + 2b] = [0]$, δηλαδή $a + 2b = 5m, m \in \mathbb{Z}$. Άρα
$$r = 5m - 2b + bi = (1 + 2i)(1 - 2i)m + (1 + 2i)(ib) \in < 1 + 2i > .$$
Συνεπώς $\ker \varphi = < 1 + 2i >$. Το ζητούμενο έπεται από το πρώτο θεώρημα ισομορφισμών.
Σημείωση. Πως σκεφτήκαμε τον ορισμό της συγκεκριμένης απεικόνισης φ ; Ας συμβολίσουμε με $\overline{r}$ την κλάση του $r \in \mathbb{Z}[i]$ στο πηλίκο $\mathbb{Z}[i]/ < 1 + 2i >$. Τότε $\overline{1} + \overline{2i} = \overline{0}$ και πολλαπλασιάζοντας με $\overline{i}$ παίρνουμε $\overline{i} = \overline{2}$. Βλέπουμε ότι στο πηλίκο, η εικόνα του i ισούται με την εικόνα του 2. Αυτό λάβαμε υπόψη στον ορισμό $\varphi(a + bi) = a + 2b$.

ii) Επειδή $5 = (1+2i)(1-2i)$, για τα αντίστοιχα κύρια ιδεώδη στο $\mathbb{Z}[i]$ έχουμε $< 5 >=< 1+2i >< 1-2i >$. Θα δείξουμε ότι τα ιδεώδη $I =< 1+2i >, J =< 1-2i >$είναι σχετικά πρώτα. Πράγματι, $2 = (1+2i)+(1-2i) \in I+J \Rightarrow 1 = (1+2i)-2i \in I+J$. Από την προηγούμενη άσκηση έχουμε $< 5 >= I \cap J$. Από το Κινέζικο θεώρημα υπολοίπων έχουμε

$$\mathbb{Z}[i]/ < 5 > \simeq \mathbb{Z}[i]/I \times \mathbb{Z}[i]/J$$

και από το προηγούμενο ερώτημα $\mathbb{Z}[i]/I \simeq \mathbb{Z}_5$. Όμοια αποδεικνύεται ότι $\mathbb{Z}[i]/J \simeq \mathbb{Z}_5$, θεωρώντας την απεικόνιση $\mathbb{Z}[i] \to \mathbb{Z}_5, a+bi \mapsto a-2b$.

12. i) Αρχικά σημειώνουμε ότι R είναι μεταθετικός. Θα δείξουμε ότι

$$U(R) = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R : a \in \{1,-1\}\}.$$

Πράγματι, αν $a \in \{1,-1\}$, τότε για κάθε $b \in \mathbb{Z}$, έχουμε

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

και επομένως $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in U(R)$.

Αντίστροφα, έστω $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$ τέτοιος ώστε $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, για κάποια $c, d \in \mathbb{Z}$. Τότε $ac = 1$ και επειδή οι a, c είναι ακέραιοι, έχουμε $a \in \{1,-1\}$.

ii) Υπόδειξη. Δείξτε ότι η απεικόνιση $R \to \mathbb{Z}, \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a$, είναι επιμορφισμός δακτυλίων με πυρήνα το I. Εφαρμόστε το πρώτο θεώρημα ισομορφισμών.

iii) Αν $\varphi : R \to \mathbb{Z}$ είναι ομομορφισμός δακτυλίων, τότε ο φ καθορίζεται μοναδικά από τις εικόνες $\varphi(I_2),\ \varphi(J)$, όπου $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ και $J = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, διότι για κάθε $a, b \in \mathbb{Z}$ είναι

$$\varphi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) = \varphi(aI_2 + bJ) = a\varphi(I_2) + b\varphi(J).$$

Από τη σχέση $I_2^2 = I_2$ παίρνουμε $(\varphi(I_2))^2 = \varphi(I_2) \Rightarrow \varphi(I_2) \in \{0,1\}$. Από τη σχέση $J^2 = 0$ παίρνουμε $(\varphi(J))^2 = 0 \Rightarrow \varphi(J)) = 0$. Δείξαμε ότι αν $\varphi : R \to \mathbb{Z}$ είναι ομομορφισμός δακτυλίων, τότε ο φ είναι ο μηδενικός ή είναι η απεικόνιση που ορίζεται από $\varphi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) = a$. Στο προηγούμενο υποερώτημα τονίσαμε ότι η απεικόνιση αυτή είναι πράγματι ομομορφισμός δακτυλίων. Συνεπώς υπάρχουν ακριβώς δύο ομομορφισμοί δακτυλίων $R \to \mathbb{Z}$, ο μηδενικός και αυτός του προηγούμενου υποερωτήματος.

iv) Υπόδειξη. Δείξτε απευθείας ότι η παρακάτω απεικόνιση είναι ισομορφισμός δακτυλίων $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mapsto a + bx + < x^2 >$.

13. i) Εύκολα επαληθεύεται ότι το πολυώνυμο x^2+2 δεν έχει ρίζα στο $\mathbb{Z}_5$. Επειδή είναι δευτέρου βαθμού και ο δακτύλιος $\mathbb{Z}_5$ είναι σώμα, είναι ανάγωγο στο $\mathbb{Z}_5[x]$. Συνεπώς ο δακτύλιος R είναι σώμα.
Εύκολα επαληθεύεται ότι $x^2+1 = (x-2)(x-3)$. Επομένως στο δακτύλιο S έχουμε

$$(x-2+J)(x-3+J) = 0_S.$$

Επειδή το $\mathbb{Z}_5$ είναι σώμα και $\deg(x-2) < \deg(x^2+1)$, έχουμε ότι το x^2+1 δεν διαιρεί το $x-2$. Άρα το $x-2$ δεν ανήκει στο $J =< x^2+1 >$, ισοδύναμα, $x-2+J \neq 0_S$. Με παρόμοιο τρόπο προκύπτει ότι $x-3+J \neq 0_S$. Συνεπώς ο δακτύλιος S δεν είναι περιοχή.

ii) Δεν αληθεύει ότι $R \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$ γιατί ο R είναι σώμα (από το προηγούμενο υποερώτημα), ενώ ο $\mathbb{Z}_5 \times \mathbb{Z}_5$ δεν είναι σώμα, καθώς έχει μη μηδενικό μηδενοδιαιρέτη (για παράδειγμα το $([1],[0])$ αφού $([1],[0])([0],[1]) = ([0],[0])$.

iii) Σύμφωνα με την Πρόταση 6.5 έχουμε $|R| = 5^2 = 25$.
Επειδή $x^2 + 1 = (x-1)(x-2)$ και τα πολυώνυμα $x-2, x-3 \in \mathbb{Z}_5[x]$ είναι σχετικά πρώτα, έχουμε $< x^2+1 >=< x-2 > \cap < x-3 >$ σύμφωνα με το Παράδειγμα 5.26(2). Τα ιδεώδη $< x-2 >, < x-3 >$ είναι σχετικά πρώτα καθώς, για παράδειγμα, $1 = (x-2) - (x+3) \in < x-2 > + < x-3 >$. Από το Κινέζικο θεώρημα υπολοίπων έχουμε

$$S \simeq \mathbb{Z}_5[x]/ < x-2 > \times \mathbb{Z}_5[x]/ < x-3 > \simeq \mathbb{Z}_5 \times \mathbb{Z}_5,$$

όπου στον δεξιό ισομορφισμό χρησιμοποιήσαμε το Παράδειγμα 6.5(1). Άρα το πλήθος των αντιστρέψιμων στοιχείων του S ισούται με το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_5 \times \mathbb{Z}_5$. Όμως ξέρουμε ότι αν A, B είναι δακτύλιοι με μονάδες, τότε $U(A \times B) = U(A) \times U(B)$. Άρα $|S| = |U(\mathbb{Z}_5)| \cdot |U(\mathbb{Z}_5)| = 4 \cdot 4 = 16$. 2ος τρόπος. Ένας άλλος τρόπος να υπολογίσουμε το $|U(S)|$ είναι να βρούμε το πλήθος των πολυωνύμων της μορφής $ax + b \in \mathbb{Z}_5[x]$ που δεν έχουν ρίζα ούτε το $2 \in \mathbb{Z}_5$ ούτε το $3 \in \mathbb{Z}_5$.

14. i) Υπόδειξη. Παρατηρήστε ότι $x^3 - x = x(x-1)(x-4)$ και τα ιδεώδη $< x >, < x-1 >, < x-4 >$ του $\mathbb{Z}_5[x]$ είναι ανά δύο σχετικά πρώτα. Εφαρμόστε το Κινέζικο θεώρημα υπολοίπων και το Παράδειγμα 6.12 (1) για να συμπεράνετε ότι $R \simeq \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Από την άσκηση 6.8 έχουμε $|U(R)| = |U(\mathbb{Z})|^3 = 4^3$. Παρατηρούμε ότι αν φ είναι ο παραπάνω ισομορφισμός και $r \in R$, τότε $\varphi(r^2) = 1 \Leftrightarrow (\varphi(r))^2 = 1$. Συνεπώς το πλήθος των $r \in R$ που ικανοποιούν $r^2 = 1$ ισούται με το πλήθος των $s \in \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$ που ικανοποιούν $s^2 = 1$. Έστω $a, b, c \in \mathbb{Z}_5$. Τότε

$$(a,b,c)^2 = (1,1,1) \Leftrightarrow a^2 = b^2 = c^2 = 1 \Leftrightarrow a, b, c \in \{1, 4\}.$$

Άρα το ζητούμενο πλήθος είναι 2^3.

ii) Αρχικά παρατηρούμε ότι αν οι R, S είναι ισόμορφοι, τότε έχουν το ίδιο πλήθος στοιχείων. Από την Πρόταση 6.5 $|R| = 5^3$ και $|S| = 5^n$, επομένως $n = 3$. Το πλήθος των ιδεωδών του R είναι, σύμφωνα με το Παράδειγμα 4 μετά την Πρόταση 6.9, 2^3, και το πλήθος των ιδεωδών του S είναι $(n_1+1)...(n_s+1)$, όπου $p_1(x)^{n_1}...p_s(x)^{n_s}$ είναι η ανάλυση του $x^3 + ax \in \mathbb{Z}_5[x]$ σε γινόμενο μονικών ανάγωγων. Λαμβάνοντας βαθμούς βλέπουμε ότι έχουμε δύο περιπτώσεις.
(1) $p_i(x) = x - a_i, i = 1, 2, 3$ και τα a_i είναι διακεκριμένα. Στην περίπτωση αυτή εφαρμόζει το Κινεζικό θεώρημα υπολοίπων όπως ακριβώς στο προηγούμενο υποερώτημα και $S \simeq \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Άρα $R \simeq S$.
(2) Χωρίς περιορισμό της γενικότητας, $p_1(x) = x$ και $p_2(x) = x^2 + a$. Στην περίπτωση αυτή το πλήθος των ιδεωδών του S είναι ίσο με $(1+1)(2+1) = 6 \neq 8$. Άρα οι R, S δεν είναι ισόμορφοι.
Από τα παραπάνω βλέπουμε ότι οι δακτύλιοι R, S είναι ισόμορφοι αν και μόνο αν το πολυώνυμο $x^3 + ax$ αναλύεται σε γινόμενο πρωτοβάθμιων παραγόντων στο $\mathbb{Z}_5[x]$. Εξετάζοντας μία προς μία τις περιπτώσεις $a = 0, 1, 2, 3, 4 \in \mathbb{Z}_5$ κατά τα γνωστά - οι πράξεις παραλείπονται, είναι παρόμοιες με το Παράδειγμα 4.22(2) - βρίσκουμε ότι η απάντηση είναι $a = 1, 4$.

15. *Λύση.*

i) Από το Παράδειγμα 4.2 έχουμε $f(x)^p = f(x^p)$ για κάθε $f(x) \in \mathbb{Z}_p[x]$. Επειδή στο $\mathbb{Z}_p[x]/ < x^p - x >$ έχουμε $x^p + < x^p - x >= x + < x^p - x >$, εύκολα επαληθεύεται ότι

$$f(x^p) + < x^p - x >= f(x) + < x^p - x >$$

για κάθε $f(x) \in \mathbb{Z}_p[x]$. Άρα $f(x)^p + < x^p - x >= f(x) + < x^p - x >$ για κάθε $f(x) \in \mathbb{Z}_p[x]$, δηλαδή $(f(x) + < x^p - x >)^p = f(x) + < x^p - x >$, που είναι το ζητούμενο.
2ος τρόπος. Υπόδειξη. Ξέρουμε ότι $x^p - x = x(x-1)...(x-(p-1))$. Από αυτό και το Κινεζικό θεώρημα υπολοίπων έπεται ότι $R \simeq \mathbb{Z}_p \times ... \times \mathbb{Z}_p$ (p παράγοντες). Τότε

το ζητούμενο έπεται από το μικρό θεώρημα του Fermat καθώς για κάθε $a_i \in \mathbb{Z}_p$ είναι

$$(a_1, ..., a_p)^p = (a_1^p, ..., a_p^p) = (a_1, ..., a_p).$$

ii) Έστω ότι $\varphi : R \to \mathbb{Z}_p[x]/ < g(x) >$ είναι ισομορφισμός δακτυλίων. Από την Πρόταση 6.5 έπεται ότι $degg(x) = deg(x^p - x)$. Από το προηγούμενο υποερώτημα, έχουμε ότι $(\varphi(r))^p = \varphi(r)$ για κάθε $r \in R$. Καθώς η φ είναι επί, έχουμε ότι $s^p = s$ για κάθε $s \in \mathbb{Z}_p[x]/ < g(x) >$. Ειδικά έχουμε

$$x^p + < g(x) >= x + < g(x) > \Rightarrow g(x)|x^p - x.$$

Επειδή το $g(x)$ είναι μονικό και βαθμού p, έπεται ότι $g(x) = x^p - x$.

16. *Λύση.* Έστω ότι $\mathbb{Z}_p[x]/ < x^2 + 1 > \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. Το δεξί μέλος δεν είναι περιοχή καθώς $([1], [0])([0], [1]) = ([0], [0])$ και $([1], [0]), ([0], [1]) \neq ([0], [0])$. Άρα δεν είναι σώμα. Συνεπώς και το αριστερό μέλος δεν είναι σώμα. Αυτό σημαίνει ότι το πολυώνυμο $x^2 + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_p[x]$ σύμφωνα με το Θεώρημα 6.8. Επειδή ο βαθμός του είναι 2, αυτό σημαίνει ότι έχει ρίζα στο $\mathbb{Z}_p$, δηλαδή υπάρχει $a \in \mathbb{Z}_p$ τέτοιο ώστε $a^2 = -1$. Αυτό είναι αδύνατο από την άσκηση 2.12.

17. 1ος τρόπος. *Λύση.* Από την Πρόταση 6.5 ξέρουμε ότι κάθε στοιχείο του R γράφεται μοναδικά στη μορφή $f(x) + I$, όπου $degf(x) < m + n$. Επίσης, $|R| = p^{m+n}$. Από το Θεώρημα 6.6, το $f(x) + I$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(f(x), x^m(x-1)^n) = 1$. Επειδή τα πολυώνυμα $x^m, (x-1)^n$ είναι σχετικά πρώτα έχουμε σύμφωνα με τη άσκηση 1.7

$$\mu\kappa\delta(f(x), x^m(x-1)^n) = 1 \Leftrightarrow \mu\kappa\delta(f(x), x^m) = \mu\kappa\delta(f(x), (x-1)^n) = 1 \Leftrightarrow$$
$$\mu\kappa\delta(f(x), x) = \mu\kappa\delta(f(x), x-1) = 1 \Leftrightarrow$$
$$x \nmid f(x) \text{ και } x - 1 \nmid f(x),$$

όπου στη δεύτερη ισοδυναμία χρησιμοποιήσαμε ότι τα πολυώνυμα $x, x-1$ είναι ανάγωγα. Θεωρούμε τα σύνολα

$$A = \{f(x) \in \mathbb{Z}_p[x] : degf(x) < m + n, f(x) = xh(x), h(x) \in \mathbb{Z}_p[x]\},$$
$$B = \{f(x) \in \mathbb{Z}_p[x] : degf(x) < m + n, f(x) = (x-1)h(x), h(x) \in \mathbb{Z}_p[x]\}.$$

Τότε

$$A \cap B = \{x(x-1)h(x) \in \mathbb{Z}_p[x] : degh(x) < m + n - 2\}.$$

Είναι σαφές ότι

$$|A| = |B| = p^{m+n-1} \text{ και } |A \cap B| = p^{m+n-2}.$$

Από τα παραπάνω έπεται ότι το πλήθος των αντιστρέψιμων στοιχείων του R είναι ίσο με

$$|R| - |A \cup B| = |R| - |A| - |B| + |A \cap B| =$$
$$p^{m+n} - p^{m+n-1} - p^{m+n-1} + p^{m+n-2} = (p^m - p^{m-1})(p^n - p^{n-1}).$$

2ος τρόπος. *Υπόδειξη.* Χρησιμοποιώντας το Κινεζικό θεώρημα υπολοίπων και την άσκηση 6.8, δείξτε ότι $|U(R)| = |U(R_1)| \times |U(R_2)|$, όπου

$$R_1 = \mathbb{Z}_p[x]/ < x^m >, \quad R_2 = \mathbb{Z}_p[x]/ < (x-1)^n > .$$

Στη συνέχεια δείξτε ότι $|U(R_1)| = p^m - p^{m-1}$ και $|U(R_2)| = p^n - p^{n-1}$ με τη βοήθεια της Πρότασης 6.5 και του Θεωρήματος 6.6.

18. *Λύση.* i) Θεωρούμε τον δακτύλιο $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{C} : a, b \in \mathbb{Q}\}$ και την απεικόνιση

$$\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}], \quad a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Εύκολα επαληθεύεται ότι η φ είναι ομομορφισμός δακτυλίων (βλ. Παράδειγμα 5.2(4) για παρόμοιο υπολογισμό). Έστω τώρα

$$f(x) = f_n x^n + \cdots + f_1 x + f_0 \in \mathbb{Q}[x] \quad \text{και} \quad f(a + b\sqrt{2}) = 0,$$

όπου $a, b \in \mathbb{Q}$. Τότε εφαρμόζοντας τον ομομορφισμό φ παίρνουμε

$$f_n(a + b\sqrt{2})^n + \cdots + f_1(a + b\sqrt{2}) + f_0 = 0.$$

Επομένως $f_n(a-b\sqrt{2})^n + \cdots + f_1(a-b\sqrt{2}) + f_0 = 0 \Rightarrow f(a-b\sqrt{2}) = 0$.
ii) Ορίζουμε

$$\psi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}], \quad f(x) \mapsto f(\sqrt{2}).$$

Εύκολα επαληθεύεται ότι η ψ επιμορφισμός δακτυλίων. Έχουμε,

$$\ker\psi = \{f(x) \in Q[x] : f(\sqrt{2}) = 0\}.$$

Χρησιμοποιώντας το $i)$ έχουμε

$$\begin{aligned} f(\sqrt{2}) = 0 \quad &\Leftrightarrow \quad f(-\sqrt{2}) = f(\sqrt{2}) = 0 \\ &\Leftrightarrow \quad x-(-\sqrt{2}) \mid f(x) \ \text{ στο } \ \mathbb{Q}[\sqrt{2}][x] \quad \text{και} \quad x-\sqrt{2} \mid f(x) \ \text{ στο } \ \mathbb{Q}[\sqrt{2}][x] \\ &\Leftrightarrow \quad (x-(-\sqrt{2}))(x-\sqrt{2}) \mid f(x) \ \text{ στο } \ \mathbb{Q}[\sqrt{2}][x] \\ &\Leftrightarrow \quad x^2-2 \mid f(x) \ \text{ στο } \ \mathbb{Q}[\sqrt{2}][x] \Leftrightarrow x^2-2 \mid f(x) \ \text{ στο } \ \mathbb{Q}[x], \end{aligned}$$

όπου στη τελευταία συνεπαγωγή χρησιμοποιήσαμε το ανάλογο του λήμματος 4.29: Αν $a(x), b(x) \in \mathbb{Q}[x]$, τότε $a(x) \mid b(x)$ στο $\mathbb{Q}[x]$ αν και μόνο αν $a(x) \mid b(x)$ στο $\mathbb{Q}[\sqrt{2}][x]$. Επομένως $f(x) \in \ker\psi \Leftrightarrow x^2-2 \mid f(x)$ στο $\mathbb{Q}[x]$, δηλαδή $\ker\psi =< x^2-2 >$. Από το πρώτο θεώρημα ισομορφισμών δακτυλίων έπεται ότι $\mathbb{Q}[x]/ < x^2-2 > \simeq \mathbb{Q}[\sqrt{2}]$.

19. *Υπόδειξη.* Έστω $x = 1$ και $y \in F - \{0,1\}$. Δείξτε ότι $(1+y)^3 - 1^3 - y^3 = y(1+y) \neq 0$.

20. *Απάντηση.* Αληθεύει, δεν αληθεύει, δεν αληθεύει, αντίστοιχα.

21. *Λύση.* Θεωρούμε τη σύνθεση

$$\varphi : R \xrightarrow{\pi_1} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}_5,$$

όπου π_1 είναι η προβολή στην πρώτη συντεταγμένη, $\pi_1(a,b) = a$, και π ο φυσικός επιμορφισμός, $\pi(a) = [a]$. Ως σύνθεση επιμορφισμών δακτυλίων, η φ είναι επιμορφισμός δακτυλίων. Έχουμε ότι

$$\ker\varphi = \{(a,b) \in R : [a] = 0\} = \{(5x,b) \in R : x, b \in \mathbb{Z}\} = I,$$

οπότε από το πρώτο θεώρημα ισομορφισμών προκύπτει ότι $R/I \simeq \mathbb{Z}_5$. Επειδή ο 5 είναι πρώτος, ο δακτύλιος $\mathbb{Z}_5$ είναι σώμα, οπότε ο R/I είναι σώμα.

22. *Λύση.* Θεωρούμε την απεικόνιση $\varphi : \mathbb{Z} \to R, \quad m \mapsto m1_R$. Από την Πρόταση 3.15 (4),(5) έπεται ότι είναι ομομορφισμός δακτυλίων. Ο πυρήνας $\ker\varphi$ είναι ιδεώδες του $\mathbb{Z}$ και επομένως υπάρχει μη αρνητικός ακέραιος k με $\mathbb{Z} =< k >$ σύμφωνα με το Θεώρημα 6.6. Θα δείξουμε ότι $k = n$.

Ο k είναι θετικός, γιατί αλλιώς ο $\varphi : \mathbb{Z} \to R$ θα ήταν 1-1, πράγμα αδύνατο καθώς το σύνολο R είναι πεπερασμένο. Παρατηρούμε ότι για κάθε $r \in R$ είναι

$$kr = k(1_R r) = (k1_R)r = 0_R r = 0_r.$$

Συνεπώς από την υπόθεση του ελαχίστου του n, έπεται ότι $n \leq k$. Από την άλλη μεριά, η υπόθεση ότι $n1_R = 0_R$ λέει ότι $n \in \ker\varphi =< k >$, δηλαδή $k|n$. Επειδή $n > 0$ παίρνουμε $k \leq n$. Άρα $k = n$.

Έχοντας δείξει ότι $\ker\varphi =< n >$, το πρώτο θεώρημα ισομορφισμών δίνει ότι υπάρχει μονομορφισμός $\mathbb{Z}/ < n > \to R$, δηλαδή μονομορφισμός $\mathbb{Z}_n \to R$. Επειδή τα σύνολα $\mathbb{Z}_n$ και R είναι πεπερασμένα και έχουν το ίδιο πλήθος στοιχείων, η προηγούμενη απεικόνιση είναι ισομορφισμός. Αποδείξαμε ότι $R \simeq \mathbb{Z}_n$.

23. *Λύση.* Η μία κατεύθυνση είναι άμεση καθώς κάθε σώμα είναι περιοχή.

Επειδή το F είναι σώμα, το Θεώρημα 6.6 δίνει ότι $I =< p(x) >$ για κάποιο $p(x) \in F[x]$. Θα δείξουμε ότι αν ο δακτύλιος $F[x]/I$ είναι περιοχή, τότε το $p(x)$ είναι ανάγωγο στο $F[x]$.

Πράγματι, είναι $p(x) \neq 0$ αφού $I \neq \{0\}$. Επίσης $degp(x) > 0$, γιατί αλλιώς θα είχαμε ότι το ιδεώδες I περιέχει αντιστρέψιμο στοιχείο, οπότε θα είχαμε ότι $I = F[x]$ και $F[x]/I$ θα ήταν ο μηδενικός δακτύλιος, αδύνατο αφού είναι περιοχή. Έστω τώρα ότι $p(x) = a(x)b(x)$, όπου $a(x), b(x) \in F[x]$. Τότε στο πηλίκο έχουμε

$$p(x) + I = a(x)b(x) + I \Rightarrow I = (a(x)+I)(b(x)+I).$$

Επειδή ο δακτύλιος $F[x]/I$ είναι περιοχή παίρνουμε

$$a(x)+I=I \ \text{ ή } \ b(x)+I=I \Rightarrow a(x)\in I \ \text{ ή } \ b(x)\in I \Rightarrow$$

$$p(x)|a(x) \ \text{ ή } \ p(x)|a(x) \Rightarrow \deg a(x)\geq \deg p(x) \ \text{ ή } \ \deg b(x)\geq \deg p(x).$$

Άρα το $p(x)\in F[x]$ είναι ανάγωγο. Από το Θεώρημα 6.8 έπεται ότι το $F[x]/I$ είναι σώμα.

24. *Λύση.* Έστω επιμορφισμός δακτυλίων $\varphi : F[x]\to S$, όπου F σώμα και S περιοχή που δεν είναι σώμα. Από το πρώτο θεώρημα ισομορφισμών έχουμε $F[x]/I\simeq S$, όπου $I=\ker\varphi$. Επειδή ο S είναι περιοχή και όχι σώμα, η προηγούμενη άσκηση δίνει $I=\{0\}$. Άρα ο φ είναι ισομορφισμός.

Έστω $\varphi:\mathbb{Q}[x]\to\mathbb{Z}$ ομομορφισμός δακτυλίων. Θα δείξουμε ότι ο φ είναι ο μηδενικός ομομορφισμός.

Από τη σχέση $\varphi(1)^2=\varphi(1)$, έπεται ότι $\varphi(1)\in\{0,1\}$. Αν $\varphi(1)=0$, τότε για κάθε $f(x)\in\mathbb{Q}[x]$ είναι $\varphi(f(x))=\varphi(1f(x))=\varphi(1)\varphi(f(x))=0$, δηλαδή ο φ είναι ο μηδενικός ομομορφισμός. Αν $\varphi(1)=1$, τότε για κάθε ακέραιο m έχουμε $\varphi(m)=m\varphi(1)=m$, που σημαίνει ότι ο φ είναι επί. Από το πρώτο ερώτημα της παρούσας άσκησης, έπεται ότι ο φ είναι 1-1. Αυτό είναι άτοπο, γιατί αν $\varphi(x)=k$, τότε $\varphi(x)=\varphi(k)$.

25. *Απαντήσεις.*

i) $U(R)=\{\begin{pmatrix}\pm1 & b\\ 0 & \pm1\end{pmatrix}\in M_2(\mathbb{Z})\}$.

ii)

iii) $R\to\mathbb{Z}_4\times\mathbb{Z}_8,\ \begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\mapsto([a]_4,[c]_8)$.

iv) $|R/I|=|\mathbb{Z}_4|\times|\mathbb{Z}_8|=4\dot{8}=32$ και $|U(R/I)|=|U(\mathbb{Z}_4)|\cdot|U(\mathbb{Z}_8)|=2\cdot4=8$.

26. *Απάντηση.* $n=1$ ή $n=$ δύναμη πρώτου.

27. *Λύση.* Έστω p_i διακεκριμένοι πρώτοι, $i=1,2,...,1821$. Εφαρμόζοντας το Πόρισμα 6.15 προκύπτει άμεσα ότι υπάρχει ακέραιος r που ικανοποιεί τις παρακάνω ισοτιμίες,

$$r\equiv -i \mod p_i^{1453},\ i=1,2,...,1821.$$

Τότε οι 1821 διαδοχικοί ακέραιοι $r+1, r+2, ..., r+1821$ έχουν τη ζητούμενη ιδιότητα.

28. *Υπόδειξη.* Δείξτε ότι η απεικόνιση $a_0+a_1x+a_2x^2+...+a_nx^n\mapsto\begin{pmatrix}a_0 & a_1 & a_2\\ 0 & a_0 & a_1\\ 0 & 0 & a_0\end{pmatrix}$, είναι επιμορφισμός δακτυλίων με πυρήνα το $<x^3>$.

29. *Λύση.* Όχι. Κάθε πεπερασμένη περιοχή είναι σώμα (Πρόταση 3.14) και κάθε πεπερασμένο σώμα έχει πληθάριθμο δύναμη πρώτου (Θεώρημα 6.19).

30. *Υπόδειξη.* Βρείτε $a\in\mathbb{Z}_{11}$ με $f(x+a)=g(x)$ και θεωρήστε τον αυτομορφισμό

$$\mathbb{Z}_{11}[x]\to\mathbb{Z}_{11}[x], h(x)\mapsto h(x+a).$$

Επαναληπτικές Ασκήσεις: Κεφάλαια 3-6

1. Έστω R πεπερασμένος μεταθετικός δακτύλιος με μονάδα. Δείξτε ότι κάθε στοιχείο του R που δεν είναι αντιστρέψιμο είναι μηδενοδιαιρέτης. Στη συνέχεια βρείτε παράδειγμα δακτυλίου R με μονάδα για τον οποίο το προηγούμενο συμπέρασμα δεν αληθεύει.
2. Δείξτε ότι αν R είναι υποδακτύλιος του $\mathbb{Z}_n$ τέτοιος ώστε $[77], [250] \in R$, τότε $R = \mathbb{Z}_n$.
3. Έστω R περιοχή τέτοια ώστε υπάρχει μη μηδενικό $a \in R$ με $6a = 0_R$. Δείξτε ότι ισχύει ακριβώς ένα από τα ακόλουθα.
   - $2r = 0_R$ για κάθε $r \in R$.
   - $3r = 0_R$ για κάθε $r \in R$.
4. Δείξτε ότι το σύνολο $R = \mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$ είναι υποδακτύλιος του $\mathbb{C}$ και βρείτε τα αντιστρέψιμα στοιχεία του.
5. Έστω R δακτύλιος τέτοιος ώστε $r^2 = r$ για κάθε $r \in R$. Δείξτε ότι ο R είναι μεταθετικός.
6. Έστω p πρώτος, $f(x) = x^4 + 3x + 4 \in \mathbb{Z}_p[x]$ και $g(x) = x^2 + x + 1 \in \mathbb{Z}_p[x]$. Βρείτε το $\mu\kappa\delta(f(x), g(x))$ για τις διάφορες τιμές του p.
7. Έστω p πρώτος και $f(x) = (x^2 + 1)^p - (x^2 + 1) \in \mathbb{Z}_p[x]$.
   i) Δείξτε ότι $x^p - x | f(x)$ στο $\mathbb{Z}_p[x]$.
   ii) Βρείτε το $\mu\kappa\delta(f(x), x(x-1))$.
   iii) Βρείτε την ανάλυση του $f(x) \in \mathbb{Z}_p[x]$ σε γινόμενο μονικών αναγώγων για $p = 2$ και $p = 3$.
8. i) Βρείτε όλους τους ομομορφισμούς δακτυλίων $\mathbb{Z} \to \mathbb{Q}$.
   ii) Βρείτε όλους τους ομομορφισμούς δακτυλίων $\mathbb{Q} \to \mathbb{Z}$.
   iii) Έστω R άπειρο σώμα και S πεπερασμένος δακτύλιος. Βρείτε όλους τους ομομορφισμούς δακτυλίων $R \to S$.
   iv) Βρείτε όλους τους επιμορφισμούς δακτυλίων $\mathbb{Z} \to \mathbb{Z}_{10}$.
9. Έστω m, n σχετικά πρώτοι ακέραιοι.
   i) Έστω R δακτύλιος τέτοιος ώστε υπάρχουν $a, b \in R$ με $ma = nb = 0$. Δείξτε ότι $ab = 0$.
   ii) Υποθέτουμε επιπλέον ότι $m, n > 1$. Αληθεύει ότι υπάρχει περιοχή που περιέχει υποδακτύλιους R_1, R_2 με $R_1 \simeq \mathbb{Z}_m, R_2 \simeq \mathbb{Z}_n$;
10. i) Διατυπώστε τον ορισμό του ιδεώδους δακτυλίου. Δώστε παράδειγμα δακτυλίου R και υποδακτύλιου S του R που δεν είναι ιδεώδες του R.
    ii) Βρείτε με απόδειξη τα ιδεώδη σώματος.
    iii) Έστω F σώμα. Δείξτε ότι κάθε ιδεώδες του $F[x]$ είναι κύριο.
    iv) Βρείτε τα ιδεώδη I του $\mathbb{Z}_3[x]$ με $< x^3 + x + 1 > \subseteq I$.
11. i) Διατυπώστε τον ορισμό του αθροίσματος $I + J$ δύο ιδεωδών I, J δακτυλίου R.
    ii) Έστω $m, n \in \mathbb{Z}_{>0}$, $d = \mu\kappa\delta(m, n)$ και $e = \varepsilon\kappa\pi(m, n)$. Δείξτε ότι $< m > \cap < n > = < e >$ και $< m > + < n > = < d >$.
    iii) Βρείτε τα ιδεώδη I του $\mathbb{Z}$ με $48\mathbb{Z} \subseteq I \subseteq 12\mathbb{Z}$.
12. Θεωρούμε το δακτύλιο $R = T_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}\}$ και τις απεικονίσεις

$$\varphi : R \to \mathbb{Z}_3, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto [a],$$

$$\psi : R \to \mathbb{Z}_3, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto [b].$$

    i) Εξετάστε αν η φ είναι ομομορφισμός δακτυλίων και, σε περίπτωση που είναι, υπολογίστε τον πυρήνα της.

ii) Εξετάστε αν η ψ είναι ομομορφισμός δακτυλίων και, σε περίπτωση που είναι, υπολογίστε τον πυρήνα της.

iii) Δείξτε ότι το σύνολο $I = \{\begin{pmatrix} 3a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}\}$ είναι ιδεώδες του R και $R/I \simeq \mathbb{Z}_3$.

iv) Βρείτε ιδεώδες J του R με $R/J \simeq \mathbb{Z}_3 \times \mathbb{Z}$.

13. Θεωρούμε το δακτύλιο $\mathbb{Z}_3[x]$, το ιδεώδες $I =< x^2 + x + 1 >$ του $\mathbb{Z}_3[x]$ και το δακτύλιο πηλίκο $R = \mathbb{Z}_3[x]/I$.
    i) Βρείτε, εφόσον υπάρχει, το αντίστροφο στο R του $x^3 + I$.
    ii) Πόσα είναι τα αντιστρέψιμα στοιχεία του R;
    iii) Είναι σωστό ότι οι δακτύλιοι R και $\mathbb{Z}_3[x]/ < x^2 + 1 >$ είναι ισόμορφοι;

Ενδεικτικές Λύσεις Επαναληπτικών Ασκήσεων

1. Καθώς ο R είναι πεπερασμένος, έστω $R = \{r_1, ..., r_n\}$. Έστω $r \in R$ μη αντιστρέψιμο. Επειδή ο R είναι μεταθετικός, έχουμε $rr_i \neq 1_R$ για κάθε $i = 1, ..., n$. Δηλαδή $rr_i \in R - \{1_R\}$ για κάθε $i = 1, ..., n$. Επειδή το σύνολο $R - \{1_R\}$ έχει $n - 1 < \infty$ στοιχεία, υπάρχουν $i \neq j$ με $rr_i = rr_j$. Τότε $r(r_i - r_j) = 0_R$ με $r_i - r_j \neq 0_R$, που σημαίνει το r είναι μηδενοδιαιρέτης.
   Ένα παράδειγμα δακτυλίου R με μονάδα για τον οποίο το συμπέρασμα της άσκησης δεν αληθεύει είναι οι ακέραιοι.
   Παρατηρήσεις. 1) Προφανώς η άσκηση 6 έπεται από την 7. Δώσαμε διαφορετικές λύσεις γιατί το αλατοπίπερο νοστιμίζει.
   2) Καλό είναι να συγκριθεί η απόδειξη της άσκησης 7 με την απόδειξη της Πρότασης 3.14. Η βασική ιδέα είναι παρόμοια.
   3) Μπορεί να αποδειχθεί το συμπέρασμα της άσκησης 7 χωρίς τη χρήση της υπόθεσης περί μεταθετικότητας, συγκεκριμένα: Αν R είναι πεπερασμένος δακτύλιος με μονάδα, τότε για κάθε $a \in R - U(R)$, υπάρχει μη μηδενικό $b \in R$ με $ab = ba = 0_R$. Πράγματι, θεωρώντας τα στοιχεία $a, a^2, a^3, ...$ του R υπάρχουν $m > n \geq 0$ με $a^m = a^n$. Επειδή το a δεν είναι αντιστρέψιμο ισχύει $n > 0$. Θεωρούμε μια επιλογή των m, n με m ελάχιστο. Για $b = a^{m-1} - a^{n-1} \in R$ έχουμε $ab = ba = 0$. Από το ελάχιστο του m έπεται ότι $b \neq 0_R$.

2. Εύκολα επαληθεύεται ότι $\mu\kappa\delta(77, 250) = 1$ και επομένως υπάρχουν ακέραιοι x, y με $1 = x \cdot 77 + y \cdot 250$. Άρα στο $\mathbb{Z}_n$ έχουμε $[1] = x[77] + y[250]$. Επειδή $[77], [250] \in R$ και ο R είναι υποδακτύλιος του $\mathbb{Z}_n$, παίρνουμε

$$x[77] + y[250] \in R \Rightarrow [1] \in R \Rightarrow [m] = m[1] \in R$$

   για κάθε $m \in \mathbb{Z}$. Άρα $\mathbb{Z}_n \subseteq R$ και συνεπώς $\mathbb{Z}_n = R$.

3. Από την υπόθεση έχουμε $(61_R)a = 6(1_R a) = 6a = 0_R$. Επειδή ο R είναι περιοχή και το $a \in R$ είναι μη μηδενικό παίρνουμε $61_R = 0_R$. Άρα $(21_R)(31_R) = 0_R$ και επειδή ο R είναι περιοχή έπεται ότι $21_R = 0_R$ ή $31_R = 0_R$. Στην πρώτη περίπτωση έχουμε για κάθε $r \in R$ ότι $2r = (21_R)r = 0_R r = 0_R$. Όμοια στη δεύτερη περίπτωση έχουμε $3r = 0_R$ για κάθε $r \in R$.
   Τέλος αν για κάθε $r \in R$ ισχύει $2r = 0_R$ και $3r = 0_R$, τότε $r = 3r - 2r = 0_R - 0_R = 0_R$. Δηλαδή $R = \{0_R\}$, αδύνατο επειδή ο R είναι περιοχή.

4. Το σύνολο $\mathbb{Z}[\sqrt{-3}]$ είναι υποδακτύλιος του $\mathbb{C}$. Πράγματι, είναι σαφές ότι το σύνολο R είναι μη κενό. Αν $a, b, c, d \in \mathbb{Z}$, τότε έχουμε,

$$(a + bi\sqrt{3}) - (c + di\sqrt{3}) = (a - c) + (b - d)i\sqrt{3} \in \mathbb{Z}[\sqrt{-3}], \text{ και}$$

$$(a + bi\sqrt{3})(c + di\sqrt{3}) = (ac - 3bd) + (ad + bc)i\sqrt{3} \in \mathbb{Z}[\sqrt{-3}].$$

   Θα δείξουμε ότι $U(R) = \{1, -1\}$.
   Πράγματι, είναι σαφές ότι $\{1, -1\} \subseteq U(R)$.
   Έστω $a + bi\sqrt{3} \in U(R)$, όπου $a, b \in \mathbb{Z}$. Τότε υπάρχουν $c, d \in \mathbb{Z}$ ώστε $(a + bi\sqrt{3})(c + di\sqrt{3}) = 1$. Παίρνοντας μέτρα μιγαδικών και χρησιμοποιώντας ότι $|z_1 z_2| = |z_1||z_2|$, όπου $z_1, z_2 \in \mathbb{C}$, έχουμε,

$$|(a + bi\sqrt{3})||(c + di\sqrt{3}| = 1 \Rightarrow |(a + bi\sqrt{3})|^2|(c + di\sqrt{3}|^2 = 1 \Rightarrow (a^2 + 3b^2)(c^2 + 3d^2) = 1.$$

   Επειδή $a, b, c, d \in \mathbb{Z}$, παίρνουμε $(a, b) = (1, 0), (-1, 0)$. Άρα $U(R) \subseteq \{1, -1\}$. Συνεπώς $U(R) = \{1, -1\}$.

5. Χρησιμοποιώντας δύο φορές την υπόθεση έχουμε για κάθε $r \in R$

$$-r = (-r)^2 = (-r)(-r) = r^2 = r.$$

Για κάθε $a, b \in R$ έχουμε

$$a + b = (a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2 = a + ab + ba + b$$

και επομένως $ba = -(ab)$. Από την πρώτη σχέση έχουμε $-(ab) = ab$ οπότε ba=ab.

6. Όπως η άσκηση 4.4.

7. Τα a, c όπως η άσκηση 4.24.

   Ο μκδ στο b είναι το $x(x-1)$. Ένας τρόπος δικαιολόγησης ανεξάρτητος από το a είναι ο εξής. Έχουμε $f(0) = 0$ και άρα $x|f(x)$ στο $\mathbb{Z}_p[x]$. Από το μικρό θεώρημα του Fermat, $f(1) = 2^p - 2 = 0$ και άρα $x - 1|f(x)$ στο $\mathbb{Z}_p[x]$. Επειδή $p > 1$, είναι $0 \neq 1$, οπότε τα $x, x - 1 \in \mathbb{Z}_p[x]$ είναι σχετικά πρώτα και άρα $x(x - 1)|f(x)$. Άρα ο ζητούμενος μκδ είναι το $x(x - 1)$.

8. i) Αν $\varphi : \mathbb{Z} \to \mathbb{Q}$ είναι ομομορφισμός δακτυλίων, τότε από $1^2 = 1$ έπεται ότι $\varphi(1) = \varphi(1^2) = \varphi(1)^2$ και επομένως $\varphi(1) = 0, 1$. Στην πρώτη περίπτωση η φ είναι η μηδενική απεικόνιση και στη δεύτερη είναι η απεικόνιση $\varphi : \mathbb{Z} \to \mathbb{Q}, a \mapsto a$, διότι για κάθε ακέραιο a και κάθε ομομορφισμό δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Q}$ είναι $\varphi(a) = a\varphi(1)$. Αντίστροφα, είναι σαφές ότι οι δύο αυτές απεικονίσεις είναι πράγματι ομομορφισμοί δακτυλίων.

   ii) Αν $\varphi : \mathbb{Q} \to \mathbb{Z}$ είναι ομομορφισμός δακτυλίων, τότε για κάθε $a \in \mathbb{Q}, m \in \mathbb{Z} - \{0\}$, έχουμε

   $$\varphi(a) = \varphi(m(a/m)) = m\varphi(a/m)$$

   που σημαίνει ότι ο ακέραιος $\varphi(a)$ είναι πολλαπλάσιος κάθε μη μηδενικού ακεραίου, οπότε $\varphi(a) = 0$. Άρα ο μοναδικός ομομορφισμός δακτυλίων $\varphi : \mathbb{Q} \to \mathbb{Z}$ είναι ο μηδενικός.

   iii) Αν $\varphi : R \to S$ είναι ομομορφισμός δακτυλίων τότε ο πυρήνας $ker\varphi$ είναι ιδεώδες του σώματος R και άρα $ker\varphi = \{0\}$ ή $ker\varphi = R$ σύμφωνα με την Πρόταση 5.15(2). Στην πρώτη περίπτωση ο φ είναι 1-1 σύμφωνα με την Πρόταση 5.11. Αυτό είναι αδύνατο, καθώς το σύνολο R είναι άπειρο και το S πεπερασμένο. Άρα υπάρχει μοναδικός ομομορφισμός δακτυλίων $R \to S$, ο μηδενικός.

   iv) Έστω $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$ επιμορφισμός δακτυλίων. Ξέρουμε ότι $\varphi(1) = [1]$ σύμφωνα με την Πρόταση 5.4. Αυτή η σχέση καθορίζει μοναδικά το φ, αφού για κάθε ακέραιο m έχουμε $\varphi(m) = m\varphi(1) = m[1]$. Άρα υπάρχει μοναδικός επιμορφισμός δακτυλίων $\varphi : \mathbb{Z} \to \mathbb{Z}_{10}$, ο φυσικός επιμορφισμός $m \mapsto [m]$.

9. i) Από την υπόθεση υπάρχουν ακέραιοι x, y με $1 = xm + yn$. Άρα στο R έχουμε

   $$1(ab) = (xm)(ab) + (yn)(ab) = (xma)b + (ya)(nb) = 0_R b + (ya)0_R = 0_R,$$

   όπου στη δεύτερη ισότητα χρησιμοποιήσαμε την Πρόταση 3.15(5).

   ii) Έστω ότι υπάρχει τέτοια περιοχή R. Θεωρούμε ισομορφισμούς δακτυλίων $\varphi_1 : \mathbb{Z}_m \simeq R_1, \varphi_2 : \mathbb{Z}_n \simeq R_2$ και τις εικόνες a, b των $[1]_m, [1]_n$ αντίστοιχα. Ισχύει $ma = nb = 0_R$. Πράγματι, $ma = m\varphi_1([1]_m) = \varphi_1(m[1]_m) = \varphi_1([0]_m) = 0_R$, και όμοια για το nb. Από το πρώτο ερώτημα παίρνουμε $ab = 0_R$. Τα $[1]_m, [1]_n$ είναι μη μηδενικά επειδή $m, n > 1$. Ως εικόνες μη μηδενικών στοιχείων κάτω από ισομορφισμούς, τα a, b είναι μη μηδενικά. Αυτό είναι άτοπο αφού R είναι περιοχή και $ab = 0_R$.

10. Τα πρώτα τρία ερωτήματα είναι γνωστά (θεωρία) από την παράγραφο 5.3 των σημειώσεων.

    Για το τέταρτο ξέρουμε ότι κάθε ιδεώδες του $\mathbb{Z}_3[x]$ είναι κύριο γιατί ο δακτύλιος $\mathbb{Z}_3$ είναι σώμα. Έστω I ιδεώδες του $\mathbb{Z}_3[x]$. Υπάρχει $f(x) \in \mathbb{Z}_3[x]$ με $I =< f(x) >$. Επιπλέον ξέρουμε ότι $< f(x) >=< g(x) >$ αν και μόνο αν υπάρχει μη μηδενικό $c \in \mathbb{Z}_3$ με $g(x) = cf(x)$.

    Έχουμε

    $$< x^3 + x + 1 > \subseteq I \Leftrightarrow x^3 + x + 1 \in < f(x) > \Leftrightarrow f(x)|x^3 + x + 1.$$

    Τα παραπάνω δείχνουν ότι τα ζητούμενα ιδεώδη είναι σε 1-1 και επί αντιστοιχία με τους μονικούς διαιρέτες του $x^3 + x + 1$.

Παρατηρούμε ότι το $1 \in \mathbb{Z}_3$ είναι ρίζα του x^3+x+1. Με Ευκλείδεια διαίρεση βρίσκουμε $x^3+x+1 = (x-1)(x^2-x+2)$. Επειδή το x^2-x+2 δεν έχει ρίζα στο $\mathbb{Z}_3$ και είναι βαθμού 2, είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_3[x]$. Έτσι η ανάλυση του x^3+x+1 σε γινόμενα ανάγωγων μονικών είναι $x^3+x+1 = (x-1)(x^2-x+2)$.

Άρα τα ζητούμενα ιδεώδη είναι τα $I =< 1 >, < x-1 >, < x^2-x+2 >, < (x-1)(x^2-x+2) >$, δηλαδή $I = \mathbb{Z}_3[x], < x-1 >, < x^2-x+2 >, < x^3+x+1 >$.

11. Τα πρώτα δύο ερωτήματα είναι γνωστά (θεωρία) από την παράγραφο 5.4 των σημειώσεων. Το τρίτο είναι όπως η άσκηση 5.10.

12. i) Ότι ο φ είναι ομομορφισμός δακτυλίων και $ker\varphi = \{\begin{pmatrix} 3a & b \\ 0 & c \end{pmatrix} : a,b,c \in \mathbb{Z}\}$ είναι υπόθεση ρουτίνας.

    ii) Ο ψ δεν είναι ομομορφισμός δακτυλίων και ένα αντιπαράδειγμα είναι το εξής. Για $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ και $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ έχουμε $\psi(AI_2) \neq \psi(A)\psi(I_2)$. Πράγματι, $\psi(AI_2) = \psi(A) = [1]$, αλλά $\psi(A)\psi(I_2) = [1][0] = [0]$. Στο $\mathbb{Z}_3, [0] \neq [1]$.

    iii) Από το πρώτο ερώτημα, το I είναι πυρήνας του ομομορφισμού φ και άρα είναι ιδεώδες του R. Επειδή η ο ομομορφισμός φ είναι επί, από το 1ο θεώρημα ισομορφισμών παίρνουμε ότι $R/I \simeq \mathbb{Z}_3$.

    iv) Θεωρούμε την απεικόνιση

$$\rho : R \to \mathbb{Z}_3 \times \mathbb{Z}, \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto ([a], c).$$

Είναι θέμα ρουτίνας η επαλήθευση ότι η ρ είναι επιμορφισμός δακτυλίων με πυρήνα

$$J = \{\begin{pmatrix} 3a & b \\ 0 & 0 \end{pmatrix} : a,b \in \mathbb{Z}\}.$$

(Εννοείται ότι σε εξετάσεις αυτοί οι υπολογισμοί πρέπει να υπάρχουν στο γραπτό σας). Από το 1ο θεώρημα ισομορφισμών παίρνουμε ότι $R/J \simeq \mathbb{Z}_3 \times \mathbb{Z}$.

13. i) Όπως το Παράδειγμα 6.7.

    ii) Βρίσκουμε την ανάλυση του x^2+x+1 σε γινόμενο ανάγωγων όπως στο ερώτημα 5iv), $x^2+x+1 = (x-1)^2$. Σύμφωνα με το Θεώρημα 6.6, το $f(x)+I$ είναι αντιστρέψιμο στο R αν και μόνο αν $\mu\kappa\delta(f(x), x^2+x+1) = 1$, ισοδύναμα

$$\mu\kappa\delta(f(x),(x-1)^2) = 1 \Leftrightarrow \mu\kappa\delta(f(x), x-1) = 1 \Leftrightarrow f(1) \neq [0].$$

Σύμφωνα με την Πρόταση 6.5(1), κάθε στοιχείο του R έχει μοναδική παράσταση της μορφής $ax+b+I$, όπου $a,b \in \mathbb{Z}_3$.
Από τα παραπάνω έπεται ότι τα αντιστρέψιμα στοιχεία του R είναι τα $ax+b+I$, όπου $a+b \neq [0]$. Για κάθε $a \in \mathbb{Z}_3$ το b μπορεί να λάβει δύο τιμές αφού, $a+b \neq [0]$. Άρα το ζητούμενο πλήθος είναι $3 \cdot 2 = 6$.

    iii) Είδαμε πριν ότι το x^3+x+1 δεν είναι ανάγωγο στο $\mathbb{Z}_3[x]$, οπότε από το Θεώρημα 6.8, ο δακτύλιος R δεν είναι σώμα. Από την άλλη μεριά, το x^2+1 είναι ανάγωγο στο $\mathbb{Z}_3[x]$ γιατί είναι δευτέρου βαθμού και δεν έχει ρίζα στο $\mathbb{Z}_3$. Άρα ο δακτύλιος $\mathbb{Z}_3[x]/ < x^2+1 >$ είναι σώμα. Συνεπώς οι δακτύλιοι $R, \mathbb{Z}_3[x]/ < x^2+1 >$ δεν είναι ισόμορφοι σύμφωνα με την Πρόταση 5.7(3).

Μέρος 3

Ομάδες

Ομάδες και συμμετρικές ομάδες

Η θεωρία ομάδων, που εξετάζεται στο Μέρος 3 (Κεφάλαια 7-10), αφορά τη μελέτη της έννοιας της συμμετρίας, για παράδειγμα ενός υποσυνόλου του $\mathbb{R}^n$, των ριζών ενός πολυωνύμου, μιας αλγεβρικής δομής, των λύσεων ενός συστήματος διαφορικών εξισώσεων.

Στο κεφάλαιο αυτό εισάγουμε την έννοια της ομάδας, εξετάζουμε μερικά σημαντικά παραδείγματα με έμφαση στις συμμετρικές ομάδες και μελετάμε την έννοια της τάξης στοιχείου.

Βασικά σημεία

- παραδείγματα ομάδων
- συμμετρικές ομάδες
- κύκλοι και ξένοι κύκλοι
- τάξη στοιχείου ομάδας

7.1. Ισομετρίες

Σκοπός μας σε αυτή την παράγραφο είναι να δώσουμε μερικά γεωμετρικά - εποπτικά παραδείγματα αυτών που θα ονομάσουμε *ομάδες* παρακάτω.

Ορισμός 7.1. (1) *Μια απεικόνιση $f : \mathbb{R}^n \to \mathbb{R}^n$ λέγεται* ***ισομετρία*** *αν $d(x, y) = d(f(x), f(y))$ για κάθε $x, y \in \mathbb{R}^n$, όπου $d(x, y)$ η συνήθης Ευκλείδεια απόσταση των x, y .*

(2) *Έστω $M \neq \emptyset$, $M \subseteq \mathbb{R}^n$. Μια ισομετρία $f : \mathbb{R}^n \to \mathbb{R}^n$, ώστε $f(M) = M$ λέγεται* ***συμμετρία*** *του M. Το σύνολο των συμμετριών του M συμβολίζεται με $S(M)$.*

Είναι σαφές ότι η σύνθεση δύο συμμετριών του M είναι συμμετρία του M. Στα παρακάτω θα συμβολίζουμε τη σύνθεση $f \circ g$ με fg. Ειδικά $f \circ f$ θα συμβολίζεται με f^2.

Παραδείγματα 7.2.

(1) Έστω $a \in \mathbb{R}$. Η απεικόνιση

$$t_a : \mathbb{R} \to \mathbb{R}, t_a(x) = a + x$$

είναι ισομετρία. Παρατηρούμε ότι $t_a t_b = t_{a+b}$ για κάθε $a, b \in \mathbb{R}$. Επίσης η απεικόνιση

$$s_a : \mathbb{R} \to \mathbb{R}, s_a(x) = 2a - x$$

είναι ισομετρία. Εύκολα επαληθεύεται ότι s_a^2 είναι η ταυτοτική απεικόνιση $\mathbb{R} \to \mathbb{R}$ και ότι $s_a t_b = s_{b-\frac{a}{2}}$ για κάθε $a, b \in \mathbb{R}$.

Εποπτικά η t_a παριστάνει τη *μετατόπιση* της πραγματικής ευθείας κατά a και s_a παριστάνει την *ανάκλαση* της πραγματικής ευθείας ως προς την κάθετο στο σημείο a.

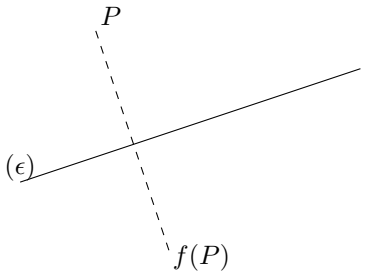
(2) Έστω $\theta \in \mathbb{R}$. Από τη Γραμμική Άλγεβρα θυμόμαστε ότι η γραμμική απεικόνιση $f_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ της οποίας ο πίνακας ως προς τη συνήθη διατεταγμένη βάση του $\mathbb{R}^2$ είναι ο

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

παριστάνει περιστροφή του επιπέδου κατά γωνία θ στη φορά $\circlearrowleft$. Η f_θ είναι ισομετρία.

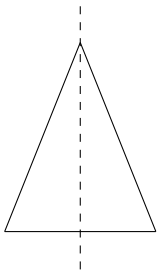
Γενικά, είχαμε αποδείξει στη Γραμμική Άλγεβρα ότι κάθε γραμμική απεικόνιση $\mathbb{R}^n \to \mathbb{R}^n$ της οποίας ο πίνακας ως προς τη συνήθη βάση είναι μοναδιαίος, διατηρεί τη συνήθη Ευκλείδεια απόσταση, δηλαδή είναι ισομετρία.

Μια άλλη οικογένεια ισομετριών του επιπέδου $\mathbb{R}^2$ είναι οι ανακλάσεις ως προς τυχαία ευθεία (ϵ) του επιπέδου, όπως δείχνει το σχήμα



(3) Στη συνέχεια θα δώσουμε μερικά διαισθητικά παραδείγματα συμμετριών συνόλου M. Δεν δικαιολογούμε γιατί οι αναγραφόμενες συμμετρίες του M είναι όλες οι συμμετρίες του M.

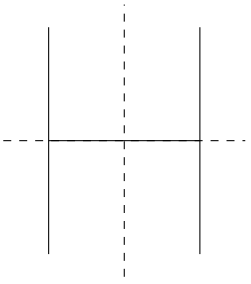
Οι συμμετρίες ισοσκελούς τριγώνου που δεν είναι ισόπλευρο,



$$S(M) = \{1, s\},$$

όπου $1 : \mathbb{R}^2 \to \mathbb{R}^2$, $1(x) = x$, είναι η ταυτοτική απεικόνιση του επιπέδου και $s : \mathbb{R}^2 \to \mathbb{R}^2$ είναι η ανάκλαση ως προς τον κατακόρυφο άξονα. Είναι σαφές ότι $s^2 = 1$.

(4) Οι συμμετρίες του γράμματος Η,



$$S(M) = \{1, s_1, s_2, r\},$$

όπου s_1 η ανάκλαση ως προς τον κατακόρυφο άξονα, s_2 η ανάκλαση ως προς τον οριζόντιο άξονα και r η περιστροφή κατά γωνία 180^o με κέντρο το κέντρο συμμετρίας και φορά $\circlearrowleft$. Παρατηρούμε ότι

$$s_1^2 = s_2^2 = r^2 = 1.$$

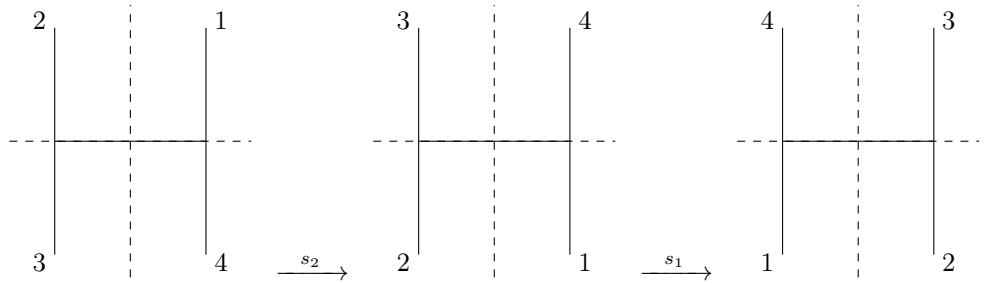
Επίσης, εύκολα επαληθεύονται οι σχέσεις

$$s_1 s_2 = s_2 s_1 = r,$$

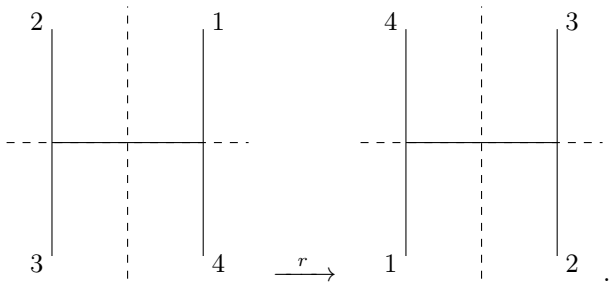
$$s_1 r = r s_1 = s_2,$$

$$s_2 r = r s_2 = s_1.$$

Πράγματι, ας συμβολίσουμε τα επίμαχα σημεία του σχήματος Η με 1,2,3,4. Σχηματικά για τη σύνθεση $s_1 s_2$ έχουμε



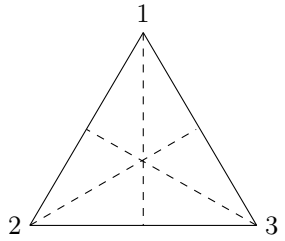
και για την απεικόνιση r έχουμε



.

Άρα $s_1 s_2 = r$.

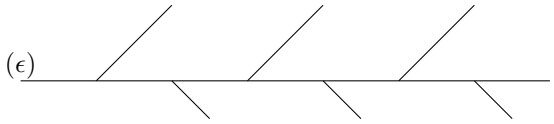
(5) Οι συμμετρίες του ισόπλευρου τριγώνου,



$$S(M) = \{1, s_1, s_2, s_3, r_1, r_2\},$$

όπου s_i η ανάκλαση ως προς άξονα το ύψος που διέρχεται από την κορυφή i $(i = 1, 2, 3)$ και r_j η περιστροφή κατά γωνία $\frac{2\pi}{3} j$ στη φορά $\circlearrowleft, j = 1, 2$. Όπως στο προηγούμενο παράδειγμα, εύκολα επαληθεύεται ότι $s_2 \circ s_1 = r_2$ και $s_1 \circ s_2 = r_1$. Επίσης, $s_i^2 = r_j^3 = 1$, $i = 1, 2, 3, j = 1, 2$.

(6) Άπειρο κλαδί.



Εδώ έχουμε την πραγματική ευθεία (ε) και δύο οικογένειες παράλληλων ευθυγράμμων τμημάτων που τέμνουν την (ε) στα σημεία $a \in \mathbb{Z}$ και που τα δύο μήκη των ευθυγράμμων τμημάτων είναι διαφορετικά. Οι συμμετρίες του M είναι

$$S(M) = \{t_{2a} : a \in \mathbb{Z}\},$$

όπου t_{2a} ορίστηκε στο πρώτο παράδειγμα.

Περισσότερα για συμμετρίες θα δούμε στο Κεφάλαιο 11. Τώρα συνεχίζουμε με την έννοια της ομάδας.

7.2. Ομάδες

Ορισμός 7.3. *Έστω G σύνολο με $G \times G \to G$, $(a, b) \mapsto a \cdot b$ πράξη στο G. Το ζεύγος $(G, \cdot)$ λέγεται* **ομάδα** *αν ισχύουν τα ακόλουθα.*

(1) *$(a \cdot b) \cdot c = a \cdot (b \cdot c)$, για κάθε $a, b, c \in G$ (προσεταιριστική ιδιότητα).*
(2) *Υπάρχει $e \in G$ ώστε $a \cdot e = e \cdot a = a$, για κάθε $a \in G$ (ύπαρξη ουδέτερου στοιχείου).*
(3) *Για κάθε $a \in G$, υπάρχει $a' \in G$ ώστε $a \cdot a' = a' \cdot a = e$ (ύπαρξη αντιστρόφου στοιχείου).*

Αν επιπλέον ισχύει $a \cdot b = b \cdot a$, για κάθε $a, b \in G$ θα λέμε ότι η ομάδα G είναι αβελιανή.

Παρατηρήσεις. Έστω $(G, \cdot)$ ομάδα.

(1) Το e του παραπάνω ορισμού είναι μοναδικό. Πράγματι, αν $e_1, e_2 \in G$ με $e_i \cdot a = a \cdot e_i$, για κάθε $a \in G$, τότε $e_1 = e_1 \cdot e_2 = e_2$.

(2) Για κάθε $a \in G$, το $a' \in G$ του ορισμού είναι μοναδικό. Πράγματι, αν

$$a \cdot a' = a' \cdot a = e \quad \text{και} \quad a \cdot a'' = a'' \cdot a = e,$$

τότε $a'' = e \cdot a'' = (a' \cdot a) \cdot a'' = a' \cdot (a \cdot a'') = a' \cdot e = a'$. Θα συμβολίζουμε το στοιχείο a' με a^{-1}.

(3) Αν $a, b \in G$ και $a \cdot b = e$, τότε $b = a^{-1}$ και $a = b^{-1}$.

(4) Για κάθε $a, b \in G$ ισχύει, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Πράγματι,

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e.$$

Παραδείγματα 7.4.

(1) Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι αβελιανές ομάδες με πράξη την πρόσθεση αριθμών (ουδέτερο στοιχείο το 0). Τα σύνολα $\{1, -1\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ είναι αβελιανές ομάδες με πράξη τον πολλαπλασιασμό αριθμών (ουδέτερο στοιχείο το 1).

(2) Γενικότερα, αν $(R, +, \cdot)$ είναι δακτύλιος τότε $(R, +)$ είναι αβελιανή ομάδα (ουδέτερο στοιχείο το 0_R). Αν $(R, +, \cdot)$ έχει μονάδα 1_R, τότε το $(U(R), \cdot)$ είναι ομάδα (όχι γενικά αβελιανή) (ουδέτερο στοιχείο είναι το 1_R). Υπενθυμίζουμε ότι $U(R)$ είναι το σύνολο των αντιστρέψιμων στοιχείων του R. Ειδικά, αν $R = \mathbb{Z}_n$, τότε έχουμε τις αβελιανές ομάδες $(\mathbb{Z}_n, +)$ και $(U(\mathbb{Z}_n), \cdot)$. Αν $R = M_n(F)$, όπου F σώμα, τότε $(M_n(F), +)$ είναι αβελιανή ομάδα και $(U(M_n(F)), \cdot)$ είναι ομάδα. Υπενθυμίζουμε ότι, όταν το F είναι σώμα,

$$U(M_n(F)) = \{A \in M_n(F) : \det A \neq 0\}.$$

Θα χρησιμοποιούμε το συμβολισμό $GL_n(F) = U(M_n(F))$, και θα καλούμε την ομάδα $GL_n(F)$ τη **γενική γραμμική ομάδα** βαθμού n με συντελεστές στο F.

(3) **Σημαντικό παράδειγμα, μεταθέσεις του X** Έστω X μη κενό σύνολο και

$$S(X) = \{f : X \to X : f \ \ 1-1 \ \text{και επί}\}.$$

Με πράξη την σύνθεση συναρτήσεων, το $S(X)$ είναι ομάδα. Πράγματι έχουμε,

i)
$$(f \circ g) \circ h = f \circ (g \circ h),$$
για κάθε $f, g, h \in S(X)$.

ii) Αν $1_X : X \to X$ είναι η ταυτοτική συνάρτηση $1_x(x) = x$ για κάθε $x \in X$, τότε
$$f \circ 1_X = 1_X \circ f = f,$$
για κάθε $f \in S(X)$.

iii) Αν $f \in S(X)$, τότε η f ως 1-1 και επί συνάρτηση, έχει αντίστροφη συνάρτηση $f^{-1} : X \to X$. Ξέρουμε ότι η f^{-1} είναι 1-1 και επί, δηλαδή $f^{-1} \in S(X)$ και
$$f^{-1} \circ f = f \circ f^{-1} = 1_X.$$

(4) **Ο κύκλος** Έστω $E = \{z \in \mathbb{C} : |z| = 1\}$ ο μοναδιαίος κύκλος. Τότε ως προς τον πολλαπλασιασμό μιγαδικών το E είναι ομάδα. Πράγματι,

i) αν $z_1, z_2 \in E$, τότε $|z_1 z_2| = |z_1||z_2| = 1$. Άρα $z_1 z_2 \in E$.

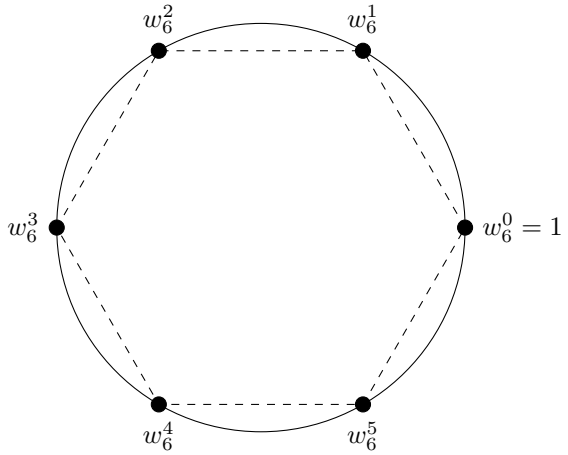
ii) Προφανώς ισχύει $z_1(z_2 z_3) = (z_1 z_2) z_3$, για κάθε $z_i \in E$.

iii) $1 \cdot z = z \cdot 1 = z$, για κάθε $z \in E$.

iv) Αν $z \in E$ τότε $z \neq 0$ και το $\frac{1}{z} \in \mathbb{C}$ ικανοποιεί τη $|\frac{1}{z}| = \frac{1}{|z|} = 1$. Άρα $\frac{1}{z} \in E$. Επίσης έχουμε $z \cdot \frac{1}{z} = 1$.

(5) **n-στες ρίζες της μονάδας** Έστω $n \in \mathbb{Z}_{>0}$. Θέτουμε $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Είναι σαφές ότι το E_n είναι μια ομάδα ως προς τον πολλαπλασιασμό μιγαδικών (όπως πριν). Εδώ έχουμε $|E_n| = n$. Πράγματι, έστω $\omega_n = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n})$. Τότε
$$1, \omega_n, \omega_n^2, ..., \omega_n^{n-1} \in E_n$$
σύμφωνα με το θεώρημα De Moivre που λέει ότι
$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$
Από την ισότητα μιγαδικών εύκολα προκύπτει ότι τα παραπάνω στοιχεία είναι διάφορα ανά δύο, οπότε $|E_n| \geq n$. Επειδή το $\mathbb{C}$ είναι σώμα και το πολυώνυμο $x^n - 1 \in \mathbb{C}[x]$ είναι βαθμού n, παίρνουμε $|E_n| \leq n$ σύμφωνα με την Πρόταση 4.21. Άρα $|E_n| = n$.

Εποπτικά μπορούμε να σκεφτόμαστε τις n-στές ρίζες της μονάδας ως τις κορυφές του κανονικού κυρτού n-γώνου. Για $n = 6$ έχουμε το ακόλουθο σχήμα.



(6) **Αφφινικοί μετασχηματισμοί της ευθείας** Έστω $a, b \in \mathbb{R},\ a \neq 0$. Ορίζουμε
$$T_{a,b} : \mathbb{R} \to \mathbb{R},\ \ T_{a,b}(x) = ax + b.$$
Έστω $G = \{T_{a,b} : a, b \in \mathbb{R},\ a \neq 0\}$. Θα δείξουμε ότι ως προς την σύνθεση συναρτήσεων η G είναι ομάδα. Έστω $T_{a,b}$ και $T_{c,d} \in G$. Τότε
$$\begin{aligned} T_{a,b} \circ T_{c,d}(x) &= T_{a,b}\left(T_{c,d}(x)\right) = T_{a,b}(cx + d) \\ &= a(cx + d) + b = acx + ad + b. \end{aligned}$$

Επειδή $a \neq 0,\ c \neq 0$, έχουμε $ac \neq 0$. Τότε

$$T_{a,b} \circ T_{c,d}(x) = T_{ac,ad+b} \in G.$$

Παρατηρούμε ότι

$$(T_{a,b} \circ T_{c,d}) \circ T_{e,f} = T_{ac,ad+b} \circ T_{e,f} = T_{ace,acf+ad+b}, \text{ και}$$
$$(T_{a,b} \circ (T_{c,d} \circ T_{e,f}) = T_{a,b} \circ T_{ce,cf+d} = T_{ace,acf+ad+b}$$

Άρα ισχύει η προσεταιριστική ιδιότητα.

Για την $T_{1,0}$ ισχύει $T_{1,0}(x) = x$ για κάθε $x \in \mathbb{R}$, άρα

$$T_{1,0} \cdot T_{a,b} = T_{a,b} \cdot T_{1,0} = T_{a,b}$$

για κάθε $T_{a,b} \in G$.

Το στοιχείο $T_{a,b}$ έχει αντίστροφο το $T_{a^{-1},-ba^{-1}}$. Πράγματι,

$$T_{a,b} \circ T_{a^{-1},-ba^{-1}} = T_{a^{-1},-ba^{-1}} \circ T_{a,b} = T_{1,0}.$$

(7) Έστω $G = \mathbb{R} \setminus \{-1\}$ με πράξη $a \star b = a + b + ab$. Θα δείξουμε ότι $(G, \star)$ είναι αβελιανή ομάδα.

Παρατηρούμε ότι αν $a, b \in \mathbb{R} \setminus \{-1\}$ και $a \star b = -1$, τότε

$$a + b + ab = -1 \Rightarrow (a+1)(b+1) = 0 \Rightarrow a = -1 \ \text{ή} \ b = -1.$$

Άρα πράγματι η $\star$ είναι πράξη στο G. Έστω $a, b, c \in G$. Τότε

$$(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + ac + bc + abc$$

και

$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + ab + ac + abc.$$

Άρα $(a \star b) \star c = a \star (b \star c)$.

Για $e = 0$, έχουμε $a \star e = e \star a = a$, για κάθε $a \in G$.

Έστω $a \in G$. Θεωρούμε το $a' = -\frac{a}{1+a}$. Τότε $a' \in \mathbb{R} \setminus \{-1\}$ και $a \star a' = a' \star a = 0$.

Σημειώνουμε ότι το σύνολο $\mathbb{R}$ με πράξη $a \star b = a + b + ab$ δεν είναι ομάδα γιατί το -1 δεν έχει αντίστροφο.

(8) **Ορθογώνιοι πίνακες** Έστω $G = \{A \in M_n(\mathbb{R}) : AA^t = A^tA = I_n\}$. Ως προς το γινόμενο πινάκων η G είναι ομάδα.

Έστω $A, B \in G$. Τότε $AA^t = A^tA = I_n$ και $BB^t = B^tB = I_n$. Άρα

$$(AB)(AB)^t = ABB^tA^t = AI_nA^t = AA^t = I_n.$$

Ομοίως παίρνουμε, $(AB)^t(AB) = I_n$. Άρα $AB \in G$, δηλαδή το γινόμενο πινάκων ορίζει πράξη στο σύνολο G.

Αν $A, B, C \in G$, τότε

$$(AB)C = A(BC) \quad \text{(γενική ιδιότητα γινομένου πινάκων)}.$$

Έχουμε $I_n \in G$ και $I_nA = AI_n = A$.

Έστω $A \in G$. Τότε ο A είναι αντιστρέψιμος και $A^{-1} \in G$. Πράγματι έχουμε $A^{-1} = A^t$ $(AA^t = A^tA = I_n)$ και $(A^{-1})(A^{-1})^t = (A^{-1})A = I_n$. Ομοίως, $(A^{-1})^t(A^{-1}) = I_n$.

(9) **Ομάδα συμμετριών** Έστω $M \subseteq \mathbb{R}^n,\ M \neq \emptyset$. Έστω

$$S(M) = \{f : \mathbb{R}^n \to \mathbb{R}^n : f \ \text{ συμμετρία του M}\}.$$

Ως προς την σύνθεση συναρτήσεων το $S(M)$ είναι ομάδα. Πράγματι εύκολα ελέγχουμε ότι αν $f, g \in S(M)$, τότε $f \circ g \in S(M)$. Επίσης η ταυτοτική απεικόνιση $1 : \mathbb{R}^n \to \mathbb{R}^n$ ανήκει στον $S(M)$ και $f \circ 1 = 1 \circ f = f$, για κάθε $f \in S(M)$. Τέλος εύκολα ελέγχουμε ότι αν $f \in S(M)$, τότε η f είναι 1-1. Αποδεικνύεται ότι η f είναι και επί. Ένας τρόπος να απόδειξης αυτού είναι με χρήση του ότι κάθε ισομετρία $X \to X$ συμπαγούς μετρικού χώρου X είναι επί. Δεδομένου ότι μια ισομετρία είναι 1-1 και επί, έπεται άμεσα ότι η αντίστροφη απεικόνιση είναι επίσης ισομετρία. Άρα η αντίστροφη απεικόνιση μιας συμμετρίας του M είναι συμμετρία του M.

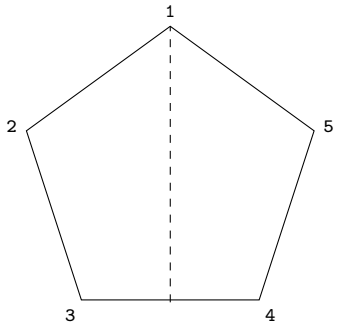
(10) **Διεδρικές ομάδας** D_n Με D_n συμβολίζουμε την ομάδα συμμετριών του κανονικού κυρτού n-γώνου. Θα δείξουμε εδώ ότι

$$|D_n| = 2n$$

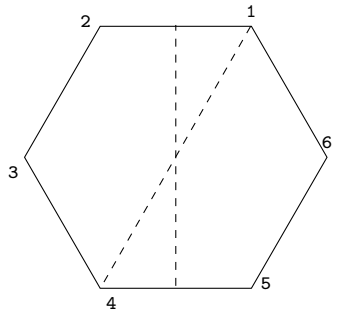
και θα βρούμε χρήσιμες παραστάσεις των στοιχείων της D_n.

Ας συμβολίσουμε με $r_i, i = 0, 1, ..., n-1$ την περιστροφή κατά γωνία $\frac{2\pi}{n}i$ στη θετική φορά, που δεχόμαστε ότι είναι η $\circlearrowleft$. Τότε $r_i \in D_n$ και οι συμμετρίες αυτές είναι διακεκριμένες. Θα θεωρήσουμε τώρα ανακλάσεις και για το σκοπό αυτό θα διακρίνουμε περιπτώσεις.

Αν το n είναι περιττός, θεωρούμε για κάθε κορυφή τον άξονα συμμετρίας που διέρχεται από αυτή. Έχουμε n το πλήθος τέτοιους άξονες και θεωρούμε τις ανακλάσεις $s_j, j = 1, ..., n$ ως προς αυτούς. Είναι σαφές ότι τα s_j είναι διακεκριμένες συμμετρίες (για παράδειγμα έχουν διαφορετικά σταθερά σημεία) και ότι συνολικά τα r_i, s_j για $i = 0, 1, ..., n-1$ και $j = 1, 2, ..., n$ είναι διακεκριμένα. Συνεπώς έχουμε $|D_n| \geq 2n$ όταν n είναι περιττός.



Αν το n είναι άρτιος, τότε κάθε άξονας συμμετρίας που διέρχεται από μια κορυφή, διέρχεται και από την απέναντι κορυφή. Όμως έχουμε και τους άξονες συμμετρίας που είναι οι μεσοκάθετοι απέναντι πλευρών. Τελικά και εδώ έχουμε n άξονες συμμετρίας που ορίζουν n ανακλάσεις οι οποίες με τις n περιστροφές είναι διάφορες ανά δύο. Συνεπώς έχουμε $|D_n| \geq 2n$ όταν n είναι άρτιος.



Μέχρι στιγμής είδαμε ότι $|D_n| \geq 2n$ για κάθε n. Θα δούμε τώρα ότι $|D_n| \leq 2n$ και άρα θα έχουμε ισότητα $|D_n| = 2n$.

Πράγματι, η εικόνα της κορυφής 1 κάτω από οποιαδήποτε συμμετρία του n-γώνου μπορεί να είναι οποιαδήποτε κορυφή i_1, άρα έχουμε το πολύ n επιλογές. Η κορυφή 2 (διαδοχική της 1) μπορεί να έχει εικόνα μια από τις 2 διαδοχικές της i_1 λόγω της διατήρησης αποστάσεων. Άρα για τις $1, 2$ έχουμε το πολύ $2n$ επιλογές. Εύκολα επαληθεύεται ότι οι υπόλοιπες κορυφές της εικόνας είναι μοναδικά ορισμένες λόγω διατήρησης αποστάσεων. (Για παράδειγμα, η κορυφή 3 έχει εικόνα διαδοχική της i_2, αλλά από τις δύο διαδοχικές κορυφές της i_2 η μία, η i_1, είναι ήδη κατειλημμένη).

Διαφορετική περιγραφή των στοιχείων της D_n.
Θα δούμε τώρα μια περιγραφή της D_n που είναι συχνά βολική σε υπολογισμούς. Έστω r

η περιστροφή κατά γωνία $\frac{2\pi}{n}$ και s οποιαδήποτε ανάκλαση ως προς άξονα συμμετρίας του κανονικού κυρτού n-γώνου. Ισχυριζόμαστε ότι

$$D_n = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}.$$

Πράγματι, τα παραπάνω στοιχεία είναι διακεκριμένα γιατί αν $r^i s^j = r^k s^l$, όπου $i, k \in \{0, 1, .., n-1\}$ και $j, l \in \{0, 1\}$, τότε

$$r^{i-k} = s^{l-j}.$$

Το αριστερό μέλος είναι περιστροφή ή η ταυτοτική απεικόνιση, ενώ το δεξί είναι ανάκλαση ή ταυτοτική απεικόνιση. Επειδή κάθε ανάκλαση έχει σταθερά σημεία και κάθε περιστροφή που δεν είναι η ταυτοτική απεικόνιση δεν έχει σταθερά σημεία, συμπεραίνουμε ότι $i - k = l - j = 0$. Έχοντας δείξει ότι τα παραπάνω στοιχεία είναι διακεκριμένα, ο ισχυρισμός έπεται από το γεγονός ότι η D_n έχει $2n$ στοιχεία.

Σημειώνουμε ότι

$$r^n = s^2 = 1 \quad \text{και} \quad sr = r^{-1}s.$$

Οι πρώτες δύο είναι άμεσες από τον ορισμό και η τρίτη αφήνεται ως άσκηση. Οι παραπάνω σχέσεις είναι χρήσιμες σε υπολογισμούς, για παράδειγμα έχουμε

$$srsr^2s = r^{-1}ssr^2s = r^{-1}r^2s = rs.$$

Τέλος, συγκρίνοντας τις δύο περιγραφές που έχουμε για τα στοιχεία της D_n έπεται ότι οι ανακλάσεις της D_n είναι ακριβώς οι

$$s, rs, \ldots r^{n-1}s.$$

(11) **Ευθύ γινόμενο** Έστω $(G_1, *)$, $(G_2, \circledast)$ δύο ομάδες. Στο σύνολο $G_1 \times G_2$ θεωρούμε την πράξη που ορίζεται ως εξής.

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 * g_1 \circledast g_2').$$

Εύκολα επαληθεύεται ότι το $(G_1 \times G_2, \cdot)$ είναι ομάδα. Σημειώνουμε ότι

$$1_{G_1 \times G_2} = (1_{G_1}, 1_{G_2}), \quad (g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$

Η $G_1 \times G_2$ λέγεται το **εξωτερικό ευθύ γινόμενο** (ή το **ευθύ γινόμενο**) των G_1, G_2.

Είδαμε στο Παράδειγμα 7.4(3) ότι αν $X \neq \emptyset$ είναι ένα σύνολο και

$$S(X) = \{f : X \to X : f \ \ 1-1 \ \text{και επί}\},$$

τότε ως προς την σύνθεση συναρτήσεων το $S(X)$ είναι ομάδα. Θα μελετήσουμε τώρα τη $S(X)$ όταν το σύνολο X είναι πεπερασμένο.

7.3. Συμμετρικές ομάδες S_n

Ορισμός 7.5. *Έστω n θετικός ακέραιος. Το σύνολο*

$$S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : f \ \ 1-1 \ \text{και επί}\}$$

εφοδιασμένο με την πράξη της σύνθεσης συναρτήσεων είναι ομάδα που καλείται η ***συμμετρική ομάδα βαθμού*** *n. Κάθε στοιχείο της S_n λέγεται* ***μετάθεση*** *του $\{1, 2, \ldots, n\}$.*

Θα χρησιμοποιούμε συχνά το συμβολισμό

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

για μεταθέσεις. Για παράδειγμα, γράφοντας

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3,$$

εννοούμε ότι σ είναι η απεικόνιση $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ που ορίζεται από

$$\sigma(1) = 3, \ \sigma(2) = 2, \ \sigma(3) = 1.$$

Παρατηρήσεις.

(1) Για $n = 1, 2, 3$ έχουμε

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

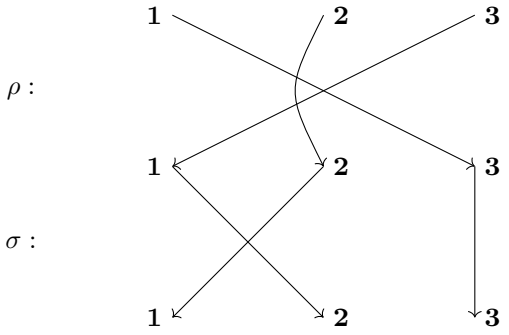
(2) Σύνθεση με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Αν $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ και $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, τότε

$$\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

αφού $1 \xrightarrow{\rho} 3 \xrightarrow{\sigma} 3$, $2 \xrightarrow{\rho} 2 \xrightarrow{\sigma} 1$, $3 \xrightarrow{\rho} 1 \xrightarrow{\sigma} 2$.

Σχηματικά, έχουμε την ακόλουθη κατακόρυφη διάταξη. Για να βρούμε, για παράδειγμα, την εικόνα $\sigma \circ \rho(3)$ της σύνθεσης $\sigma \circ \rho$ στο 3, ακολουθούμε το μονοπάτι που αρχίζει από πάνω με το 3.



(3) Υπολογισμός της σ^{-1} με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Αν $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$, τότε

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

(4) Αν $n \geq 3$, τότε η ομάδα S_n δεν είναι αβελιανή.
Πράγματι, αν
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$ και $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$, τότε

$$\sigma \circ \rho(3) = \sigma(\rho(3)) = \sigma(2) = 1, \text{ και}$$
$$\rho \circ \sigma(3) = \rho(\sigma(3)) = \rho(3) = 2.$$

Άρα $\sigma \circ \rho(3) \neq \rho \circ \sigma(3)$, οπότε $\sigma \circ \rho \neq \rho \circ \sigma$.

Πρόταση 7.6. $|S_n| = n!$.

Απόδειξη. Κάθε μετάθεση του S_n γράφεται μοναδικά στη μορφή

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Για το $\sigma(1)$ υπάρχουν n περιπτώσεις.

Για το $\sigma(2)$ υπάρχουν $n-1$ περιπτώσεις, αφού $\sigma(2) \neq \sigma(1)$ (σ είναι 1-1).

Για το $\sigma(3)$ υπάρχουν $n-2$ περιπτώσεις, αφού $\sigma(3) \neq \sigma(2), \sigma(3) \neq \sigma(1)$.

Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι για το $\sigma(n-1)$ υπάρχουν 2 περιπτώσεις και για το $\sigma(n)$ υπάρχει 1 περίπτωση.
Επομένως $|S_n| = n(n-1)\cdots 2 \cdot 1 = n!$. □

7.4. Κύκλοι

Ορισμός 7.7. *Μια μετάθεση $\sigma \in S_n$ λέγεται* ***κυκλική μετάθεση*** *(ή* ***κύκλος****) αν υπάρχουν $a_1, a_2, \cdots, a_m \in \{1, 2, \cdots, n\}$, ώστε*

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \sigma(a_3) = a_4, \cdots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1, \text{ και}$$

$$\sigma(i) = i \text{ για κάθε } i \in \{1, 2, 3, \cdots, n\} \setminus \{a_1, \cdots, a_m\}.$$

Το m λέγεται το ***μήκος*** *της κυκλικής μετάθεσης. Συμβολίζουμε τον παραπάνω κύκλο με $\sigma = (a_1\ a_2\ \cdots\ a_m)$.*

Παραδείγματα 7.8.

(1) Ο κύκλος $\sigma = (4213) \in S_4$ είναι η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

(2) Ο κύκλος $\sigma = (4213) \in S_5$ είναι η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$.

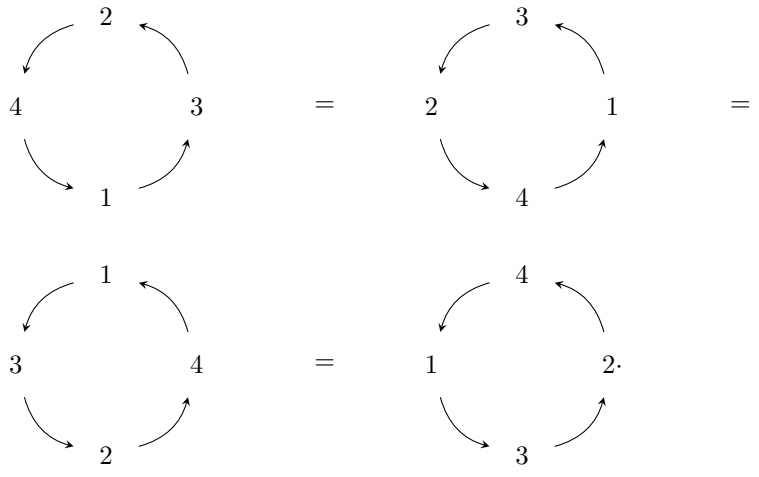
(3) Η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$ δεν είναι κύκλος.

(4) Κάθε κύκλος μήκους 1 είναι η ταυτοτική μετάθεση, $(i) = 1$. Έτσι στο παράδειγμα (2), θα μπορούσαμε να γράψουμε $\sigma = (4213)(5)$ για να το διακρίνουμε από τον κύκλο του παραδείγματος (1).

Παρατήρηση. Τα a_i στην παράσταση $(a_1\ a_2\ \cdots\ a_m)$ ενός κύκλου δεν είναι μοναδικά. Πράγματι, έχουμε

$$(2413) = (3241) = (1324) = (4132).$$

Σχηματικά οι παραπάνω ισότητες φαίνονται στο εξής διάγραμμα.



Γενικά έχουμε

$$(a_1\ a_2\ a_3 \cdots a_m) =$$
$$(a_m\ a_1\ a_2 \cdots a_{m-1}) = (a_{m-1}\ a_m\ a_1 \cdots a_{m-2}) = \cdots = (a_2\ a_3 \cdots a_m\ a_1).$$

Για τη (4213) έχουμε $4 \mapsto 2$, ενώ για τη (2413) έχουμε $4 \mapsto 1$ άρα $(4213) \neq (2134)$.

Παρατήρηση. Αν $\sigma = (a_1\ a_2 \cdots a_{m-1}\ a_m)$, τότε σ^{-1} είναι πάλι κύκλος και μάλιστα $\sigma^{-1} = (a_m\ a_{m-1} \cdots a_2\ a_1)$. Για παράδειγμα, $(4213)^{-1} = (3124)$.

Πρόταση 7.9. *Έστω $\sigma \in S_n$ κύκλος μήκους m. Τότε*
(1) *$\sigma^m = 1$ και*
(2) *$\sigma^k \neq 1$, για κάθε $k = 1, 2, \cdots, m-1$.*

Απόδειξη. Έστω $\sigma = (a_1\ a_2\ a_3 \cdots a_m)$. Τότε $\sigma(a_1) = a_2$, $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$ κλπ. Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι

$$\sigma^{m-1}(a_1) = \sigma(\sigma^{m-2}(a_1)) = \sigma(a_{m-1}) = a_m.$$

Άρα $\sigma,\ \sigma^2, \cdots, \sigma^{m-1} \neq 1$. Επίσης $\sigma^m(a_1) = \sigma(\sigma^{m-1}(a_1)) = \sigma(a_m) = a_1$. Ομοίως

$$\sigma^m(a_i) = a_i, \quad \text{για κάθε} \quad i = 1, 2, \cdots, m.$$

Άρα $\sigma^m = 1$ (θυμίζουμε ότι $\sigma(b) = b$, για κάθε $b \neq a_1, \cdots, a_m$). □

Ορισμός 7.10. *Έστω $\sigma, \tau \in S_n$. Οι σ, τ λέγονται **ξένες**, αν*

$$\{i : \sigma(i) \neq i\} \cap \{j : \tau(j) \neq i\} = \emptyset.$$

Παρατηρούμε ότι αν σ, τ είναι ξένες μεταθέσεις, τότε όποιο στοιχείο μετακινεί η μία, η άλλη το αφήνει σταθερό, δηλαδή

$$\sigma(i) \neq i \Rightarrow \tau(i) = i \quad \text{και} \quad \tau(i) \neq i \Rightarrow \sigma(i) = i.$$

Παραδείγματα 7.11.

(1) Οι μεταθέσεις $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ είναι ξένες, αφού
$$\{i : \sigma(i) \neq i\} = \{1, 3, 5\} \quad \text{και} \quad \{j : \tau(j) \neq i\} = \{2, 4\}.$$
(2) Οι $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}$ δεν είναι ξένες, αφού $\sigma(1) \neq 1$ και $\tau(1) \neq 1$.
(3) Οι κύκλοι $(a_1\ a_2 \cdots a_k)$, $(b_1\ b_2 \cdots b_l)$ είναι ξένοι αν και μόνο αν
$$\{a_1, a_2, \cdots, a_k\} \cap \{b_1, b_2, \cdots, b_l\} = \emptyset.$$

Είδαμε ότι για $n \geq 3$ η ομάδα S_n δεν είναι αβελιανή. Όμως ισχύει η ακόλουθη πρόταση.

Πρόταση 7.12. *Έστω ξένες μεταθέσεις $\sigma, \tau \in S_n$. Τότε $\sigma\tau = \tau\sigma$.*

Απόδειξη. Έστω $i \in \{1, 2, \cdots, n\}$. Διακρίνουμε τις δύο ακόλουθες περιπτώσεις.

(1) Έστω $\tau(i) = i$. Τότε $\sigma\tau(i) = \sigma(i)$. Έστω
$$\tau(\sigma(i)) \neq \sigma(i).$$
Επειδή σ, τ ξένες και $\tau(\sigma(i)) \neq \sigma(i)$, έπεται $\sigma(\sigma(i)) = \sigma(i)$. Επειδή όμως η σ είναι 1-1, έπεται $\sigma(i) = i$. Επομένως $\tau(\sigma(i)) = \tau(i) = i = \sigma(i)$, άτοπο. Άρα $\tau\sigma(i) = \sigma(i)$, δηλαδή δείξαμε ότι αν $\tau(i) = i$, τότε $\sigma\tau(i) = \tau\sigma(i)$.
(2) Έστω $\tau(i) \neq i$. Επειδή οι τ, σ είναι ξένες μεταθέσεις, έχουμε $\sigma(i) = i$. Από αυτό που δείξαμε στην περίπτωση 1 (εναλλάσσοντας τους ρόλους των τ, σ), προκύπτει ότι $\sigma\tau(i) = \tau\sigma(i)$.

□

Μια άμεση συνέπεια της προηγούμενης πρότασης είναι ότι αν οι μεταθέσεις σ, τ είναι ξένες, τότε για κάθε θετικό ακέραιο k έχουμε $(\sigma\tau)^k = \sigma^k\tau^k$.

Θεώρημα 7.13. *Κάθε $\sigma \in S_n$, $\sigma \neq 1$, γράφεται ως γινόμενο ξένων ανά δύο κύκλων, $\sigma = \sigma_1\sigma_2 \dots \sigma_m$, όπου οι σ_i έχουν μήκος τουλάχιστον 2 και είναι μοναδικοί (χωρίς να λαμβάνεται υπόψη η σειρά τους).*

Απόδειξη. *Ύπαρξη.* Έστω $a_1 \in \{1, 2, \dots, n\}$ και

$$\mathcal{O}_{a_1} = \{\sigma^t(a_1) : t \in \mathbb{N}\} \ \ (\text{για } \ t = 0 \ \ \sigma^0 = 1).$$

Επειδή $\mathcal{O}_{a_1} \subseteq \{1, 2, \cdots, n\}$ που είναι πεπερασμένο σύνολο, υπάρχουν s, t με $0 \leq s < t$ ώστε $\sigma^s(a_1) = \sigma^t(a_1)$. Επιλέγουμε ελάχιστο τέτοιο $t_1 > 0$. Ισχυριζόμαστε ότι $\sigma^t(a_1) = a_1$. Πράγματι, αν $\sigma^s(a_1) = \sigma^t(a_1)$ με $0 < s < t$, τότε $\sigma^{s-1}(a_1) = \sigma^{t-1}(a_1)$, άτοπο από τον ορισμό του t_1. Άρα

$$\mathcal{O}_{a_1} = \{a_1, \sigma(a_1), \sigma^2(a_1), \dots, \sigma^{t_1-1}(a_1)\}.$$

Έστω $a_2 \in \{1, 2, \dots, n\} \setminus \mathcal{O}_{a_1}$ και $\mathcal{O}_{a_2} = \{\sigma^t(a_2) : t \in \mathbb{N}\}$. Όπως πριν προκύπτει ότι

$$\mathcal{O}_{a_2} = \{a_2, \sigma(a_2), \sigma^2(a_2), \dots, \sigma^{t_2-1}(a_2)\}.$$

Στη συνέχεια επιλέγουμε $a_3 \in \{1, 2, \dots, n\} \setminus (\mathcal{O}_{a_1} \cup \mathcal{O}_{a_2})$ κοκ. Με τον τρόπο αυτό προκύπτουν $\mathcal{O}_{a_1}, \dots, \mathcal{O}_{a_m} \subseteq \{1, 2, \cdots, n\}$ ώστε

(1) $\mathcal{O}_{a_i} \cap \mathcal{O}_{a_j} = \emptyset$, για κάθε $i \neq j$ και

(2) $\mathcal{O}_{a_1} \cup \mathcal{O}_{a_2} \cup \cdots \cup \mathcal{O}_{a_m} = \{1, 2, \dots, n\}$

Το (2) είναι άμεσο. Για το (1), αν $\sigma^t(a_i) = \sigma^s(a_j)$, αφού $t \leq s$, έχουμε $a_i = \sigma^{s-t}(a_j) \in \mathcal{O}_{a_j}$, άτοπο.

Θέτουμε

$$\sigma_i = (a_i \ \sigma(a_i) \ \sigma^2(a_i) \dots \sigma^{t_i-1}(a_i)) \in S_n$$

που είναι κύκλος (αφού $\sigma^{t_i}(a_i) = a_i$). Οι κύκλοι $\sigma_1, \dots, \sigma_m$ είναι ξένοι λόγω του (1). Από τον ορισμό και από το (2), έπεται ότι $\sigma = \sigma_1\sigma_2 \dots \sigma_m$.

Μοναδικότητα. Έστω

$$\sigma_1\sigma_2 \dots \sigma_m = \tau_1\tau_2 \dots \tau_{m'},$$

όπου $\sigma_1, \cdots, \sigma_m$ ξένοι ανά δύο κύκλοι μήκους ≥ 2 και όμοια $\tau_1, \cdots, \tau_{m'}$ ξένοι ανά δύο κύκλοι μήκους ≥ 2. Θα δείξουμε ότι $m = m'$ και μετά από ενδεχόμενη αναδιάταξη $\sigma_i = \tau_i$, για κάθε i.

Χρησιμοποιούμε επαγωγή στο $M = \max\{m, m'\}$. Αν $M = 1$, το ζητούμενο προφανώς ισχύει. Έστω $M \geq 2$ και $\sigma_1\sigma_2 \cdots \sigma_m = \tau_1\tau_2 \cdots \tau_{m'}$. Επειδή το μήκος του σ_1 είναι διάφορο του 1, υπάρχει $i \in \{1, 2, \cdots, n\}$ ώστε $\sigma_1(i) \neq i$. Επειδή $\sigma_1, \sigma_2, \dots, \sigma_m$ είναι ανά δύο ξένοι, έχουμε $\sigma_j(i) = i$, για κάθε $j \neq 1$. Επομένως

$$\sigma(i) = \sigma_1\sigma_2 \cdots \sigma_m(i) = \sigma_1(i) \neq i.$$

Άρα $\tau_1\tau_2 \cdots \tau_{m'}(i) \neq i$, οπότε υπάρχει q ώστε $\tau_q(i) \neq i$. Καθώς ξένοι κύκλοι αντιμετατίθενται, με μια αναδιάταξη μπορούμε να υποθέσουμε ότι $q = 1$.

Ισχυριζόμαστε ότι $\sigma_1 = \tau_1$. Πράγματι, είδαμε πριν ότι αν το i μετακινείται από τη σ_1, τότε $\sigma(i) = \sigma_1(i)$. Το αποτέλεσμα αυτό για $\sigma_1(i)$ στη θέση του i δίνει $\sigma(\sigma_1(i)) = \sigma_1^2(i)$ οπότε $\sigma^2(i)) = \sigma_1^2(i)$. Επαγωγικά προκύπτει ότι για κάθε θετικό ακέραιο k, $\sigma^k(i) = \sigma_1^k(i)$. Όμοια έχουμε $\sigma^k(i) = \tau_1^k(i)$. Άρα

$$\sigma_1^k(i) = \tau_1^k(i).$$

Επειδή οι σ_1, τ_1 είναι κύκλοι και το i μετακινείται από αυτούς, παίρνουμε $\sigma_1 = \tau_1$.

Έχοντας τώρα ότι $\sigma_1 = \tau_1$, πολλαπλασιάζουμε τη σχέση $\sigma_1\sigma_2\dots\sigma_m = \tau_1\tau_2\dots\tau_{m'}$ από αριστερά με $\sigma_1^{-1} = \tau_1^{-1}$ και παίρνουμε

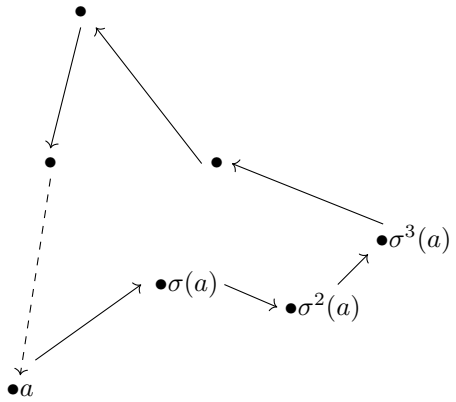
$$\sigma_2\dots\sigma_m = \tau_2\dots\tau_{m'}.$$

Από την επαγωγική υπόθεση έχουμε το ζητούμενο. □

Το σύνολο

$$\mathcal{O}_a = \{\sigma^t(a) : t \in \mathbb{N}\}$$

στην απόδειξη λέγεται η **τροχιά** του a κάτω από τις δυνάμεις του σ. Η κεντρική ιδέα της ύπαρξης στην προηγούμενη απόδειξη, δηλαδή ότι τα στοιχεία του $\mathcal{O}_a$ ορίζουν κατά φυσικό τρόπο κύκλο, συνοψίζεται στο ακόλουθο σχήμα.



Παραδείγματα 7.14.

(1) Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 9 & 8 & 6 & 7 & 1 \end{pmatrix} \in S_9$. Θα εφαρμόσουμε τον αλγόριθμο που είδαμε στην παραπάνω απόδειξη διατηρώντας το συμβολισμό της.
Επιλέγοντας $a_1 = 1 \in \{1, 2, ..., 9\}$, έχουμε

$$\sigma(1) = 3,\ \sigma(3) = 5,\ \sigma(5) = 9,\ \sigma(9) = 1.$$

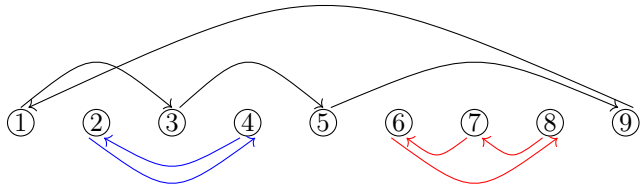
Άρα $\mathcal{O}_{a_1} = \{1, 3, 5, 9\}, \sigma_1 = (1\ 3\ 5\ 9)$.
Επιλέγοντας $a_2 = 2 \in \{1, 2, ..., 9\} - \{1, 3, 5, 9\}$, έχουμε

$$\sigma(2) = 4,\ \sigma(4) = 2.$$

Άρα $\mathcal{O}_{a_2} = \{2, 4\}, \sigma_2 = (2\ 4)$.
Επιλέγοντας $a_3 = 6 \in \{1, 2, ..., 9\} - \{1, 3, 5, 9, 2, 4\}$, έχουμε

$$\sigma(6) = 8,\ \sigma(8) = 7,\ \sigma(7) = 6.$$

Άρα $\mathcal{O}_{a_3} = \{6, 8, 7\}, \sigma_3 = (687)$.
Επομένως τελικά, $\sigma = \sigma_1\sigma_2\sigma_3 = (1359)(24)(687)$. Εποπτικά, οι τρεις τροχιές και οι αντίστοιχοι κύκλοι φαίνονται στο ακόλουθο γράφημα.



Αν $\sigma(i) = j$, τότε υπάρχει προσανατολισμένη ακμή με αρχή την κορυφή i και τέλος την κορυφή j.

(2) Να βρεθεί η ανάλυση της σ^{2020} σε γινόμενο κύκλων ξένων ανά δύο, $\sigma = (1234)(34567) \in S_7$.

Σημειώνουμε ότι οι κύκλοι $(1234), (34567)$ δεν είναι ξένοι. Υπολογίζοντας έχουμε

$$\sigma(1) = 2,\ \sigma(2) = 3,\ \sigma(3) = 1,$$
$$\sigma(4) = 5,\ \sigma(5) = 6,\ \sigma(6) = 7,\ \sigma(7) = 4.$$

Άρα $\sigma = (123)(4567)$, που είναι γινόμενο ξένων κύκλων. Σύμφωνα με την Πρόταση 7.9 είναι $(123)^3 = (4567)^4 = 1$. Άρα $(123)^{12} = (4567)^{12} = 1$. Επειδή ξένες μεταθέσεις αντιμετατίθενται, ισχύει ότι $\sigma^m = (123)^m(4567)^m$ για κάθε ακέραιο m, ειδικά $\sigma^{12} = (123)^{12}(4567)^{12} = 1$. Επειδή $2020 = 12 \cdot 168 + 4$, έχουμε

$$\sigma^{2020} = (\sigma^{12})^{168}\sigma^4 = \sigma^4 = (123)^4(4567)^4 = (123)^4 = (123).$$

7.5. Τάξη στοιχείου ομάδας

Έστω G ομάδα και $a, b \in G$. Συνήθως θα γράφουμε ab για την εικόνα του διατεταγμένου ζεύγους $(a, b) \in G \times G$ κάτω από την πράξη της G και επίσης θα συμβολίζουμε με 1_G ή απλά 1 το ουδέτερο στοιχείο της G.

Αν $a \in G$, ορίζουμε επαγωγικά

$$a^0 = 1 \text{ και } a^{m+1} = aa^m,$$

όπου $m \in \mathbb{N}$. Επίσης ορίζουμε

$$a^{-m} = (a^{-1})^m,$$

όπου $m \in \mathbb{N}$. Αφήνουμε την επαλήθευση των εξής ισοτήτων ως άσκηση (η τυχερή σας μέρα).

Έστω $a, b \in G$, όπου G ομάδα. Για κάθε $m, n \in \mathbb{Z}$,

- $a^m a^n = a^{m+n} = a^n a^m$,
- $(a^m)^n = a^{mn} = (a^n)^m$,
- αν $ab = ba$, τότε $(ab)^m = a^m b^m$.

Προσοχή. Τα παραπάνω έχουν γραφεί έχοντας υπόψη *πολλαπλασιαστικό* συμβολισμό, ab, για την πράξη της G. Αν είχαμε προσθετικό συμβολισμό, $a + b$, τότε στη θέση του a^m θα γράφαμε ma και οι προηγούμενες ισότητες θα γράφονταν ως εξής (βλ. Παράγραφο 3.3 στους δακτυλίους).

- $ma + na = (m + n)a = na + ma$,
- $n(ma) = (mn)a = m(na)$,
- αν $a + b = b + a$, τότε $m(a + b) = ma + mb$.

Ορισμός 7.15. *Έστω G ομάδα και $g \in G$. Αν υπάρχει $m \in \mathbb{Z}_{>0}$ με $g^m = 1$, τότε ο ελάχιστος τέτοιος m λέγεται η **τάξη** του g και συμβολίζεται με $|g|$ ή $o(g)$. Αν δεν υπάρχει τέτοιος m, θα λέμε ότι η τάξη του g είναι **άπειρη**.*

Παραδείγματα 7.16.

(1) Έστω $\sigma \in S_n$ κύκλος μήκους k. Τότε $\sigma^k = 1$ και $\sigma^j \neq 1$, για κάθε $j = 1, 2, \ldots, k-1$, σύμφωνα με την Πρόταση 7.9 Δηλαδή $|\sigma| = k$.

(2) Έστω $G = \mathbb{R} \setminus \{0\}$ με πράξη τον πολλαπλασιασμό. Το στοιχείο 2 έχει άπειρη τάξη αφού $2^m \neq 1$ για κάθε θετικό ακέραιο m. Το στοιχείο -1 έχει τάξη 2 αφού $-1 \neq 1$ και $(-1)^2 = 1$.

(3) Έστω $G = GL_2(\mathbb{R})$ και $A, B, C, D \in G$, όπου

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Επειδή $A^2 = I_2$ και $A \neq I_2$, η τάξη του A είναι 2. Όμοια, η τάξη του B είναι 2. Με επαγωγή στο m εύκολα αποδεικνύεται ότι για κάθε θετικό ακέραιο m, $C^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. Άρα $C^m \neq I_2$ για κάθε $m > 0$. Αυτό σημαίνει ότι το στοιχείο C έχει άπειρη τάξη. Για το D παρατηρούμε ότι

$$D^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq I_2,\ D^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq I_2,\ D^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Άρα η τάξη του D είναι 4.

(4) Θεωρούμε την ομάδα $\mathbb{Z}_8$. Εδώ έχουμε προσθετικό συμβολισμό για την πράξη και το ουδέτερο στοιχείο είναι το $[0]$. Για να βρούμε την τάξη του $g = [6]$ υπολογίζουμε

$$2g = [12] = [4] \neq [0],\ 3g = [18] = [2] \neq [0],\ 4g = [24] = [0].$$

Άρα η τάξη του $g = [6]$ είναι 4.

(5) Θεωρούμε το σύνολο $U(\mathbb{Z}_8)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_8$. Ξέρουμε ότι είναι ομάδα με πράξη τον πολλαπλασιασμό του $\mathbb{Z}_8$. Επίσης ξέρουμε ότι $U(\mathbb{Z}_8) = \{[1], [3], [5], [7]\} = \{[a] \in \mathbb{Z}_8 : \mu\kappa\delta(a, 8) = 1\}$. Παρατηρούμε ότι

g	$[1]$	$[3]$	$[5]$	$[7]$
$\lvert g\rvert$	1	2	2	2

για παράδειγμα $3^2 \equiv 9 \equiv 1 \mathrm{mod} 8$, δηλαδή $[3]^2 = [1]$ ($[3] \neq [1]$).

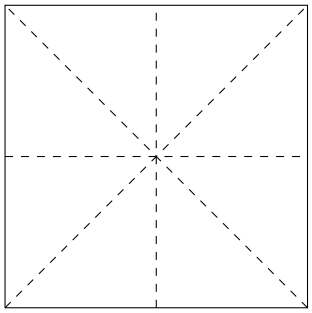
(6) Σύμφωνα με το πρώτο παράδειγμα, οι τάξεις των στοιχείων της ομάδας S_3 είναι

$g \in S_3$	1	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(2\ 1\ 3)$
$\lvert g\rvert$	1	2	2	2	3	3

(7) Θυμίζουμε ότι η διεδρική ομάδα D_4, δηλαδή η ομάδα των συμμετριών του τετραγώνου, έχει 8 στοιχεία

$$D_4 = \{1, r_1, r_2, r_3, s_1, s_2, s_3, s_4\},$$

όπου r_i είναι η περιστροφή κατά γωνία $\frac{\pi}{2} i$ και s_j είναι οι ανακλάσεις ως προς τους 4 άξονες συμμετρίας.



Είναι σαφές ότι $r_1^2 = r_2, r_1^3 = r_3$ και $r_1^4 = 1$. Άρα η τάξη του r_1 είναι ίση με 4. Με όμοιο τρόπο έχουμε ότι $|r_2| = 2$ και $|r_3| = 4$. Για τις ανακλάσεις είναι σαφές ότι $|s_j| = 2$ για κάθε j.

(8) Σημειώνουμε ότι αν G είναι πεπερασμένη ομάδα, τότε κάθε $g \in G$ έχει πεπερασμένη τάξη. Πράγματι, θεωρώντας την ακολουθία στοιχείων της G,

$$1, g, g^2, g^3, ...$$

είναι σαφές ότι υπάρχουν φυσικοί αριθμοί $m > n$ με $g^m = g^n$. Άρα $g^{m-n} = 1$.

(9) Έστω R δακτύλιος με μονάδα 1_R ο οποίος έχει θετική χαρακτηριστική n, βλ. Παράγραφο 6.6. Η τάξη του 1_R στην προσθετική ομάδα $(R, +)$ είναι ίση με n.

Θεώρημα 7.17. *Έστω G ομάδα και $g \in G$. Έστω ότι $|g| = k < \infty$. Τότε ισχύουν τα ακόλουθα.*
(1) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $g^m = 1 \Leftrightarrow k|m$.*
(2) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $|g^m| = \frac{k}{\mu\kappa\delta(k,m)}$.*

Απόδειξη. (1) Από την Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ ώστε $m = qk + r,\ 0 \leq r < k$. Τότε

$$g^m = (g^k)^q g^r = 1^q g^r = g^r.$$

Αν $g^m = 1$, τότε $g^r = 1$ και επειδή $0 \leq r < k$, όπου $k = |g|$ παίρνουμε $r = 0$. Αν $k|m$, τότε $r = 0$ και $g^m = 1$.

(2) Παρατηρούμε ότι $(g^m)^{\frac{k}{\mu\kappa\delta(k,m)}} = (g^k)^{\frac{m}{\mu\kappa\delta(k,m)}} = 1$. Άρα

$$|g^m| \leq \frac{k}{\mu\kappa\delta(k,m)}.$$

Έστω $(g^m)^s = 1,\ s \in \mathbb{Z}_{>0}$. Τότε $g^{ms} = 1$, οπότε από το (1) του θεωρήματος έπεται ότι $k|ms$. Τότε

$$\frac{k}{\mu\kappa\delta(k,m)} \Big| \frac{m}{\mu\kappa\delta(k,m)} s.$$

Όμως $\mu\kappa\delta\left(\frac{k}{\mu\kappa\delta(k,m)}, \frac{m}{\mu\kappa\delta(k,m)}\right) = 1$, άρα $\frac{k}{\mu\kappa\delta(k,m)} \Big| s \Rightarrow \frac{k}{\mu\kappa\delta(k,m)} \leq s$. Συνεπώς $|g^m| = \frac{k}{\mu\kappa\delta(k,m)}$. □

Για παράδειγμα, αν $\sigma \in S_n$ είναι κύκλος μήκους 8, τότε $\left|\sigma^{50}\right| = \frac{8}{\mu\kappa\delta(50,8)} = \frac{8}{2} = 4$.

Σχόλιο. Είδαμε πριν ότι αν g είναι στοιχείο ομάδας, τότε η τάξη του g^m καθορίζεται από την τάξη του g και το m. Για το γινόμενο ab δυο στοιχείων μια ομάδας δεν αληθεύει ότι η τάξη του ab καθορίζεται από τις τάξεις των a, b. Για παράδειγμα, στην ομάδα S_4 καθένα από τα στοιχεία $(12), (23), (34)$ έχει τάξη 2, το γινόμενο $(12)(23) = (132)$ έχει τάξη 3 ενώ το γινόμενο $(12)(34)$ έχει τάξη 2. Επίσης, είναι δυνατό δύο στοιχεία πεπερασμένης τάξης να έχουν γινόμενο άπειρης τάξης. Με το συμβολισμό του Παραδείγματος 7.16(3), έχουμε $AB = C$, οι τάξεις των A και B είναι 2, αλλά το C έχει άπειρη τάξη.

Συνεπώς τίθεται το ερώτημα: Ποια είναι γενικά η σχέση των τάξεων των a, b, ab; Απάντηση: Απολύτως καμία. Συγκεκριμένα αναφέρουμε χωρίς απόδειξη το εξής αποτέλεσμα. Για κάθε $l, m, n \in \mathbb{Z}_{>0}$, υπάρχουν ομάδα G και στοιχεία a, b αυτής τέτοια ώστε $|a| = l, |b| = m, |ab| = n$. Όμως για ξένες μεταθέσεις η εικόνα είναι ευχάριστη σύμφωνα με το ακόλουθο αποτέλεσμα.

Θεώρημα 7.18. *Έστω $\sigma, \tau \in S_n$ ξένες μεταθέσεις με $|\sigma| = l$ και $|\tau| = m$. Τότε $|\sigma\tau| = \epsilon\kappa\pi(l, m)$.*

Απόδειξη. Έστω $k = \epsilon\kappa\pi(l, m)$. Επειδή ξένες μεταθέσεις αντιμετατίθενται, έχουμε

$$(\sigma\tau)^k = \sigma^k \tau^k = 1 \cdot 1 = 1$$

(αφού k πολλαπλάσιο του l και k πολλαπλάσιο του m.) Άρα $|\sigma\tau| \leq k$.

Έστω $(\sigma\tau)^s = 1$. Τότε $\sigma^s\tau^s = 1 \Rightarrow \sigma^s = \tau^{-s} = (\tau^{-1})^s$. Επειδή οι μεταθέσεις σ, τ είναι ξένες, και οι σ και τ^{-1} είναι ξένες, αφού τα σταθερά σημεία της τ ταυτίζονται με τα σταθερά σημεία της τ^{-1}. Άρα οι μεταθέσεις σ^s και $(\tau^{-1})^s$ είναι ξένες. Επειδή είναι ίσες, συμπεραίνουμε ότι $\sigma^s = (\tau^{-1})^s = 1$. Τότε $l|s$ και $m|s$. Επομένως $\epsilon\kappa\pi(l, m) \leq s$. Άρα $|\sigma\tau| = \epsilon\kappa\pi(l, m)$. □

Πόρισμα 7.19. *Αν $\sigma \in S_n$, $\sigma = \sigma_1\sigma_2\cdots\sigma_m$, όπου σ_i ξένοι ανά δύο κύκλοι με μήκη $k_1, k_2, \cdots, k_m$, τότε $|\sigma| = \epsilon\kappa\pi(k_1, k_2, \cdots, k_m)$.*

Απόδειξη. Επαγωγή στο m (άσκηση). □

Παραδείγματα 7.20.

(1) Βρείτε όλους τους $n \in \mathbb{Z}_{>0}$ ώστε $9^n \equiv 1 \mod 14$.
Παρατηρούμε ότι $[9] \in U(\mathbb{Z}_{14})$ αφού $\mu\kappa\delta(9,14) = 1$. Υπολογίζουμε την τάξη του $[9] \in U(\mathbb{Z}_{14})$.

$$\begin{aligned} [9]^2 &= [81] = [11] \neq [1] \\ [9]^3 &= [99] = [1]. \end{aligned}$$

Άρα $\big|[9]\big| = 3$. Από το Θεώρημα 7.17(1) παίρνουμε $9^n \equiv 1 \mod 14 \Leftrightarrow n = 3m, m \in \mathbb{Z}_{>0}$.

(2) Βρείτε την τάξη του $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 9 & 7 & 6 & 8 & 2 & 4 \end{pmatrix} \in S_9$ και του σ^{50}.
Βρίσκουμε πρώτα την ανάλυση του σ σε γινόμενο ξένων κύκλων. Παρατηρούμε ότι

$$\sigma(1) = 3,\ \sigma(3) = 1,$$
$$\sigma(2) = 5,\ \sigma(5) = 7,\ \sigma(7) = 8,\ \sigma(8) = 2,$$
$$\sigma(4) = 9,\ \sigma(9) = 4$$

και $\sigma(6) = 6$. Επομένως $\sigma = (13)(2578)(49)$. Από το Πόρισμα 7.19, έχουμε $|\sigma| = \text{εκπ}(2,4,2) = 4$. Από το Θεώρημα 7.17 έχουμε $\big|\sigma^{50}\big| = \frac{4}{\mu\kappa\delta(50,4)} = 2$.

(3) Να βρεθούν όλοι οι θετικοί ακέραιοι m έτσι ώστε σ^m είναι κύκλος μήκους 4, όπου $\sigma = (1234)(34567) \in S_7$.
Βρίσκουμε κατά τα γνωστά την ανάλυση της σ σε γινόμενο ξένων κύκλων

$$\sigma = (123)(4567).$$

Επειδή ξένες μεταθέσεις αντιμετατίθενται, έχουμε για κάθε θετικό ακέραιο m ότι

$$\sigma^m = (123)^m(4567)^m.$$

Οι μεταθέσεις $(123)^m, (4567)^m$ είναι ξένες. Από τη μοναδικότητα της ανάλυσης μετάθεσης σε γινόμενο ξένων κύκλων, έπεται ότι αναγκαία συνθήκη ώστε η $(123)^m(4567)^m$ να είναι κύκλος, είναι

$$(123)^m = 1 \ \text{ή}\ (4567)^m = 1.$$

Στη δεύτερη περίπτωση θα είχαμε $\sigma^m = (123)^m$ που δεν είναι κύκλος μήκους 4. Άρα λαμβάνουμε την αναγκαία συνθήκη $(123)^m = 1$ που με βάση το Θεώρημα 7.17 ισοδυναμεί με $3|m$. Έστω ότι $3|m$. Τότε $\sigma^m = (4567)^m$. Έστω $m = 4q + r$, όπου $q, r \in \mathbb{N}$ και $r < 4$. Τότε

$$\sigma^m = (4567)^r.$$

Με άμεσο υπολογισμός έχουμε $(4567)^2 = (46)(57)$ και $(4567)^3 = (4765)$. Επομένως βρήκαμε ότι αν σ^m είναι κύκλος μήκους 4, τότε

$$m \equiv 0 \mod 3 \ \text{και}\ m \equiv 1, 3 \mod 4,$$

ισοδύναμα $m \equiv 3, 9 \mod 12$.

Αντίστροφα, αν $m \equiv 3, 9 \mod 12$, δηλαδή $m = 12q + r$, όπου $r = 3, 9$, τότε με άμεσο υπολογισμό έχουμε ότι $\sigma^m = (123)^r(4567)^r = (4765), (4567)$.

Σημείωση. Επειδή τα μήκη των κύκλων (123) και (4567) είναι 3, 4 αντίστοιχα και εκπ(3,4)=12, θα μπορούσαμε εξαρχής να δουλέψουμε $\mod 12$: Δηλαδή γράφοντας $m = 12q + r, 0 \leq r \leq 11$, θα είχαμε $\sigma^m = (123)^r(4567)^r$ και θα εξετάζαμε τις περιπτώσεις $r = 0, ..., 11$.

Ασκήσεις Κεφαλαίου 7

Ομάδα1: 1-5, 21, 23, 27.
Ομάδα2: 6-10, 12, 14-19, 20, 24.
Ομάδα3: 11, 13, 22, 25, 26.

1. Αποδείξτε το Πόρισμα 1.17
2. Δείξτε ότι η ομάδα G των συμμετριών του κύκλου περιέχει
   i) στοιχείο άπειρης τάξης, και
   ii) στοιχείο τάξης m για κάθε θετικό ακέραιο m.
3. Έστω n θετικός ακέραιος. Δείξτε ότι για κάθε θετικό διαιρέτη d του n, η διεδρική ομάδα D_n περιέχει στοιχείο τάξης d.
4. Έστω $\sigma = \sigma_1\, \sigma_2 \cdots \sigma_m \in S_n$, όπου σ_i ξένοι ανά δύο κύκλοι. Τότε $\sigma = \sigma^{-1}$ αν και μόνο αν κάθε σ_i έχει μήκος ≤ 2.
5. $\star$ Έστω G ομάδα και $a, b \in G$. Τότε
   i) $|a| = |a^{-1}|$.
   ii) $|b^{-1}ab| = |a|$.
   iii) $|ab| = |ba|$.
   iv) Αν $b^{-1}a^2b = a^3$ και $a \neq 1$, τότε $|a| \geq 5$.
6. Έστω G ομάδα τέτοια ώστε υπάρχει μοναδικό στοιχείο $a \in G$ με $|a| = 2$. Τότε $ab = ba$, για κάθε $b \in G$.
7. Έστω G ομάδα και $a, b, c \in G$ με $abc = 1$. Αληθεύει ότι $bca = 1$; Αληθεύει ότι $bac = 1$;
8. Δείξτε ότι αν μια ομάδα περιέχει στοιχείο πεπερασμένης τάξης n, τότε περιέχει τουλάχιστον $\varphi(n)$ στοιχεία τάξης n, όπου φ η συνάρτηση του Euler.
9. Πόσα στοιχεία τάξης 2 έχει η διεδρική ομάδα D_n;
10. Πόσα στοιχεία τάξης
    i) 2 έχει η S_4;
    ii) 3 έχει η S_5;
    iii) 3 έχει η S_9;
11. Αν $\sigma \in S_{10}$ έχει τάξη 14, δείξτε ότι υπάρχει μοναδικό $i \in \{1, 2, \cdots, 10\}$ με $\sigma(i) = i$.
12. Έστω G ομάδα τέτοια ώστε κάθε $g \in G \setminus \{1\}$ έχει τάξη 2. Τότε η G είναι αβελιανή.
13. Έστω G πεπερασμένη ομάδα και $A \subseteq G$ με $|A| > \frac{|G|}{2}$. Τότε για κάθε $g \in G$, υπάρχουν $a, a' \in A$ ώστε $g = aa'$.
14. Ποιες από τις ακόλουθες προτάσεις αληθεύουν; Δώστε απόδειξη ή αντιπαράδειγμα σε κάθε περίπτωση.
    i) Υπάρχει ομάδα με μοναδικό στοιχείο τάξης 3.
    ii) Αν G ομάδα, $a, b \in G$ και $a^3 = b^3$, τότε $a = b$.
    iii) Αν G ομάδα, $a, b \in G$ με $a^3 = b^3$ και $a^5 = b^5$, τότε $a = b$.
    iv) Το μέγιστο στοιχείο του $\{|\sigma| : \sigma \in S_6\}$ είναι το 6.
15. Έστω m θετικός ακέραιος και $\sigma \in S_n$ κύκλος μήκους k και $d = \mu\kappa\delta(m, k)$. Δείξτε ότι η μετάθεση σ^m είναι γινόμενο d το πλήθος κύκλων ξένων ανά δύο που ο καθένας έχει μήκος k/d.
16. Έστω $\tau = (123...n) \in S_n$ και $\sigma \in S_n$. Δείξτε ότι $\tau\sigma = \sigma\tau \Leftrightarrow \sigma = \tau^m,\ m \in \mathbb{N}$.
17. Έστω $\sigma = (1234)(3456) \in S_6$. Βρείτε την τάξη της σ^{100}. Στη συνέχεια εξετάστε αν υπάρχει $\tau \in S_6$ με $\tau^3 = \sigma$.
18. Βρείτε (αν υπάρχουν) όλα τα $\sigma \in S_5$ με $\sigma^2 = (12345)$.

19. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 1 & 7 & 2 & 6 \end{pmatrix} \in S_7$. Για ποιος ακέραιους m η μετάθεση σ^m είναι κύκλος;

20. Έστω $[a] \in \mathbb{Z}_n$. Θεωρούμε την απεικόνιση $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n,\ n \geq 1$, με $\sigma([b]) = [ab]$.
    i) Δείξτε ότι η σ είναι μετάθεση αν και μόνο αν $\mu\kappa\delta(a, n) = 1$,
    ii) Για $n = 9$ και $a = 4$ βρείτε την ανάλυση της σ^{2020} σε γινόμενο ξένων ανά δύο κύκλων.

21. Έστω G, H ομάδες και $g \in G, h \in H$. Δείξτε ότι το $(g, h) \in G \times H$ έχει πεπερασμένη τάξη αν και μόνο τάξεις των g, h είναι πεπερασμένες. Στην περίπτωση αυτή, δείξτε ότι η τάξη του (g, h) ισούται με το εκπ$(|g|, |h|)$.

22. Έστω g στοιχείο ομάδας G με $|g| = mn$ όπου οι m, n είναι σχετικά πρώτοι. Δείξτε ότι υπάρχουν $x, y \in G$ με $g = xy = yx$ και $x^m = y^n = 1$. Στη συνέχεια δείξτε ότι τα x, y είναι μοναδικά.

23. Βρείτε τους θετικούς ακέραιους n έτσι ώστε $5^n \equiv 1 \mod 21$.

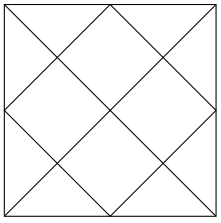
24. Πόσα στοιχεία σ της ομάδας S_p, όπου p πρώτος, ικανοποιούν $\sigma^p = 1$;

25. ≀ Έστω G ομάδα στην οποία ισχύει ότι $(ab)^i = a^i b^i$ για τρεις διαδοχικούς ακέραιους i. Δείξτε ότι η G είναι αβελιανή.

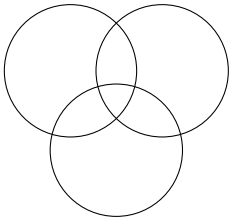
26. ≀ Να βρεθεί η μέγιστη πεπερασμένη τάξη στοιχείου της ομάδας $\{M \in M_2(\mathbb{Z}) : detA = 1\}$

27. Ποιες είναι οι ομάδες συμμετριών των επόμενων σχημάτων;

i)

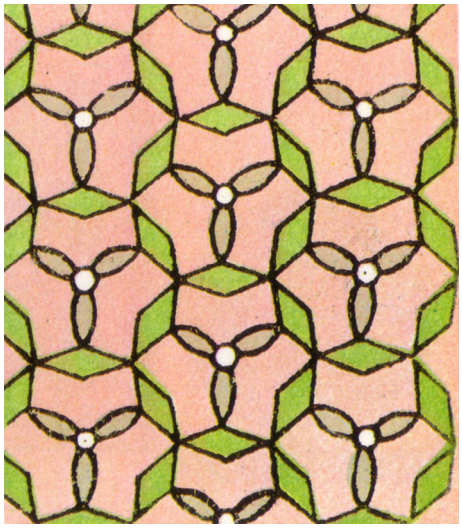


ii)

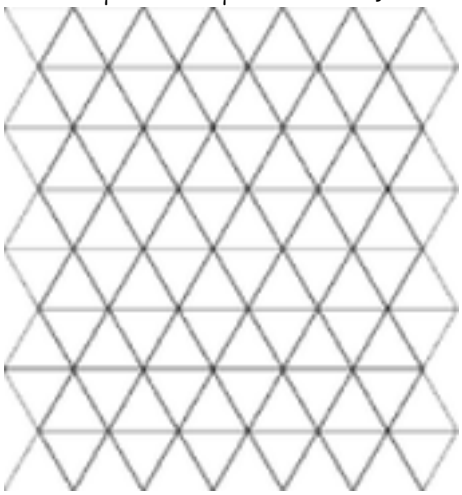


28. **Επίπεδες κρυσταλλογραφικές ομάδες** Θα δούμε εδώ δύο παραδείγματα άπειρων ομάδων συμμετριών που σχετίζονται με επικαλύψεις του επιπέδου. Θα περιορισθούμε σε διαισθητικές παρατηρήσεις.

    Φανταστείτε το επίπεδο καλυμμένο με το ακόλουθο μοτίβο και θεωρείστε την ομάδα G των ισομετριών του επιπέδου που διατηρούν την επικάλυψη αυτή. Αληθεύει ότι η G περιέχει άπειρο το πλήθος μεταφορές και άπειρο το πλήθος ανακλάσεις και άπειρο το πλήθος περιστροφές; Αληθεύει ότι η G περιέχει αντίγραφο της ομάδας D_3; Της D_4;



Στη συνέχεια θεωρείστε την επικάλυψη του επιπέδου από ίσα ισόπλευρα τρίγωνα όπως υποδεικνύει η ακόλουθη εικόνα και εξετάστε τα ίδια ερωτήματα για την νέα ομάδα H.



Διαισθητικά, οι ομάδες G, H είναι ΄ίδιες΄; Ποια επικάλυψη είναι ΄πιο συμμετρική΄; Ποια έχει περισσότερες οικογένειες παραλλήλων αξόνων συμμετρίας;

Στο σύνδεσμο Wallpaper groups μπορείτε να δείτε μερικά πράγματα για τις επίπεδες κρυσταλλογραφικές ομάδες. Η ομάδα G είναι η $p31m$ και η ομάδα H είναι η $p6m$.

Υποδείξεις Ασκήσεων Κεφαλαίου 7

1.

2. *Λύση.* Έστω $r_a \in G$ η περιστροφή του επιπέδου κατά γωνία a. Είναι σαφές ότι για κάθε θετικό ακέραιο m έχουμε $(r_a)^m = r_{ma}$. Άρα $(r_a)^m = 1 \Leftrightarrow ma = 2k\pi, k \in \mathbb{Z}$. Συνεπώς επιλέγοντας $a = 2\pi x$, όπου x άρρητος, έχουμε $(r_a)^m \neq 1$ για κάθε $m \in \mathbb{Z}$, δηλαδή το r_a έχει άπειρη τάξη.

   Από τα παραπάνω έπεται ότι για κάθε θετικό ακέραιο m η περιστροφή κατά γωνία $\frac{2\pi}{m}$ έχει τάξη m.

3. *Λύση.* Έστω r η περιστροφή κατά γωνία $\frac{2\pi}{n}$. Ξέρουμε ότι $r \in S(D_n)$ και $|r| = n$. Συνεπώς το στοιχείο r^m έχει τάξη d όπου $m = \frac{n}{d}$

4. *Λύση.* Έχουμε $\sigma = \sigma^{-1} \Leftrightarrow \sigma^2 = 1 \Leftrightarrow |\sigma| \leq 2$. Από το Πόρισμα 7.19, η τελευταία σχέση ισοδυναμεί με $|\sigma_i| \leq 2$ για κάθε i, δηλαδή με $l(\sigma_i) \leq 2$.

5. *Λύση.*
   i) Παρατηρούμε ότι $a^s = 1 \Leftrightarrow (a^s)^{-1} = 1 \Leftrightarrow (a^{-1})^s = 1$. Άρα $|a| = |a^{-1}|$.
   ii) Παρατηρούμε ότι $(b^{-1}ab)^2 = b^{-1}abb^{-1}ab = b^{-1}a^2b$. Γενικά με επαγωγή παίρνουμε, $(b^{-1}ab)^s = b^{-1}a^sb$, για κάθε $s \in \mathbb{Z}_{>0}$. Επομένως $(b^{-1}ab)^s = 1 \Leftrightarrow b^{-1}a^sb = 1 \Leftrightarrow a^s = 1$. Άρα $|b^{-1}ab| = |a|$.
   iii) Χρησιμοποιώντας το ii) έχουμε $b^{-1}(ba)b = ab \Rightarrow |ba| = |ab|$.
   iv) Έστω $a = |k| < \infty$. Από την ισότητα $b^{-1}a^2b = a^3$ και από ii), έχουμε

$$|a^2| = |a^3| \Rightarrow \frac{k}{\mu\kappa\delta(k,2)} = \frac{k}{\mu\kappa\delta(k,3)} \Rightarrow \mu\kappa\delta(k,2) = \mu\kappa\delta(k,3).$$

   Επομένως $2 \nmid k$ και $3 \nmid k$. Επειδή $a > 1$, έπεται ότι $k \geq 5$.

6. *Λύση.* Έστω $b \in G$. Τότε από το δεύτερο ερώτημα της άσκησης 2, παίρνουμε $|b^{-1}ab| = |a|$, άρα $|b^{-1}ab| = 2$. Από τη μοναδικότητα έπεται ότι $b^{-1}ab = a$, δηλαδή $ab = ba$.

7. *Λύση.* Από $abc = 1$ έχουμε $bc = a^{-1}$ και επομένως $bca = 1$.

   Δεν αληθεύει ότι $bac = 1$. Ένα παράδειγμα είναι η ομάδα S_3,
   όπου $(12)(13)(123) = 1$, αλλά $(13)(12)(123) = (132) \neq 1$.

8. *Λύση.* Αν $|g| = n$, τότε για κάθε ακέραιο m σχετικό πρώτο με το n, ξέρουμε ότι $|g^m| = \frac{n}{\mu\kappa\delta(m,n)} = n$. Από τον ορισμό της τάξης, τα στοιχεία $g, g^2, ..., g^{n-1}$ είναι διακεκριμένα Το πλήθος αυτών που έχουν εκθέτη m σχετικά πρώτο με το n είναι η τιμή $\varphi(n)$ της συνάρτησης του Euler.

9. Υπόδειξη. Με το συμβολισμό του Παραδείγματος 7.4(10), δείξτε ότι καθένα από τα $s, rs, ..., r^{n-1}s$ έχει τάξη 2. Στη συνέχεια εξετάστε ποιες περιστροφές έχουν τάξη 2.
   Απάντηση. Το ζητούμενο πλήθος είναι n αν το n είναι περιττός και $n+1$ αν το n είναι άρτιος.

10. *Λύση.* Γνωρίζουμε ότι κάθε $\sigma \in S_n$ γράφεται ως γινόμενο ξένων κύκλων και αν $\sigma = \sigma_1\sigma_2\cdots\sigma_m$, όπου σ_i κύκλοι ανά δύο ξένοι, τότε $|\sigma| = \text{εκπ}(k_1, k_2, \cdots, k_n)$, $k_i = l(\sigma_i)$.

    i) Άρα κάθε $\sigma \in S_4$ τάξης 2 είναι ή κύκλος μήκους 2, $(i\ j)$, ή γινόμενο 2 ξένων κύκλων μήκους 2, $(i\ j)(k\ l)$, (δεν μπορούμε να έχουμε περισσότερους από 2 παράγοντες διότι είμαστε στη S_4). Επομένως έχουμε $\binom{4}{2} + \frac{1}{2}\binom{4}{2} = 6 + 3 = 9$ στοιχεία τάξης 2.

    ii) Μια μετάθεση $\sigma \in S_5$ έχει τάξη $|\sigma| = 3$ αν και μόνο αν είναι γινόμενο ξένων ανά δύο κύκλων μήκους 3. Επειδή $3+3 > 5$ δεν μπορούμε να έχουμε περισσότερους από έναν τέτοιο κύκλο. Άρα $\sigma = (a_1\ a_2\ a_3)$. Υπενθυμίζουμε ότι αν A πεπερασμένο σύνολο με n στοιχεία, τότε το πλήθος των υποσυνόλων του A που έχουν k στοιχεία είναι $\binom{n}{k}$, $1 \leq k \leq n$. Για το σύνολο $\{a_1, a_2, a_3\} \subseteq \{1, 2, \cdots, 5\}$ υπάρχουν $\binom{5}{3} = 10$ επιλογές.

Εξετάζουμε τώρα πόσοι διαφορετικοί κύκλοι $(b_1\ b_2\ b_3)$ υπάρχουν με $\{b_1, b_2, b_3\} = \{a_1, a_2, a_3\}$. Παρατηρούμε ότι

$$\begin{aligned}(a_1\ a_2\ a_3) &\neq (a_2\ a_1\ a_3),\\ (a_1\ a_2\ a_3) &= (a_2\ a_3\ a_1) = (a_3\ a_1\ a_2),\\ (a_2\ a_1\ a_3) &= (a_1\ a_3\ a_2) = (a_3\ a_2\ a_1).\end{aligned}$$

Τελικά υπάρχουν $\binom{5}{3} \cdot 2 = 20$ στοιχεία της S_5 τάξης 3.

ii)Συνεχίζοντας το προηγούμενο επιχείρημα απαρίθμησης, δείξτε ότι η S_9 έχει

- $2\binom{9}{3}$ κύκλους μήκους 3,
- $\frac{2\binom{9}{3}2\binom{6}{3}}{2}$ γινόμενα δύο ξένων κύκλων μήκους 3, και
- $\frac{2\binom{9}{3}2\binom{6}{3}2\binom{3}{3}}{6}$ γινόμενα τριών κύκλων μήκους 3 που είναι ξένα ανά δύο.

Ο ζητούμενος αριθμός είναι το άθροισμα των παραπάνω, 5768.

11. *Λύση.* Έστω $\sigma = \sigma_1\sigma_2\cdots\sigma_m$, όπου σ_i είναι κύκλοι ξένοι ανά δύο. Αφού $\sigma \in S_{10}$ έχει τάξη 14, έπεται ότι αν k_i είναι το μήκος του σ_i, τότε $14 = \text{εκπ}\{k_1, \cdots, k_m\}$. Γνωρίζουμε ότι $1 \leq k_i \leq 10,\ k_1 + k_2 + \cdots + k_m = 10$. (Στην ανάλυση συμπεριλαμβάνουμε και τους 1-κύκλους αν υπάρχουν.) Επειδή $7|14$ υπάρχει k_i ώστε $7|k_i$, δηλαδή $k_i = 7$. Έστω ότι $k_1 = 7$. Ομοίως το $2|14$, άρα υπάρχει k_j ώστε $2|k_j$. Έχουμε $j \neq 1$, αφού $k_1 < 14$. Έστω $2|k_2$. Άρα $k_2 = 2$. (Αν $k_2 \geq 4$, τότε $k_1 + k_2 > 10$.) Επειδή $k_1 = 7,\ k_2 = 2$ και $\sum k_i = 10$, έπεται ότι $m = 3$ και $k_3 = 1$. Δηλαδή $\sigma = \sigma_1\sigma_2\sigma_3$ και $\sigma_3 = (i)$, όπου $i \notin \{a_1, \cdots, a_7\} \cup \{b_1, b_2\}$, $\sigma_1 = (a_1\ a_2 \cdots a_7),\ \sigma_2 = (b_1\ b_2)$. Επειδή $\{a_1, \cdots, a_7\} \cap \{b_1, b_2\} = \emptyset$, για το i υπάρχει μοναδική επιλογή

12. *Λύση.* Έστω $a, b \in G$. Από την υπόθεση έπεται ότι $(ab)^2 = 1$. Άρα

$$abab = 1 \Rightarrow ba = a^{-1}b^{-1} = ab,$$

αφού $a^2 = b^2 = 1$.

13. *Λύση.* Θεωρούμε το σύνολο $B = \{a^{-1}g \in G : a \in A\}$. Έστω $g \in G$. Θα δείξουμε ότι $|B| > \frac{|G|}{2}$. Η απεικόνιση $f : A \to B$ με $f(a) = a^{-1}g$ είναι 1-1. Πράγματι, έστω $a_1, a_2 \in A$ με $f(a_1) = f(a_2)$. Τότε $a_1^{-1}g = a_2^{-1}g \Rightarrow a_1^{-1} = a_2^{-1} \Rightarrow a_1 = a_2$. Προφανώς η f είναι και επί. Άρα $|B| = |A| > \frac{|G|}{2}$. Επομένως $A \cap B \neq \emptyset$. Δηλαδή υπάρχει $a' \in A$ και $a^{-1}g \in B$ $(a \in A)$ ώστε $a^{-1}g = a' \Rightarrow g = aa'$.

14. *Λύση.*
    i) Λάθος. Αν το $a \in G$ έχει $|a| = 3$, τότε $|a^2| = \frac{3}{\mu\kappa\delta(3,2)} = 3$ και $a \neq a^2$. (Αν $a = a^2$, τότε $a = 1$ που δεν έχει τάξη 3.)
    Σημείωση. Αν η G έχει στοιχεία τάξης $m(< \infty)$, τότε η G έχει τουλάχιστον $\varphi(m)$ στοιχεία τάξης m. Αυτό έπεται από την $|a^k| = \frac{m}{\mu\kappa\delta(k,m)}$.
    ii) Λάθος. Έστω $G = S_3$ και $a = (123),\ b = (213)$. Τότε $a \neq b$, ενώ $a^3 = b^3 = 1$.
    iii) Σωστό. Υπάρχουν $m, n \in \mathbb{Z}$ ώστε $1 = 3m + 5n$. Τότε

$$a = a^1 = (a^3)^m(a^5)^n = (b^3)^m(b^5)^n = b^{3m+5n} = b.$$

    iv) Σωστό. Υπενθυμίζουμε ότι κάθε $\sigma \in S_6$ γράφεται ως γινόμενο κύκλων ξένων ανά δύο, $\sigma = \sigma_1\sigma_2\cdots\sigma_m$. Επίσης $|\sigma| = \text{εκπ}(k_1, k_2, \cdots, k_m)$, όπου k_i το μήκος του κύκλου σ_i. Καταγράφουμε όλες τις δυνατές περιπτώσεις για το στοιχείο $(k_1, k_2, \cdots, k_m) \in \mathbb{Z}_{>0}^m$ με τον προηγούμενο συμβολισμό. Επειδή οι ξένοι κύκλοι αντιμετατίθενται μπορούμε να υποθέσουμε ότι $k_1 \geq k_2 \geq \cdots \geq k_m$.

$(k_1 \geq ... \geq k_m)$	$\varepsilon\kappa\pi(k_1, ..., k_m)$
(6)	6
(5,1)	5
(4,2)	4
(4,1,1)	4
(3,3)	3
(3,2,1)	6
(3,1,1,1)	3
(2,2,2)	2
(2,2,1,1)	2
(2,1,1,1,1)	2
(1,1,1,1,1,1)	1

Τάξεις στοιχείων της S_6

Άρα το max του $\{|\sigma| : \sigma \in S_6\}$ είναι το 6.

15. *Υπόδειξη.* Αν $\sigma = (a_1\ a_2\ ...\ a_k)$, τότε $\sigma^m(a_i) = a_{[i+m]}$ όπου $[i+m]$ το υπόλοιπο της διαίρεσης του $i+m$ με το k. Δείξτε ότι η τροχιά του a_i κάτω από τη σ^m είναι

$$a_i, a_{[i+m]}, a_{[1+2m]}, ..., a_{[i+(\frac{k}{d}-1)m]}.$$

(Μην ξεχάσετε να δείξτε ότι τα στοιχεία αυτά είναι διακεκριμένα).

16. *Λύση.* Έστω ότι $(123...n)\sigma = \sigma(123...n)$. Θεωρώντας στα δύο μέλη την εικόνα του i παίρνουμε $[\sigma(i)+1] = \sigma([i+1])$, όπου $[j]$ είναι το υπόλοιπο της διαίρεσης του j με το n. Με μια άμεση επαγωγή προκύπτει ότι $\sigma([i+1]) = [m+i]$, όπου $m = \sigma(1)$. Άρα $\sigma = (123...n)^m$. Το αντίστροφο είναι άμεσο.

17. Κατά τα γνωστά βρίσκουμε την ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων, $\sigma = (123)(456)$. Έχουμε $|\sigma| = \varepsilon\kappa\pi(3,3) = 3$ και επομένως $|\sigma^{100}| = \frac{3}{\mu\kappa\delta(3,100)} = 3$.

Έστω ότι υπάρχει $\tau \in S_6$ τέτοιο ώστε $\tau^3 = \sigma$. Τότε $\tau^9 = \sigma^3 = 1$ πράγμα που σημαίνει ότι $|\tau| \in \{1, 3, 9\}$. Η περίπτωση $|\tau| = 9$ αποκλείεται διότι η ομάδα S_6 δεν διαθέτει στοιχείο τάξης 9, όπως είδαμε στην άσκηση 7.14. Η περίπτωση $|\tau| = 1$, δηλαδή $\tau = 1$, επίσης αποκλείεται καθώς τότε θα είχαμε $\sigma = \tau^3 = 1$. Και η περίπτωση $|\tau| = 3$ αποκλείεται καθώς τότε θα είχαμε $\sigma = \tau^3 = 1$. Τελικά δεν υπάρχει $\tau \in S_6$ με $\tau^3 = \sigma$.

18. *Υπόδειξη.* Δείξτε ότι αν σ είναι όπως στην εκφώνηση, τότε $|\sigma| = 5$ και άρα η σ είναι κύκλος μήκους 5. Στη συνέχεια δείξτε ότι υπάρχει μοναδικό τέτοιο σ, $\sigma = (14253)$.

19. *Υπόδειξη.* Όπως το Παράδειγμα 7.20(3). *Απάντηση.* $m \equiv 0, 3, 4, 8, 9 \mod 12$.

20. *Λύση.* Έστω $\mu\kappa\delta(a, n) = d > 1$. Παρατηρούμε ότι

$$\sigma\left(\left[\frac{n}{d}\right]\right) = \left[a\frac{n}{d}\right] = \left[\frac{a}{d}n\right] = [0].$$

Δηλαδή,

$$\sigma([0]) = ([0]) \quad \text{και} \quad \sigma\left(\left[\frac{n}{d}\right]\right) = ([0]),$$

με $\left[\frac{n}{d}\right] \neq 0$ αφού $d > 1$. Άρα η σ δεν είναι 1-1 (άρα δεν είναι μετάθεση).

Αντίστροφα, έστω $\mu\kappa\delta(a, n) = 1$. Θα δείξουμε ότι η σ είναι μετάθεση του $\mathbb{Z}_n$. Παρατηρούμε πρώτα ότι η σ είναι 1-1. Πράγματι, έστω $\sigma([b_1]) = \sigma([b_2])$. Τότε

$$[ab_1] = [ab_2] \Rightarrow n|a(b_1 - b_2) \overset{\mu\kappa\delta(a,n)=1}{\Longrightarrow} n|b_1 - b_2 \Rightarrow [b_1] = [b_2].$$

Επίσης η σ είναι επί. Πράγματι είναι 1-1 και το $\mathbb{Z}_n$ είναι πεπερασμένο σύνολο.

Για $n = 9$ και $a = 4$ έχουμε

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 3 & 7 & 2 & 6 & 1 & 5 & 9 \end{pmatrix}.$$

(Για παράδειγμα $\sigma[5] = [4 \cdot 5] = [20] = [2]$.) Παρατηρούμε ότι

$$\sigma(1) = 4,\ \sigma(4) = 7,\ \sigma(7) = 1,$$
$$\sigma(2) = 8,\ \sigma(8) = 5,\ \sigma(5) = 2,\ \text{και}$$

$$\sigma(3) = 3,\ \sigma(6) = 6,\ \sigma(9) = 9.$$

Επομένως η ανάλυση της σ σε ξένους κύκλους είναι, $\sigma = (147)(285)$. Επειδή οι ξένες μεταθέσεις αντιμετατίθενται έχουμε,

$$\sigma^{2020} = ((147)(285))^{2020} = (147)^{2020}(285)^{2020}.$$

Από την Πρόταση 7.8, έπεται ότι $(147)^3 = 1$, άρα

$$(147)^{2020} = \left((147)^3\right)^{673}(147) = 1^{673}(147) = (147).$$

Ομοίως, $(285)^{2020} = (285)$. Άρα $\sigma^{2020} = (147)(285)$.

21. *Λύση* για το δεύτερο ερώτημα. Έστω ότι οι τάξεις των g, h είναι m, n αντίστοιχα και $e =$εκπ(m, n). Για κάθε θετικό ακέραιο k έχουμε $(g, h)^k = (g^k, h^k)$. Άρα

$$(g, h)^k = (1_G, 1_H) \Leftrightarrow g^k = 1_G, h^k = 1_H \Leftrightarrow m|k, n|k \Leftrightarrow e|k.$$

Άρα η τάξη του (g, h) είναι e.

22. *Λύση.* Επειδή οι m, n είναι σχετικά πρώτοι, υπάρχουν $a, b \in \mathbb{Z}$ με $1 = am + bn$. Θέτοντας $x = g^{bn}$ και $y = g^{am}$, έχουμε $xy = yx = g^{am+bn} = g$ και επίσης $x^m = (g^{mn})^b = 1, y^n = (g^{mn})^a = 1$. Για τη μοναδικότητα, έστω $w, z \in G$ με $wz = zw = g, w^m = z^n = 1$. Τότε

$$g^n = (wz)^n = w^n z^n = w^n \Rightarrow g^{bn} = w^{bn} = x^{1-am} = w.$$

Όμοια αποδεικνύεται ότι $z = g^{am}$. Άρα τα x, y είναι μοναδικά.

23. *Υπόδειξη.* Όπως το Παράδειγμα 7.20(1). *Απάντηση.* Τα θετικά πολλαπλάσια του 6.

24. *Απάντηση.* $(p-1)! + 1$.

25.

26.

27. *Απάντηση.* Του τετραγώνου και του ισόπλευρου τριγώνου αντίστοιχα, δηλαδή, D_4 και D_3.

Υποομάδες και το θεώρημα του Lagrange

Εδώ συνεχίζουμε τη μελέτη ομάδων. Αρχικά εξετάζουμε υποομάδες και το θεώρημα του Lagrange. Στη συνέχεια μελετάμε κυκλικές ομάδες και δείχνουμε ότι η πολλαπλασιαστική ομάδα πεπερασμένου σώματος είναι κυκλική. Τέλος εξετάζουμε τις άρτιες και περιττές μεταθέσεις και την έννοια της υποομάδας που παράγεται από σύνολο.

Βασικά σημεία

- υποομάδες
- θεώρημα του Lagrange
- κυκλικές ομάδες
- η πολλαπλασιαστική ομάδα πεπερασμένου σώματος
- πρόσημο μετάθεσης και η υποομάδα των άρτιων μεταθέσεων
- παραγόμενες υποομάδες

8.1. Υποομάδες

Ορισμός 8.1. *Έστω G ομάδα. Ένα μη κενό υποσύνολο $H \subseteq G$ λέγεται* **κλειστό** *υποσύνολο της G, αν $ab \in H$ για κάθε $a, b \in H$.*

Σημειώνουμε ότι αν το $H \subseteq G$ είναι κλειστό, τότε ορίζεται μια πράξη στο H

$$H \times H \to H,\ (a, b) \mapsto ab,$$

που είναι απλά ο περιορισμός της πράξης της G.

Ορισμός 8.2. *Έστω G ομάδα και $H \subseteq G$ κλειστό υποσύνολο της G. Το H λέγεται* **υποομάδα** *της G, αν το H είναι ομάδα ως προς την παραπάνω πράξη του H. Στην περίπτωση αυτή θα γράφουμε $H \leq G$.*

Παρατηρήσεις. Έστω $H \leq G$. Τότε ισχύουν τα ακόλουθα.

(1) $1_H = 1_G$.

(2) Έστω $h \in H$. Τότε το αντίστροφο του h στην H είναι ίσο με το αντίστροφο του h στη G.

Παραδείγματα 8.3.

(1) Έστω $G = \mathbb{Z}$ (με πράξη την πρόσθεση). Το $\mathbb{N}$ είναι κλειστό υποσύνολο του $\mathbb{Z}$, αλλά όχι υποομάδα.

(2) $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Z} \leq \mathbb{R}$, $\mathbb{Z} \leq \mathbb{C}$, $\mathbb{Q} \leq \mathbb{R}$, $\mathbb{Q} \leq \mathbb{C}$, $\mathbb{R} \leq \mathbb{C}$.

(3) $\mathbb{R} \setminus \{0\}$ είναι υποομάδα του $\mathbb{C} \setminus \{0\}$ (με πράξη τον πολλαπλασιασμό).

(4) Έστω $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Τότε $E_n \leq \mathbb{C} \setminus \{0\}$.

Πριν δούμε λιγότερο βαρετά παραδείγματα, σημειώνουμε ένα απλό και χρήσιμο κριτήριο.

Πρόταση 8.4. *Έστω G ομάδα και $H \subseteq G$, $H \neq \emptyset$. Τότε οι ιδιότητες (1) – (3) είναι ισοδύναμες.*

(1) *$H \leq G$.*
(2) *Για κάθε $a, b \in H$, ισχύει $ab \in H$ και $a^{-1} \in H$.*
(3) *Για κάθε $a, b \in H$, ισχύει $ab^{-1} \in H$.*
Αν επιπλέον το σύνολο H είναι πεπερασμένο, τότε οι παραπάνω ιδιότητες είναι ισοδύναμες με την (4).
(4) *Για κάθε $a, b \in H$, ισχύει $ab \in H$.*

Απόδειξη. (1) $\Rightarrow$ (2). Άμεσο από τον ορισμό.
(2) $\Rightarrow$ (3). Έστω $a, b \in H$. Τότε από την υπόθεση έπεται ότι $a, b^{-1} \in H$. Επομένως πάλι από την υπόθεση παίρνουμε ότι $ab^{-1} \in H$.
(3) $\Rightarrow$ (1). Έστω $a \in H$ ($H \neq \emptyset$). Τότε $aa^{-1} \in H$, δηλαδή $1_G \in H$. Έστω $a \in H$. Από πριν έχουμε $1_G \in H$, άρα $1_G a^{-1} \in H$, οπότε $a^{-1} \in H$. Έστω $a, b \in H$. Τότε $ab^{-1} \in H$, άρα $a(b^{-1})^{-1} \in H$, δηλαδή $ab \in H$, άρα H κλειστό. Τέλος, αν $a, b, c \in H$, τότε

$$a(bc) = (ab)c,$$

αφού $H \subseteq G$ και G ομάδα. Από τον ορισμό της ομάδας έχουμε ότι $H \leq G$.
Υποθέτουμε τώρα ότι το σύνολο H είναι πεπερασμένο. Αρκεί να δείξουμε ότι (4) $\Rightarrow$ (2). Έστω $a \in H$. Από την υπόθεση, τα στοιχεία $a, a^2, a^3, \ldots$ ανήκουν στο πεπερασμένο σύνολο H. Συνεπώς υπάρχουν θετικοί ακέραιοι $m > n$ με $a^m = a^n$. Άρα στη G έχουμε $a^{m-n} = 1_G$, που σημαίνει ότι $1_G \in H$. Πάλι στη G έχουμε

$$a^{-1} = a^{m-n-1}.$$

Αν $m - n - 1 = 0$, τότε $a^{-1} = 1_G \in H$. Αν $m - n - 1 > 0$, τότε πάλι $a^{-1} = a^{m-n-1} \in H$. □

Παραδείγματα 8.5.

(1) Έστω $G = GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$. Ξέρουμε ότι η G είναι ομάδα ως προς τον πολλαπλασιασμό πινάκων, βλ. Παράδειγμα 7.4 (2). Έστω $H = SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$. Τότε $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.
Πράγματι, αν $A, B \in SL_n(\mathbb{R})$, τότε $\det A = \det B = 1$ και επομένως

$$\det(AB) = (\det A)(\det B) = 1 \Rightarrow AB \in SL_2(\mathbb{R}), \text{ και}$$

$$\det A^{-1} = \frac{1}{\det A} = 1 \Rightarrow A^{-1} \in SL_n(\mathbb{R}).$$

(2) Έστω $G = S_n$ και $H = \{\sigma \in S_n : \sigma(n) = n\}$. Τότε $H \leq S_n$.
Πράγματι, το H είναι μη κενό πεπερασμένο υποσύνολο του S_n και αν $\sigma, \tau \in H$, τότε

$$\sigma\tau(n) = \sigma(\tau(n)) = \sigma(n) = n \Rightarrow \sigma\tau \in H.$$

Επομένως $H \leq S_n$.

(3) Έστω G αβελιανή ομάδα και $H = \{g \in G : g^2 = 1\}$. Τότε $H \leq G$.

Πράγματι, $H \neq \emptyset$, αφού $1 \in H$. Έστω $a, b \in H$. Τότε $a^2 = b^2 = 1$. Επειδή η G είναι αβελιανή έχουμε

$$(ab)^2 = a^2b^2 = 1,$$

άρα $ab \in H$. Επειδή $a^2 = 1$, έχουμε $(a^{-1})^2 = (a^2)^{-1} = 1$. Επομένως $a^{-1} \in H$.

Σημείωση. Αν η ομάδα G δεν είναι αβελιανή τότε το σύνολο $H = \{g \in G : g^2 = 1\}$ δεν είναι αναγκαστικά υποομάδα. Πράγματι έστω $G = S_3$. Τότε $H = \{1, (12), (13), (23)\}$. Παρατηρούμε ότι $(12)(13) = (132) \notin H$, άρα $H \not\leq G$.

(4) Έστω G ομάδα και

$$Z(G) = \{a \in G : ag = ga, \ \text{για κάθε} \ a \in G\}.$$

Το $Z(G)$ λέγεται το **κέντρο** της ομάδας G. Έχουμε $Z(G) \leq G$.

Πράγματι, $Z(G) \neq \emptyset$, αφού $1g = g1$ για κάθε $g \in G$. Άρα $1 \in Z(G)$. Έστω $a, b \in Z(G)$. Τότε $ag = ga$ και $bg = gb$ για κάθε $g \in G$. Συνεπώς $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$. Άρα $ab \in Z(G)$.

Έστω $a \in Z(G)$. Τότε $ag = ga$ για κάθε $g \in G$. Επομένως

$$(ag)^{-1} = (ga)^{-1} \Rightarrow g^{-1}a^{-1} = a^{-1}g^{-1},$$

που ισχύει για κάθε $g \in G$. Γράφοντας την παραπάνω σχέση για g^{-1} στην θέση του g παίρνουμε, $(g^{-1})^{-1}a^{-1} = a^{-1}(g^{-1})^{-1} \Rightarrow ga^{-1} = a^{-1}g$. Δηλαδή $a^{-1} \in Z(G)$.

(5) 'Εστω G ομάδα και H, K υποομάδες της G. Τότε η τομή $H \cap K$ είναι υποομάδα της G.

Πράγματι, επειδή $1_G \in H$ και $1_G \in K$, έχουμε $1_G \in H \cap K$, δηλαδή $H \cap K$ είναι μη κενό σύνολο.

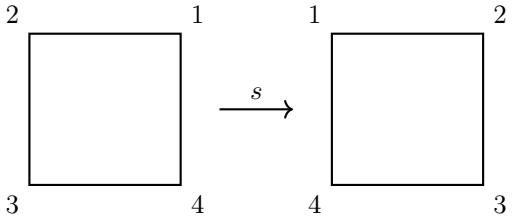
Αν $a, b \in H \cap K$, τότε $a \in H$ και $b \in K$, οπότε σύμφωνα με την Πρόταση 8.4

$$ab^{-1} \in H \ \text{ και } \ ab^{-1} \in K.$$

Άρα $ab^{-1} \in H \cap K$. Συνεπώς $H \cap K \leq G$.

Όμοια αποδεικνύεται ότι η τομή οποιασδήποτε οικογένειας υποομάδων ομάδας G είναι υποομάδα της G. Η ένωση δύο υποομάδων της G δεν είναι γενικά υποομάδα της G, βλ. άσκηση 8.35.

(6) **Συμμετρίες ως μεταθέσεις** Εδώ θα δούμε πως περιγράφουμε την ομάδα D_4 των συμμετριών του τετραγώνου ως υποομάδα της S_4. Ένα στοιχείο της D_4 είναι η ανάκλαση s ως προς τον κατακόρυφο άξονα όπως δείχνει το σχήμα



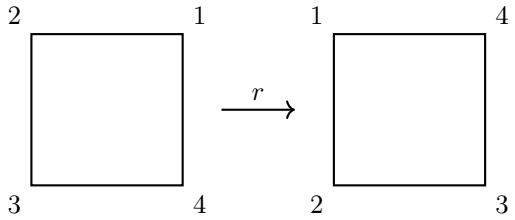
Παρατηρούμε ότι οι εικόνες των κορυφών κάτω από την απεικόνιση s είναι

$$1 \mapsto 2, \ 2 \mapsto 1, \ 3 \mapsto 4, \ 4 \mapsto 3.$$

Έτσι η s αντιστοιχεί στη μετάθεση

$$s \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34).$$

Με τον ίδιο τρόπο, βλέπουμε ότι η περιστροφή r κατά γωνία $\pi/2$



αντιστοιχεί στον κύκλο (1234).

Συνεχίζοντας τα παραπάνω για κάθε στοιχείο της D_4 βρίσκουμε το ακόλουθο σύνολο μεταθέσεων

$$\{1, (12)(34), (14)(23), (24), (13), (1234), (13)(14), (1432)\}.$$

Εύκολα αποδεικνύεται ότι το παραπάνω σύνολο είναι κλειστό υποσύνολο της S_4 και άρα είναι υποομάδα. Είναι σαφές ότι κάτω από την προηγούμενη αντιστοίχιση, η σύνθεση συμμετριών του τετραγώνου αντιστοιχεί στο γινόμενο μεταθέσεων.
Με ανάλογο τρόπο μπορεί να περιγραφεί η D_n ως υποομάδα της S_n.

(7) Έστω $m, n \in \mathbb{Z}_{>0}$ και $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Τότε $E_m \leq E_n$ αν και μόνο αν $m|n$.

Πράγματι, έστω $E_m \leq E_n$. Είδαμε στο Παράδειγμα 7.4(5) ότι , $z = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m} \in E_m$ έχει τάξη m. Αφού $z \in E_n$ έπεται $z^n = 1$, οπότε από το Θεώρημα 7.15 παίρνουμε $m|n$. (Το τελευταίο συμπέρασμα θα μπορούσε να προκύψει και από πράξεις μιγαδικών με το θεώρημα του De Moivre).

Αντίστροφα, έστω $m|n$. Αφού οι E_m, E_n είναι ομάδες ως προς τον πολλαπλασιασμό μιγαδικών αριθμών, για να δείξουμε ότι $E_m \leq E_n$ είναι αρκετό να παρατηρήσουμε ότι $E_m \subseteq E_n$: αν $z^m = 1$, τότε $z^n = (z^m)^{\frac{n}{m}} = 1$.

8.2. Θεώρημα του Lagrange

Είδαμε στο τελευταίο από τα προηγούμενα παραδείγματα, ότι αν $E_m \leq E_n$, τότε $m|n$. Αυτό είναι ειδική περίπτωση του επόμενου θεωρήματος που είναι ένα από τα πιο σημαντικά αποτελέσματα του μαθήματος.

Θεώρημα 8.6 (Lagrange). *Έστω G πεπερασμένη ομάδα και $H \leq G$. Τότε*
$$|H| \mid |G|.$$

Απόδειξη. Θα δείξουμε ότι το σύνολο G είναι ξένη ένωση υποσυνόλων καθένα από τα οποία έχει $|H|$ στοιχεία. Έστω $a, b \in G$. Ορίζουμε την σχέση

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

Αυτή είναι μια σχέση ισοδυναμίας. Πράγματι,

(1) $a \sim a$ για κάθε $a \in G$, αφού $a^{-1}a = 1 \in H$.

(2) Αν $a \sim b$, τότε $b^{-1}a \in H \Rightarrow (b^{-1}a)^{-1} \in H \Rightarrow a^{-1}(b^{-1})^{-1} = a^{-1}b \in H$. Δηλαδή $b \sim a$.

(3) Αν $a \sim b$ και $b \sim c$, τότε $b^{-1}a \in H$ και $c^{-1}b \in H$. Τότε $(c^{-1}b)(b^{-1}a) = c^{-1}a \in H$. Δηλαδή $a \sim c$.

Από την Παράγραφο 2.2 ξέρουμε ότι για τις κλάσεις ισοδυναμίας

$$[a] = \{g \in G : g \sim a\}$$

ισχύουν τα εξής.

(1) $[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow b^{-1}a \in H$.

(2) Αν $a \nsim b$, τότε $[a] \cap [b] = \emptyset$.

Άρα έχουμε ξένη ένωση της μορφής $G = \bigcup_{a\in A}[a]$ για κάποιο $A \subseteq G$. Αν $a \in G$, θέτουμε

$$aH = \{ah : h \in H\}.$$

Τότε $[a] = aH$. Πράγματι, $[a] = \{g \in G : g \sim a\}$ και

$$g \sim a \Leftrightarrow a^{-1}g \in H \quad \Leftrightarrow \quad \text{υπάρχει } h \in H \text{ ώστε } g = ah.$$

Άρα έχουμε από πριν μια ξένη ένωση,

$$G = \bigcup aH, \quad a \in A.$$

Θα δείξουμε τώρα ότι

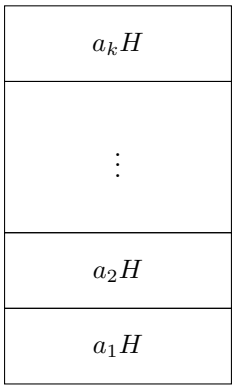
$$|aH| = |H|, \quad \text{για κάθε} \quad a \in G.$$

Πράγματι, η απεικόνιση $f : H \to aH, \quad f(h) = ah$ είναι 1-1 (αν $f(h_1) = f(h_2)$ τότε $ah_1 = ah_2 \Rightarrow h_1 = h_2$) και επί.

Έστω τώρα ότι η G είναι πεπερασμένη. Τότε έχουμε πεπερασμένη ξένη ένωση,

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH.$$

Άρα $|G| = |a_1H| + \cdots + |a_kH| = |H| + \cdots + |H| = k|H|$. Συνεπώς $|H| \mid |G|$. □



Η πεπερασμένη ομάδα G έχει διαμερισθεί σε k αριστερές κλάσεις της υποομάδας H καθεμιά από τις οποίες έχει $|H|$ στοιχεία.

Δείκτης υποομάδας

Έστω G ομάδα και $H \leq G$. Με G/H συμβολίζουμε το σύνολο των κλάσεων ισοδυναμίας της σχέσης ισοδυναμίας στο σύνολο G

$$a \sim b \Leftrightarrow b^{-1}a$$

που θεωρήσαμε στην απόδειξη του θεωρήματος του Lagrange. Τονίζουμε ότι στο σημείο εκείνο της απόδειξης δεν χρησιμοποιήσαμε ότι η G είναι πεπερασμένη, οπότε αυτά που θα πούμε εδώ ισχύουν και για άπειρες G. Είδαμε ότι

$$G/H = \{aH : a \in G\} \text{ και } aH = \{ah \in G : h \in G\}.$$

Θα καλούμε την κλάση aH την **αριστερή κλάση** της H στη G με αντιπρόσωπο το a.

Ορισμός 8.7. *Ο δείκτης της H στη G είναι το πλήθος των στοιχείων του συνόλου G/H και συμβολίζεται με $[G : H]$.*

Με τον παραπάνω συμβολισμό, η απόδειξη του θεωρήματος του Lagrange δίνει ότι

Θεώρημα 8.8. *αν G είναι πεπερασμένη ομάδα και H υποομάδα της G, τότε $[G : H] = \dfrac{|G|}{|H|}$.*

Παραδείγματα 8.9.

(1) Έστω G ομάδα με $n \leq 200$ και περιέχει υποομάδες H, K,με τάξεις 10 και 11 αντίστοιχα.
   i) Βρείτε την τάξη της G.
   ii) Δείξτε ότι $G = \{hk : h \in H, k \in K\}$ και επιπλέον, για κάθε $g \in G$ η παράσταση $g = hk$ με $h \in H, k \in K$ είναι μοναδική

Από το θεώρημα του Lagrange έχουμε $10|n$ και $11|n$. Επειδή οι 10, 11 είναι σχετικά πρώτοι, παίρνουμε $110|n$ και επειδή $n \leq 200$, έχουμε $n = 110$.
Για το δεύτερο ερώτημα, αρχικά παρατηρούμε ότι $G \supseteq \{hk : h \in H, k \in K\}$ γιατί τα σύνολα H, K είναι υποσύνολα της ομάδας G. Για να δείξουμε την ισότητα, αρκεί να δείξουμε ότι το δεξιό μέλος έχει τουλάχιστον $|G|$ στοιχεία. Αν $h' \in H, k' \in K$ είναι τέτοια ώστε $hk = h'k'$, τότε

$$(h')^{-1}h = k'k^{-1} \in H \cap K$$

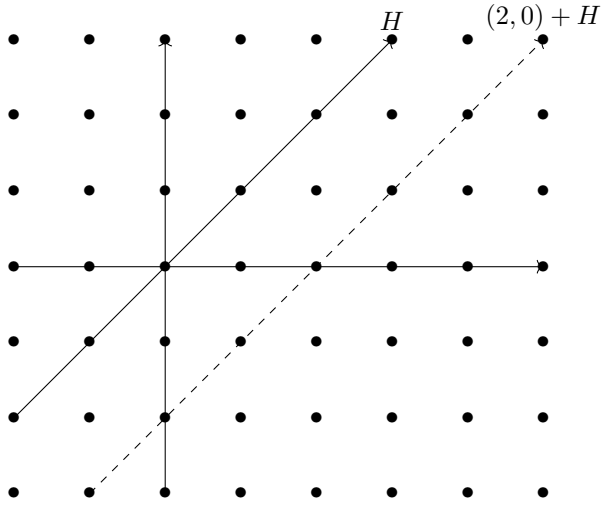
διότι οι H, K είναι υποομάδες. Ξέρουμε ότι η τομή $H \cap K$ είναι υποομάδα και της H και της K. Από το θεώρημα του Lagrange, η τάξη της τομής $H \cap K$ διαιρεί και το 10 και το 11, που είναι σχετικά πρώτοι. Άρα $H \cap K = \{1\}$ και επομένως $(h')^{-1}h = k'k^{-1} = 1$, δηλαδή $h = h', k = k'$. Συνεπώς, καθώς τα στοιχεία h, k διατρέχουν τα σύνολα H, K αντίστοιχα, τα στοιχεία hk είναι διακεκριμένα. Το πλήθος τους είναι $|H| \cdot |K| = 110 = |G|$.

(2) Έστω $G = \mathbb{Z}, m \in \mathbb{Z}$ και $H = m\mathbb{Z}$. Στην περίπτωση αυτή, η σχέση ισοδυναμίας που ορίσαμε στην απόδειξη του θεωρήματος του Lagrange, είναι ακριβώς η γνωστή ισοδυναμία ακεραίων $\mod m$, οπότε $G/H = \mathbb{Z}_m$.

(3) Έστω $G = \mathbb{Z} \times \mathbb{Z}$ και $H = \{(m, m) \in G : m \in \mathbb{Z}\}$. Υπενθυμίζουμε ότι η G είναι ομάδα με πράξη τη κατά συντεταγμένες πρόσθεση, $(x, y) + (x', y') = (x + x', y + y')$. Εύκολα επαληθεύεται ότι η H είναι υποομάδα. Εποπτικά, τα στοιχεία της G μπορούμε να τα σκεφτόμαστε ως τα σημεία του επιπέδου που έχουν ακέραιες συντεταγμένες. Τα στοιχεία της H αντιστοιχούν στα σημεία της ευθείας $y = x$ που έχουν ακέραιες συντεταγμένες. Η αριστερή κλάση του στοιχείου $(2, 0)$ είναι εξ ορισμού

$$(2, 0) + H = \{(2 + m, m) \in G : m \in \mathbb{Z}\}.$$

Στο σχήμα πρόκειται για τα σημεία με ακέραιες συντεταγμένες που βρίσκονται στη διακεκομμένη ευθεία $y = x - 2$.



(4) Είδαμε ότι αν G είναι πεπερασμένη ομάδα και $H \leq G$, τότε υπάρχει ξένη ένωση της μορφής

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH,$$

όπου $k = [G : H]$.

Έστω $G = S_4$ και $H = \{\sigma \in S_4 : \sigma(4) = 4\}$. Τότε $H \leq G$ (Παράδειγμα 8.5(2)). Παρατηρούμε ότι $[G : H] = \frac{|G|}{|H|} = \frac{4!}{3!} = 4$. Ας βρούμε μια επιλογή στοιχείων a_1, a_2, a_3, a_4

όπως παραπάνω. Θα δείξουμε ότι έχουμε την ξένη ένωση

$$S_4 = H \cup (14)H \cup (24)H \cup (34)H \ .$$

Δηλαδή εδώ έχουμε $a_1 = 1, a_2 = (14), a_3 = (24), a_4 = (34)$.

Πράγματι στο δεξί μέλος έχουμε μια ξένη ένωση, για παράδειγμα

$$\text{για κάθε } \ \sigma \in H, \ \sigma(4) = 4,$$

$$\text{για κάθε } \ \sigma \in (14)H, \ \ \sigma(4) = 1,$$

$$\text{για κάθε } \ \sigma \in (24)H, \ \ \sigma(4) = 2,$$

$$\text{για κάθε } \ \sigma \in (34)H, \ \ \sigma(4) = 3.$$

(Επίσης στο ίδιο συμπέρασμα καταλήγουμε δείχνοντας ότι για κάθε $i \neq j$ έχουμε $a_i^{-1}a_j(4) \neq 4$, δηλαδή $a_i^{-1}a_j \notin H$). Παρατηρούμε ότι

$$S_4 \supseteq a_1H \cup \cdots \cup a_4H$$

και επειδή

$$|S_4| = |a_1H| + \cdots + |a_4H|$$

(αφού $|a_1H| + \cdots + |a_4H| \overset{(\text{ξένη ένωση})}{=} 3! + 3! + 3! + 3! = 4! = 24$), έπεται ότι

$$S_4 = a_1H \cup \cdots \cup a_4H.$$

Είδαμε πριν ότι ο δείκτης $[G : H]$ είναι το πλήθος των αριστερών κλάσεων της H στη G. Θα εξετάσουμε τώρα δεξιές κλάσεις της H στη G και θα δούμε ότι ο αντίστοιχος δείκτης ταυτίζεται με τον προηγούμενο. Η ανάπτυξη εδώ θα είναι παρόμοια με πριν και επομένως θα είμαστε συνοπτικοί.

Έστω G ομάδα και $H \leq G$. Εύκολα αποδεικνύεται ότι η ακόλουθη σχέση στο σύνολο G είναι σχέση ισοδυναμίας,

$$a \sim b \Leftrightarrow ab^{-1} \in H.$$

Η κλάση ισοδυναμίας του a είναι

$$\{ha \in G : h \in H\}$$

που θα συμβολίζουμε με Ha και θα καλούμε τη **δεξιά κλάση** της H στη G με αντιπρόσωπο το a.

Η βασική παρατήρηση εδώ είναι η ακόλουθη. Έστω $a, b \in G$. Τότε

$$aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}.$$

Πράγματι, $aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow b^{-1}(a^{-1})^{-1} \in H \Leftrightarrow Hb^{-1} = Ha^{-1}$. Από την παρατήρηση έπεται ότι η αντιστοιχία $aH \leftrightarrow Ha^{-1}$ μεταξύ των αριστερών κλάσεων της H στη G και των δεξιών κλάσεων της H στη G είναι 1-1 και επί. Συνεπώς τώρα ξέρουμε ότι ο δείκτης $[G : H]$ ισούται με το πλήθος των αριστερών κλάσεων H στη G και το πλήθος των δεξιών κλάσεων της H στη G.

8.3. Κυκλικές ομάδες

Έστω G ομάδα και $g \in G$. Θεωρούμε το υποσύνολο

$$< g >= \{g^m \in G : m \in \mathbb{Z}\}.$$

Παρατηρούμε ότι $< g > \leq G$. Πράγματι, αν $g^{m_1} \in < g >$ και $g^{m_2} \in < g >$, τότε

$$(g^{m_1})(g^{m_2})^{-1} = g^{m_1}g^{-m_2} = g^{m_1-m_2} \in < g > .$$

Άρα $< g > \leq G$.

Η υποομάδα $< g >$ καλείται η **κυκλική υποομάδα** της G που παράγεται από το g. Καλό είναι να συγκριθεί αυτός ο ορισμός με τον ορισμό του κυρίου ιδεώδους που είδαμε στην Παράγραφο 5.3.

Με κίνδυνο ενοχλητικής επανάληψης, επισημαίνουμε ότι αν έχουμε προσθετικό συμβολισμό για την πράξη της G, τότε

$$< g >= \{mg \in G : m \in \mathbb{Z}\}.$$

Μια ομάδα G λέγεται **κυκλική** αν $G =< g >$ για κάποιο $g \in G$. Στην περίπτωση αυτή, θα λέμε ότι το g **παράγει** τη G ή ότι το g είναι **γεννήτορας** της G. Είναι σαφές ότι κάθε κυκλική υποομάδα είναι κυκλική ομάδα.

Παραδείγματα 8.10.

(1) Η κυκλική υποομάδα της $\mathbb{Z}$ που παράγεται από το $m \in \mathbb{Z}$ είναι $< m >= \{mg : g \in \mathbb{Z}\} = m\mathbb{Z}$.

(2) Η ομάδα $\mathbb{Z}$ είναι κυκλική και ένας γεννήτορας είναι το 1, δηλαδή $\mathbb{Z} =< 1 >$. Είναι σαφές ότι οι μόνοι γεννήτορες της κυκλικής ομάδας $\mathbb{Z}$ είναι οι 1 και -1.

(3) Για κάθε ακέραιο n, η ομάδα $\mathbb{Z}_n$ είναι κυκλική και ένας γεννήτορας είναι το στοιχείο $[1]$.

(4) Θεωρούμε την ομάδα $G = GL_2(\mathbb{Z})$ και το στοιχείο αυτής $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Με επαγωγή αποδεικνύεται ότι $g^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ για κάθε ακέραιο m. Άρα $< g >= \{\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} : m \in \mathbb{Z}\}$, που είναι μια άπειρη ομάδα.

Έστω p πρώτος. Θεωρούμε την ομάδα $H = GL_2(\mathbb{Z}_p)$ και το στοιχείο αυτής $h = \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix}$. Με επαγωγή αποδεικνύεται ότι $h^m = \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix}$ για κάθε ακέραιο m. Άρα $< h >= \{\begin{pmatrix} [1] & a \\ [0] & [1] \end{pmatrix} : a \in \mathbb{Z}_p\}$, που είναι μια πεπερασμένη ομάδα.

(5) Η ομάδα $U(\mathbb{Z}_5)$ είναι κυκλική καθώς, για παράδειγμα,

$$< [2] >= \{[1], [2], [4], [8]\} = \{[1], [2], [3], [4]\} = U(\mathbb{Z}_5).$$

Αντίθετα, η ομάδα $U(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$ δεν είναι κυκλική καθώς για κάθε $[a] \in U(\mathbb{Z}_8)$, είναι $[a]^2 = [1]$.

(6) Σημειώνουμε ότι κάθε κυκλική ομάδα G είναι αβελιανή. Πράγματι, έστω $G =< g >$ και $a, b \in G$. Τότε υπάρχουν ακέραιοι $m, n \in \mathbb{Z}$ με $a = g^m$ και $b = g^n$. Συνεπώς

$$ab = g^m g^n = g^{m+n} = g^n g^m = ba.$$

Συνεπώς κάθε μη αβελιανή ομάδα δεν είναι κυκλική. Για παράδειγμα, οι συμμετρικές ομάδες S_n, όπου $n \geq 3$, δεν είναι κυκλικές (βλ. Παρατήρηση (4) μετά τον Ορισμό 7.5)

Ο Fraleigh λέει ότι η απόδειξη του επόμενου πορίσματος είναι αγαπημένο θέμα εξετάσεων.

Πόρισμα 8.11. *Κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική.*

Απόδειξη. Έστω G ομάδα με $|G| = p$ πρώτος και έστω $g \in G, g \neq 1$. Τότε η υποομάδα $H =< g >$ της G δεν είναι τετριμμένη, $|H| > 1$ και από το θεώρημα του Lagrange έχει τάξη που διαιρεί το p. Άρα $|H| = p$, δηλαδή $|H| = |G|$. Επειδή η G είναι πεπερασμένη, παίρνουμε $G = H$, δηλαδή $G =< g >$ κυκλική. □

Θα δούμε τώρα πιο αναλυτικά τι συμβαίνει όταν κυκλική ομάδα παράγεται από στοιχείο πεπερασμένης τάξης.

Πρόταση 8.12. *Έστω G ομάδα και $g \in G$.*

(1) *Έστω ότι το g έχει πεπερασμένη τάξη, $|g| = k$. Τότε $< g >= \{1, g, ..., g^{k-1}\}$. Επιπλέον, για κάθε θετικό διαιρέτη d του k, το πλήθος των στοιχείων της $< g >$ που έχουν τάξη d είναι $\varphi(d)$.*

(2) *Αν η G είναι πεπερασμένη, $|G| = n$, και $|g| = k$, τότε $g^n = 1$ και $k|n$.*

Απόδειξη. (1) Πράγματι τα στοιχεία στο δεξί σύνολο είναι ανά δύο διαφορετικά (αφού $k = |g|$). Ο εγκλεισμός $\supseteq$ είναι προφανής. Έστω $g^m \in < g >$. Επειδή $g^k = 1$, έπεται ότι $g^m = g^r$, όπου το r είναι το υπόλοιπο της διαίρεσης του m με το k. Άρα $g^m = g^r \in \{1, g, g^2, \cdots, g^{k-1}\}$, δηλαδή $< g > \subseteq \{1, g, g^2, \cdots, g^{k-1}\}$.
(2) Είδαμε πριν ότι η τάξη της ομάδας $< g >$ είναι k. Από το θεώρημα του Lagrange έπεται ότι $k|n$. Από το Θεώρημα 7.17(1) έχουμε $g^n = 1$. □

Πόρισμα 8.13.

(1) *(Euler) Έστω $a, m \in \mathbb{Z}, m > 0$, με $\mu\kappa\delta(a, m) = 1$. Τότε $a^{\varphi(m)} \equiv 1 \mod m$.*

(2) *(Fermat) Έστω p πρώτος και $a \in \mathbb{Z}$. Τότε $a^p \equiv a \mod p$.*

Απόδειξη. (1) Θεωρούμε την ομάδα $U(\mathbb{Z}_m)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_m$ (με πράξη τον πολλαπλασιασμό του $\mathbb{Z}_m$). Ξέρουμε ότι $|U(\mathbb{Z}_m)| = \varphi(m)$ και

$$U(\mathbb{Z}_m) = \{[a] \in \mathbb{Z}_m : \mu\kappa\delta(a, m) = 1\}.$$

Από την προηγούμενη πρόταση έπεται ότι, αν $\mu\kappa\delta(a, m) = 1$, τότε $[a]^{\varphi(m)} = [1]$, δηλαδή $a^{\varphi(m)} \equiv 1 \mod m$.
(2)Αν $p|a$, τότε το ζητούμενο είναι σαφές. Αν $p \not| a$, τότε το ζητούμενο έπεται άμεσα από το (1). □

Παρατήρηση. Έστω G ομάδα, $g \in G$ και $H = < g >$. Είδαμε στην προηγούμενη πρόταση, ότι αν η τάξη του στοιχείου g είναι πεπερασμένη, $|g| = k$, τότε η τάξη της ομάδας H είναι $|H| = k$. Έτσι δικαιολογείται η χρήση της ίδιας ονομασίας 'τάξης'. Στην περίπτωση που το g έχει άπειρη τάξη, τότε και η ομάδα H έχει άπειρη τάξη καθώς αν $g^m = g^n$ για κάποιους $m > n$, τότε $g^{m-n} = 1$, που σημαίνει ότι η τάξη του g είναι πεπερασμένη.

Παραδείγματα 8.14.

(1) Έστω $G = < g >$ κυκλική ομάδα τάξης 12. Ποια είναι η τάξη της ομάδας $< g^{99} > \cap < g^{22} >$;
Επειδή το υπόλοιπο της διαίρεσης του 99 με το 12 είναι 3, έχουμε

$$< g^{99} > = < g^3 > = \{1, g^3, g^6, g^9\}.$$

Επειδή το υπόλοιπο της διαίρεσης του 26 με το 12 είναι 2, έχουμε

$$< g^{26} > = < g^2 > = \{1, g^2, g^4, g^6, g^8, g^{10}\}.$$

Άρα $< g^{99} > \cap < g^{26} > = \{1, g^6\}$ που έχει τάξη 2.

(2) Έστω $G = < g >$ κυκλική ομάδα τάξης 12 και $H = < g^3 > = \{1, g^3, g^6, g^9\}$. Άρα ο δείκτης $[G : H]$ ισούται με $|G|/|H| = 12/4 = 3$. Δηλαδή το πλήθος των αριστερών κλάσεων της H στη G είναι 3. Ισχυριζόμαστε ότι έχουμε την ξένη ένωση

$$G = H \cup gH \cup g^2H.$$

Πράγματι, επειδή το πλήθος των παραπάνω κλάσεων είναι ίσο με $[G : H]$, αρκεί να δείξουμε ότι είναι διακεχριμένες, ισοδύναμα ότι

$$g^{-i}g^j \notin H,$$

για κάθε $i, j \in \{0, 1, 2\}, i \neq j$. Αυτό επαληθεύεται άμεσα καθώς $H = \{1, g^3, g^6, g^9\}$.

Λίγο διαφορετικά θα μπορούσαμε απλά να σημειώσουμε ότι

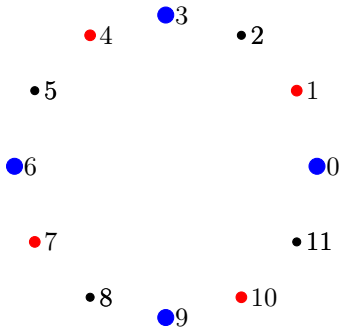
$$H = \{1, g^3, g^6, g^9\},$$

$$gH = \{g, g^4, g^7, g^{10}\},$$

$$g^2H = \{g^2, g^5, g^8, g^{11}\},$$

που προφανώς είναι ανά δύο ξένα σύνολα.
Στο ακόλουθο σχήμα φαίνονται οι αριστερές κλάσεις. Οι κορυφές του κανονικού κυρτού 12-γώνου αντιστοιχούν στα στοιχεία της κυκλικής ομάδας τάξης 12 : η κορυφή i αντιστοιχεί στο στοιχείο g^i.

Οι κορυφές 0, 3, 6, 9 αντιστοιχούν στην κλάση H.
Οι κορυφές 1, 4, 7, 10 αντιστοιχούν στην κλάση gH.
Οι κορυφές 2, 5, 8, 11 αντιστοιχούν στην κλάση g^2H.



(3) **Το διάγραμμα των υποομάδων της** S_3.

Το διάγραμμα υποομάδων πεπερασμένης ομάδας G ορίζεται ως εξής. Οι κορυφές του γραφήματος αντιστοιχούν στις υποομάδες της G. Δύο υποομάδες A, B της G συνδέονται με μία ακμή αν ισχύει $A \subset B$ ή $B \subset A$ και δεν υπάρχει υποομάδα C με $A \subset C \subset B$ ή $B \subset C \subset A$. Στην περίπτωση αυτή, η υποομάδα που αντιστοιχεί στο άνω άκρο της ακμής περιέχει την υποομάδα που αντιστοιχεί στο κάτω άκρο.

Στο παράδειγμα αυτό θα βρούμε το διάγραμμα υποομάδων της S_3.

Σύμφωνα με το θεώρημα του Lagrange, κάθε γνήσια υποομάδα H της S_3 έχει τάξη 1,2 ή 3. Άρα κάθε H είναι κυκλική (Πόρισμα 8.11). Επειδή

$$S_3 = \{1, (12), (13), (23), (123), (132)\},$$

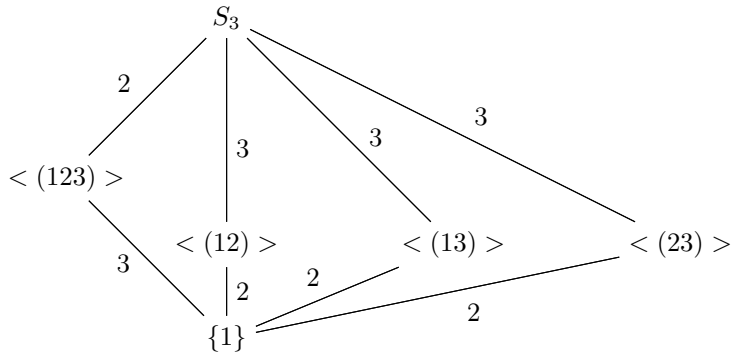
έχουμε ότι η H είναι μία από τις

$$\begin{aligned}
&< 1 >= \{1\},\\
&< (12) >= \{1, (12)\},\\
&< (13) >= \{1, (13)\},\\
&< (23) >= \{1, (23)\},\\
&< (123) >= \{1, (123), (123)^2\},\\
&< (132) >= \{1, (132), (132)^2\}.
\end{aligned}$$

Όμως $< (123) >=< (132) >$ και επομένως

$$H =< 1 >, < (12) >, < (13) >, < (23) >, < (123) > .$$

Το διάγραμμα την υποομάδων της S_3 είναι το ακόλουθο, όπου έχουμε σημειώσει στις ακμές τους αντίστοιχους δείκτες, για παράδειγμα $[S_3 :< (12) >] = \frac{6}{2} = 3$.



Διάγραμμα υποομάδων της S_3

8.4. Πολλαπλασιαστική ομάδα πεπερασμένου σώματος

Ξέρουμε ότι αν R είναι δακτύλιος με μονάδα, τότε το σύνολο των αντιστρέψιμων στοιχείων $U(R)$ του R είναι ομάδα ως προς τον περιορισμό του πολλαπλασιασμού του R. Θα καλούμε την ομάδα $U(R)$ την **πολλαπλασιαστική ομάδα** του R. Για παράδειγμα, όταν ο R είναι σώμα $R = k$, τότε $U(k) = k - \{0\}$. Θα συμβολίζουμε την πολλαπλασιαστική ομάδα σώματος k με k^*.

Θεώρημα 8.15. *Η πολλαπλασιαστική ομάδα πεπερασμένου σώματος είναι κυκλική.*

Απόδειξη. Έστω k πεπερασμένο σώμα και $G = k^*$ η πολλαπλασιαστική ομάδα του k. Θα δείξουμε ότι η G περιέχει στοιχείο τάξης n, όπου $n = |G|$. Θα χρησιμοποιήσουμε την εξής ταυτότητα για τη συνάρτηση φ του Euler,

$$n = \sum_{d|n} \varphi(d)$$

που είδαμε στην άσκηση 2.22.

Ξέρουμε ότι η τάξη κάθε στοιχείου της G διαιρεί το n. Για κάθε θετικό διαιρέτη d του n, έστω $N(d)$ το πλήθος των στοιχείων της G τάξης d. Είναι σαφές ότι

$$n = \sum_{d|n} N(d).$$

Θα δείξουμε ότι για κάθε d είναι $N(d) \leq \varphi(d)$. Τότε από τις παραπάνω ταυτότητες έπεται άμεσα ότι $N(d) = \varphi(d)$ και ειδικά $N(n) = \varphi(n) > 0$, που σημαίνει ότι η G διαθέτει στοιχείο τάξης n.

Έστω $a \in G$ τάξης d. Τα στοιχεία $1, a, ..., a^{d-1}$ είναι διακεκριμένα και ρίζες του πολυωνύμου $x^d - 1 \in k[x]$. Επειδή αυτό έχει συντελεστές από σώμα, σύμφωνα με την Πρόταση 4.21 τα παραπάνω στοιχεία είναι όλες οι ρίζες του στο K. Επομένως το $N(d)$ ισούται με το πλήθος των στοιχείων από τα $1, a, ..., a^{d-1}$ που έχουν τάξη d. Από το Θεώρημα 7.17(2) παίρνουμε $N(d) = \varphi(d)$. □

Παρατηρήσεις. 1) Η απόδειξη του προηγούμενου θεωρήματος είναι υποψήφια για μετάλλιο κομψότητας των αποδείξεων στις σημειώσεις αυτές.
2) Σύμφωνα με το προηγούμενο θεώρημα, η πολλαπλασιαστική ομάδα του $\mathbb{Z}_p$ είναι κυκλική για κάθε πρώτο p. Οι γνώστες της θεωρίας αριθμών θα αναγνωρίσουν το αποτέλεσμα αυτό ως την ύπαρξη πρωταρχικής ρίζας modulo p. Αξίζει να τονισθεί ότι δεν είναι γνωστή κάποια 'απλή μορφή' γεννήτορα. Η φημισμένη εικασία του Artin, που παραμένει μέχρι σήμερα ανοικτή, λέει μεταξύ των άλλων, ότι το [2] είναι γεννήτορας της $\mathbb{Z}_p^*$ για άπειρο το πλήθος πρώτων p.
3) Ένα θεώρημα του Gauss λέει ότι η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική αν και μόνο αν $n =$

$1, 2, 4, p^m, 2p^m$, όπου p περιττός πρώτος. Μια απόδειξη σκιαγραφούμε στις ασκήσεις του Κεφαλαίου 9.

8.5. Άρτιες και περιττές μεταθέσεις

Μια μετάθεση $\sigma \in S_n$ λέγεται **αντιμετάθεση** αν η σ είναι κύκλος μήκους 2. Συνεπώς κάθε αντιμετάθεση είναι της μορφής $\sigma = (i\ j)$, όπου $i \neq j$. Για παράδειγμα, οι αντιμεταθέσεις στη S_3 είναι οι $(12), (13), (23)$. Τα υπόλοιπα στοιχεία της S_3 μπορούν να γραφούν ως γινόμενα αντιμεταθέσεων,

$$1 = (12)(12),\ (123) = (13)(12),\ (132) = (12)(13).$$

Πρόταση 8.16. *Κάθε μετάθεση είναι γινόμενο αντιμεταθέσεων.*

Απόδειξη. Ξέρουμε ότι κάθε μετάθεση είναι γινόμενο κύκλων. Αρκεί να δείξουμε ότι κάθε κύκλος είναι γινόμενο αντιμεταθέσεων. Εύκολα επαληθεύεται ότι

$$(a_1\ a_2 \cdots a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2).$$

□

Ορισμός 8.17. *Έστω $\sigma \in S_n$. Η σ λέγεται*
(1) ***άρτια*** *αν είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων,*
(2) ***περιττή*** *αν είναι γινόμενο περιττού πλήθους αντιμεταθέσεων.*

Παραδείγματα 8.18.

(1) Η $\sigma = (123)$ είναι άρτια αφού $\sigma = (13)(12)$.

(2) Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 1 & 2 & 5 & 4 \end{pmatrix} \in S_7$. Βρίσκοντας κατά τα γνωστά την ανάλυση της σ σε γινόμενο ξένων κύκλων, έχουμε $\sigma = (174)(2365)$. Λόγω της σχέσης που είδαμε στην απόδειξη της Πρότασης 8.15 παίρνουμε,

$$\sigma = (14)(17)(25)(26)(23).$$

Άρα η σ είναι περιττή.

Παρατηρήσεις

(1) Από τον ορισμό έπεται ότι το γινόμενο δύο άρτιων μεταθέσεων είναι άρτια μετάθεση. Επίσης, το γινόμενο μια άρτιας και μιας περιττής (με οποιαδήποτε σειρά) είναι περιττή. Το γινόμενο δύο περιττών μεταθέσεων είναι άρτια.

(2) Αν έχουμε $\sigma = \sigma_1 ... \sigma_m$, με σ_i αντιμεταθέσεις, τότε

$$\sigma^{-1} = \sigma_m^{-1} ... \sigma_1^{-1} = \sigma_m ... \sigma_1$$

αφού κάθε αντιμετάθεση ικανοποιεί $\sigma_i^2 = 1$. Η παραπάνω σχέση λέει ότι η σ είναι άρτια (αντίστοιχα περιττή) αν και μόνο αν η σ^{-1} είναι άρτια (αντίστοιχα περιττή).

(3) Από τα παραπάνω έπεται ότι για κάθε ακέραιο m και για κάθε μετάθεση σ, η σ^{2m} είναι άρτια μετάθεση.

Μέχρι στιγμής είδαμε ότι κάθε μετάθεση είναι άρτια ή περιττή. Θα δούμε τώρα ότι δεν υπάρχει μετάθεση που να είναι και τα δύο. Θα δώσουμε δύο διαφορετικές αποδείξεις, η πρώτη με ορίζουσες η δεύτερη με δράση των μεταθέσεων στη διακρίνουσα.

Πρόταση 8.19. *Δεν υπάρχει $\sigma \in S_n$ που να είναι και άρτια και περιττή.*

Απόδειξη. *Πρώτη απόδειξη.* Έστω $\sigma = \sigma_1\sigma_2\cdots\sigma_s$, σ_i αντιμετάθεση για κάθε i και $\sigma = \tau_1\tau_2\cdots\tau_t$, τ_j αντιμετάθεση για κάθε j.

Θα δείξουμε ότι $s \equiv t \mod 2$. Αν $A \in M_n(\mathbb{R})$, με $\sigma(A)$ συμβολίζουμε τον πίνακα που έχει $\sigma(i)$- στήλη την i- στήλη του A.

Για παράδειγμα, αν $n = 3$, $A = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ και $\sigma = (1\ 2)$, τότε $\sigma(I_3) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ και αν $\sigma = (2\ 1\ 3)$ Τότε $\sigma(I_3) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Δηλαδή ο $\sigma(I_n)$ προκύπτει από τον I_n εναλλάσσοντας τις στήλες του I_n κατά την μετάθεση σ.

Είναι σαφές ότι $\sigma\tau(A) = \sigma(\tau(A))$ για κάθε $\sigma, \tau \in S_n$, $A \in M_n(\mathbb{R})$.

Από την Γραμμική Άλγεβρα θυμίζουμε ότι αν ο πίνακας B προκύπτει εναλλάσσοντας τις θέσεις δύο στηλών ενός πίνακα A, τότε $\det B = -\det A$. Άρα από τη σχέση $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ παίρνουμε

$$\det\sigma(I_n) = (-1)^s$$

και από $\sigma = \tau_1\tau_2\cdots\tau_t$ παίρνουμε

$$\det\sigma(I_n) = (-1)^t.$$

Επομένως $(-1)^s = (-1)^t \Rightarrow s \equiv t \mod 2$.

Δεύτερη απόδειξη. Θεωρούμε το πολυώνυμο

$$\Delta = \prod_{1\le i<j\le n} (x_j - x_i) \in \mathbb{Z}[x_1, ..., x_n].$$

Για παράδειγμα, αν $n = 3$, έχουμε $\Delta = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$.

Έστω $\sigma \in S_n$. Ορίζουμε πολυώνυμο

$$f_\sigma(\Delta) = \prod_{1\le i\ <j\le n} (x_{\sigma(j)} - x_{\sigma(i)}).$$

Παρατηρούμε ότι $f_\sigma(\Delta) = \Delta$ ή $f_\sigma(\Delta) = -\Delta$. Επίσης, αν σ, ρ είναι μεταθέσεις, τότε $f_\sigma \circ f_\rho = f_{\sigma\rho}$.

Έστω $\tau = (i\ j)$ με $i < j$. Εξετάζουμε το $f_\tau(\Delta)$ διακρίνοντας τις εξής περιπτώσεις για τους παράγοντες του Δ.

(1) Θεωρούμε $x_u - x_j$ με $i < u < j$.

(2) Θεωρούμε $x_i - x_v$ με $i < v < j$.

(3) Θεωρούμε $x_i - x_j$ με $i < v < j$.

Στην περίπτωση (1) αντιστοιχούν $j - i + 1$ παράγοντες $x_u - x_j$ που οι εικόνες τους $x_u - x_i$ στο $f_\tau(\Delta)$ συνεισφέρουν $j - i + 1$ αλλαγές προσήμου.
Στην περίπτωση (2) αντιστοιχούν $j - i + 1$ παράγοντες $x_i - x_v$ που οι εικόνες τους $x_j - x_v$ στο $f_\tau(\Delta)$ συνεισφέρουν $j - i + 1$ αλλαγές προσήμου.
Στην περίπτωση (3) αντιστοιχεί μοναδικός παράγοντας $x_i - x_j$ που η εικόνα του $x_j - x_j$ στο $f_\tau(\Delta)$ συνεισφέρει 1 αλλαγή προσήμου.
Συνολικά έχουμε $2(j - i + 1) + 1$ αλλαγές προσήμου που είναι περιττός αριθμός. Συνεπώς αποδείξαμε ότι για κάθε αντιμετάθεση τ είναι

$$f_\tau(\Delta) = -\Delta.$$

Τώρα ας υποθέσουμε ότι έχουμε δύο αναλύσεις της σ σε γινόμενο αντιμεταθέσεων,

$$\sigma = \tau_1\cdots\tau_r = \rho_1\cdots\rho_s.$$

Τότε από την πρώτη παίρνουμε

$$f_\sigma(\Delta) = f_{\tau_1\cdots\tau_r}(\Delta) = f_{\tau_1} \circ \cdots \circ f_{\tau_r}(\Delta) = (-1)^r\Delta$$

και όμοια από τη δεύτερη

$$f_\sigma(\Delta) = f_{\rho_1\cdots\rho_s}(\Delta) = f_{\rho_1}\circ\cdots\circ f_{\rho_s}(\Delta) = (-1)^s\Delta.$$

Άρα $(-1)^r\Delta = (-1)^s\Delta$, οπότε $r \equiv s \mod 2$. □

Ορισμός 8.20. $A_n = \{\sigma \in S_n : \sigma \text{ άρτια}\}$.

Για παράδειγμα η μετάθεση (123) της S_3 ανήκει στο A_3 αφού $(123) = (13)(12)$.

Θεώρημα 8.21. *Ισχύει $A_n \leq S_n$. Αν $n \geq 2$, τότε $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.*

Απόδειξη. Έστω $\sigma, \tau \in A_n$. Τότε $\sigma = \sigma_1\sigma_2\cdots\sigma_s$, s άρτιος και σ_i αντιμετάθεση για κάθε i. Όμοια $\tau = \tau_1\tau_2\cdots\tau_t$, t άρτιος τ_j αντιμετάθεση για κάθε j. Άρα

$$\sigma\tau = \sigma_1\sigma_2\cdots\sigma_s\tau_1\tau_2\cdots\tau_t \in A_n,$$

αφού $s+t$ άρτιος. Επίσης,

$$\sigma^{-1} = (\sigma_1\sigma_2\cdots\sigma_s)^{-1} = \sigma_s^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1} = \sigma_s\cdots\sigma_2\sigma_1 \in A_n,$$

αφού s άρτιος. Άρα $A_n \leq S_n$.

Θα δείξουμε τώρα ότι $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$. Έστω

$$B_n = \{\sigma \in S_n : \sigma \text{ περιττός}\}.$$

Από την Πρόταση 8.17 η ένωση $S_n = A_n \cup B_n$ είναι ξένη ένωση. Άρα $|S_n| = |A_n| + |B_n|$. Αρκεί να δείξουμε ότι $|A_n| = |B_n|$. Θεωρούμε την απεικόνιση

$$f : A_n \to B_n, \quad f(\sigma) = (12)\sigma.$$

Παρατηρούμε ότι αν $\sigma \in A_n$, τότε $(12)\sigma \in B_n$. Επίσης αν $f(\sigma) = f(\tau)$, τότε $(12)\sigma = (12)\tau \Rightarrow \sigma = \tau$, δηλαδή η f είναι 1-1. Έστω $\tau \in B_n$. Τότε $(12)\tau \in A_n$ και $f((12)\tau) = (12)(12)\tau = \tau$. Άρα η f είναι επί. Επομένως $|A_n| = |B_n|$. □

Σχόλια στην απόδειξη του θεωρήματος.

(1) Στη θέση του (12) στην απόδειξη θα μπορούσαμε να πάρουμε οποιαδήποτε περιττή μετάθεση.

(2) Από την απόδειξη έπεται ότι για κάθε $\sigma \in S_n$ περιττή μετάθεση έχουμε την ξένη ένωση αριστερών κλάσεων $S_n = A_n \cup \sigma A_n$.

Η υποομάδα A_n της S_n καλείται **η εναλλάσσουσα υποομάδα ή η υποομάδα των άρτιων μεταθέσεων**.

Παραδείγματα 8.22.

(1) Παρατηρούμε τα εξής.
   i) $A_1 = \{1\}$.
   ii) $A_2 = \{1\}$.
   iii) $A_3 = \{1, (123), (132)\}$.
   iv) Έχουμε $\sigma = (1234) \notin A_4$, αφού $\sigma = (14)(13)(12)$. Επίσης, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in A_4$, αφού $\tau = (14)(23)$.

(2) Αν $\sigma \in S_n$ έχει περιττή τάξη, τότε $\sigma \in A_n$.
Πράγματι, αρχικά παρατηρούμε ότι ότι κάθε κύκλος περιττού μήκους ανήκει στην A_n διότι

$$(a_1\ a_2\cdots a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_3)(a_1\ a_2).$$

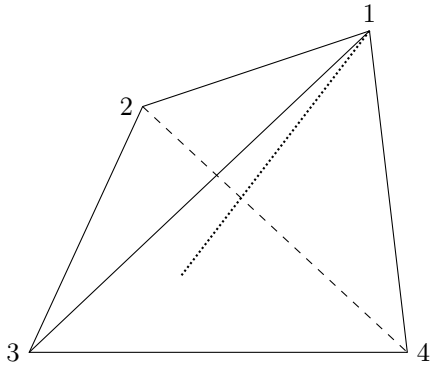
Αν τώρα $\sigma \in S_n$, έχουμε $\sigma = \sigma_1\cdots\sigma_k$, όπου σ_i κύκλος. Ξέρουμε ότι η τάξη του σ είναι το εκπ των μηκών $l(\sigma_i)$ των σ_i. Αν η τάξη της σ είναι περιττή, τότε παίρνουμε ότι κάθε $l(\sigma_i)$ είναι περιττός, δηλαδή $\sigma_i \in A_n$. Άρα $\sigma = \sigma_1\cdots\sigma_k \in A_n$.

Ας δούμε μια άλλη απόδειξη. Αν η σ έχει περιττή τάξη, τότε $\sigma^{2m+1} = 1$ για κάποιο m. Άρα $\sigma = \sigma^{2m+1}\sigma = \sigma^{2m+2}$ που είναι άρτια μετάθεση αφού ο ακέραιος $2m+2$ είναι άρτιος.

(3) **Ομάδα συμμετριών του τετραέδρου** Θα προσδιορίσουμε εδώ την ομάδα συμμετριών G του κανονικού τετραέδρου (οι έδρες είναι ισόπλευρα τρίγωνα) και την υποομάδα H των περιστροφικών συμμετριών. Ταυτίζοντας κάθε ισομετρία του τετραέδρου με την αντίστοιχη μετάθεση των κορυφών του 1,2,3,4, όπως εξηγήσαμε στο Παράδειγμα 8.5(6), έχουμε ότι $G \subseteq S_4$. Θα δείξουμε ότι

$$G = S_4 \text{ και } H = A_4.$$

Θα βρούμε αρχικά 12 διαφορετικές περιστροφικές συμμετρίες του τετραέδρου. Υπάρχουν οι περιστροφές κατά γωνίες $2\pi/3$ και $\pi/3$ γύρω από το ύψος που διέρχεται από την κορυφή 1, όπως δείχνει το σχήμα.

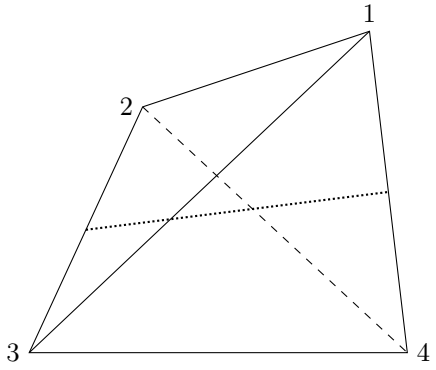


Έτσι έχουμε $(234), (243) \in H$. Θεωρώντας τα υπόλοιπα ύψη, παίρνουμε ότι

$$(ijk) \in H$$

για κάθε διακεκριμένα $i, j, k \in \{1, 2, 3, 4\}$. Το πλήθος των στοιχείων αυτών είναι 8. (Εδώ θα μπορούσαμε να συντομεύσουμε την αναζήτηση περιστροφικών συμμετριών, γιατί είναι γεγονός ότι κάθε στοιχείο της $A_n, n \geq 3$, είναι γινόμενο κύκλων μήκους 3. Επειδή η ομάδα G περιέχει τους κύκλους αυτούς, έπεται ότι $A_4 \subseteq H$. Θα αγνοήσουμε το γεγονός αυτό που αποδεικνύεται στην άσκηση 8.25 παρακάτω και θα βρούμε άλλες περιστροφικές συμμετρίες του τετραέδρου.)

Υπάρχουν και οι περιστροφές γύρω από τους άξονες που διέρχονται από τα μέσα απέναντι πλευρών, όπως δείχνει το σχήμα



Η περιστροφή κατά γωνία π δίνει ότι $(14)(23) \in H$. Θεωρώντας τους άλλους 2 άξονες έχουμε $(12)(34) \in H$ και $(13)(24) \in H$.

Τελικά, μαζί με την ταυτοτική απεικόνιση έχουμε βρει 8+3+1=12 διακεκριμένα στοιχεία της H. Εύκολα βλέπουμε ότι καθένα από τα 12 αυτά στοιχεία είναι άρτια μετάθεση.

Επειδή $|A_4| = 12$, έχουμε μέχρι στιγμής ότι

$$A_4 \subseteq H.$$

Για να δείξουμε την ισότητα $A_4 = H$, αρκεί να δείξουμε ότι υπάρχει συμμετρία του τετραέδρου που δεν είναι περιστροφική, γιατί τότε θα έχουμε $|H| = 12$ από το θεώρημα του Lagrange.

Το επίπεδο που περιέχει την πλευρά 34 και διέρχεται από το μέσο της πλευράς 12, τέμνει την πλευρά 12 κάθετα. Συνεπώς έχουμε την ανάκλαση $(12) \in G$. Άρα η G περιέχει τουλάχιστον 13 στοιχεία και επειδή είναι υποομάδα της S_4 που έχει 24 στοιχεία, συμπεραίνουμε από το θεώρημα του Lagrange ότι $G = S_4$.
Μένει να δειχθεί ότι η ανάκλαση (12) δεν είναι περιστροφή ως προς κάποιο άξονα. Αυτό είναι σαφές καθώς, αν η συμμετρία (12) ήταν περιστροφή, τότε από $(12)^2 = 1$ έπεται ότι θα ήταν στροφή κατά γωνία π. Τα σταθερά σημεία κάθε περιστροφής που είναι διάφορη της ταυτοτικής απεικόνισης, ανήκουν στον άξονα περιστροφής. Καθώς τα σημεία 3,4 είναι σταθερά κάτω από τη συμμετρία (12), θα έπρεπε ο άξονας να είναι η πλευρά 34. Αυτό είναι αδύνατο καθώς η κορυφή 2 δεν προκύπτει από την κορυφή 1 με περιστροφή κατά γωνία π με άξονα την ευθεία 34.

8.6. Παραγόμενες υποομάδες

Θα δούμε εδώ έναν πολύ χρήσιμο τρόπο να βρίσκουμε υποομάδες μιας ομάδας. Έστω G ομάδα και X μη κενό υποσύνολο της G. Θέτουμε $X^{-1} = \{x^{-1} \in G : x \in G\}$.

Ορισμός 8.23. *Η υποομάδα της G που* **παράγεται** *από το X είναι*

$$< X >= \{y_1 y_2 \cdots y_m \in G : m \geq 1, y_i \in X \cup X^{-1}.\}$$

Δηλαδή κάθε στοιχείο του συνόλου $< X >$ είναι ένα γινόμενο, με οποιοδήποτε πεπερασμένο πλήθος παραγόντων, στοιχείων από το σύνολο $X \cup X^{-1}$. Για παράδειγμα, αν $x_1, x_2 \in X$, τότε $x_1^2 x_2^{-3} x_1^{-5} x_2 \in < X >$. Χρησιμοποιώντας την Πρόταση 8.4 εύκολα επαληθεύεται ότι το $< X >$ είναι πράγματι υποομάδα της G (άσκηση).

Στην ειδική περίπτωση που το X έχει ένα στοιχείο $X = \{g\}$, τότε το $< X >$ είναι η κυκλική υποομάδα $< g >$. Αν το $X = \{x_1, ..., x_m\}$ είναι πεπερασμένο σύνολο, μπορούμε να χρησιμοποιούμε το συμβολισμό $< x_1, ..., x_m >=< X >$ και θα λέμε ότι τα $x_1, ..., x_m$ **παράγουν** την ομάδα $< X >$.

Πρόταση 8.24. *Έστω G ομάδα και $X \subseteq G, X \neq \emptyset$. Τότε*

$$< X >= \bigcap_{X \subseteq H \leq G} H$$

όπου το H διατρέχει τις υποομάδες της G που περιέχουν το X.

Απόδειξη. Για κάθε H στο δεξί μέλος έχουμε $X \subseteq H$ και άρα $< X > \subseteq H$, γιατί το H είναι ομάδα. Άρα $< X >$ περιέχεται στο δεξί μέλος.

Αντίστροφα, ένα από τα H στο δεξί μέλος είναι το $< X >$. Άρα το δεξί μέλος περιέχεται στο $< X >$. □

Σύμφωνα με την προηγούμενη Πρόταση, το $< X >$ είναι η μικρότερη υποομάδα της G που περιέχει το σύνολο X. Καλό είναι τα παραπάνω να συγκριθούν με το ιδεώδες που παράγεται από σύνολο, βλ. Παράγραφο 5.4, καθώς η βασική ιδέα είναι όμοια.

Παραδείγματα 8.25.

(1) Έστω G ομάδα και $H \leq G$. Αν $X = H$, τότε $< X >= H$.

(2) Έστω $G = S_n$ και X το σύνολο των αντιμεταθέσεων της S_n. Η Πρόταση 8.15 λέει ότι $< X >= S_n$.

(3) Έστω $G = S_n$ και X το σύνολο των γινομένων $\sigma\tau$, όπου σ, τ αντιμεταθέσεις της S_n. Τότε $< X >= A_n$ σύμφωνα με τον Ορισμό 8.18.

(4) Έστω $G = S_3$ και $X = \{(12), (13)\}$. Τότε $S_3 =< (12), (13) >$ καθώς

$$\begin{aligned} (23) &= (13)(12)(13), \\ (123) &= (13)(12), \\ (132) &= (12)(13). \end{aligned}$$

Γενικά ισχύει ότι $S_n =< (12), (13), ..., (1n) >$.

Πράγματι, ξέρουμε ότι κάθε στοιχείο της S_n είναι γινόμενο αντιμεταθέσεων (ij). Από την ακόλουθη σχέση

$$(ij) = (1i)(1j)(1i), \;\; 1 < i < j$$

που εύκολα επαληθεύεται με άμεσο υπολογισμό, έπεται ότι κάθε στοιχείο της S_n είναι γινόμενο αντιμεταθέσεων της μορφής $(1j)$. Συνεπώς

$$S_n \subseteq < (12), (13), ..., (1n) > .$$

Η άλλη σχέση περιέχεσθαι είναι προφανής και άρα έχουμε ισότητα.

(5) Έστω $G = D_n$ η διεδρική ομάδα. Με το συμβολισμό του Παραδείγματος 7.4(10) είχαμε ότι $D_n = \{1, r, ..., r^{n-1}, s, sr, ..., sr^{n-1}\}$. Άρα $D_n =< r, s >$

Ασκήσεις Κεφαλαίου 8

Ομάδα1: 1, 3-6, 18.
Ομάδα2: 7-17, 19-24, 26-32, 35.
Ομάδα3: 2, 25,33, 34, 36.

1. ⋆ Έστω G ομάδα και $H \leq G,\ K \leq G$. Αν $|H| = m,\ |K| = n,\ \mu\kappa\delta(m,n) = 1$, τότε $H \cap K = \{1\}$.
2. ⋆ ≀ Έστω G ομάδα και $a, b \in G$ τέτοια ώστε $ab = ba$. Αν $|a| = m < \infty, |b| = n < \infty$, τότε η G περιέχει στοιχείο τάξης $\varepsilon\kappa\pi(m,n)$.
3. Έστω G πεπερασμένη ομάδα και $H \leq G,\ K \leq G$. Δείξτε τα εξής.
   i) Αν $H \subseteq K$, τότε $[G : H] = [G : K][K : H]$. (Βλ. άσκηση 8.33 για γενίκευση).
   ii) Κάθε υποομάδα της S_n περιττού δείκτη, περιέχει περιττή μετάθεση.
   iii) $[G : H \cap K] \leq [G : H][G : K]$.
4. Έστω G ομάδα τάξης pq, όπου p, q πρώτοι. Δείξτε ότι κάθε γνήσια υποομάδα της G είναι κυκλική.
5. Έστω G ομάδα τάξης 105.
   i) Δείξτε ότι αν $H \leq G$ και $|H| > 35$, τότε $H = G$.
   ii) Δείξτε ότι αν $g \in G$ και $g^{39} = 1$, τότε $g^3 = 1$
6. Δείξτε ότι κάθε ομάδα τάξης p^n, όπου p πρώτος, έχει υποομάδα τάξης p.
7. Δείξτε ότι το αντίστροφο του θεωρήματος του Lagrange αληθεύει για την ομάδα S_4.
8. Έστω G πεπερασμένη ομάδα και p πρώτος.
   i) Έστω $a, b \in G$ με $|a| = |b| = p$. Τότε
   $$< a > \cap < b >= \{1\} \quad \text{ή} \quad < a >=< b > .$$
   ii) Το πλήθος των στοιχείων της G τάξης p είναι πολλαπλάσιο του $p - 1$.
   iii) Αν $|G| = 33$, τότε η G έχει στοιχείο τάξης 3 .
9. Έστω G ομάδα τάξης $2m$.
   i) Δείξτε ότι η G έχει στοιχείο τάξης 2.
   ii) Δείξτε ότι το πλήθος των στοιχείων της G τάξης 2 είναι περιττός.
   iii) Δείξτε ότι αν το m είναι περιττός και η G αβελιανή, τότε υπάρχει μοναδικό στοιχείο τάξης 2.
10. Έστω G ομάδα και $H \leq G$ με $[G : H] = n < \infty$. Δείξτε ότι για κάθε $g \in G$ υπάρχει $m \in \mathbb{Z},\ 1 \leq m \leq n$ ώστε $g^m \in H$.
11. i) Δείξτε ότι η $U(\mathbb{Z}_{18})$ είναι κυκλική και η $U(\mathbb{Z}_{20})$ δεν είναι κυκλική.
    ii) Αν G είναι πεπερασμένη κυκλική ομάδα τάξης n, δείξτε ότι το πλήθος των γεννητόρων της G ισούται με $\varphi(n)$. Χρησιμοποιώντας το αποτέλεσμα αυτό, δείξτε ότι για κάθε $m \geq 2$ η ομάδα $U(\mathbb{Z}_{4m})$ δεν είναι κυκλική.
12. Έστω G πεπερασμένη ομάδα τάξης n. Δείξτε ότι αν m, n είναι σχετικά πρώτοι ακέραιοι, τότε για κάθε $y \in G$ υπάρχει $x \in G$ με $x^m = y$.
13. Δείξτε ότι κάθε πεπερασμένη υποομάδα της $\mathbb{C} - \{0\}$ είναι της μορφής E_n για κάποιο n. Ποιες είναι οι πεπερασμένες υποομάδες της $\mathbb{R} - \{0\}$;
14. Έστω G αβελιανή ομάδα τάξης 2^n. Δείξτε ότι το πλήθος των στοιχείων της G τάξης 2 είναι $2^m - 1$ για κάποιο m.
15. 'Εστω G πεπερασμένη ομάδα και d θετικός ακέραιος. Δείξτε ότι το πλήθος των στοιχείων της G που έχουν τάξη d είναι πολλαπλάσιο του $\varphi(d)$ (συμπεριλαμβανομένου και του μηδενικού).
16. Έστω $G \leq S_n$. Δείξτε ότι αν η G περιέχει περιττή μετάθεση, τότε η τάξη της G είναι άρτιος ακέραιος και ακριβώς τα μισά στοιχεία της G είναι περιττές μεταθέσεις.

17. Βρείτε (αν υπάρχουν) όλα τα $\sigma \in S_8$ με $\sigma^2 = (12345678)$.
18. Έστω $\sigma \in S_n,\ \sigma = \sigma_1\sigma_2\cdots\sigma_m,\ \sigma_i$ κύκλος μήκους k_i για κάθε i και $t = \sum_{i=1}^{m}(k_i - 1)$. Τότε σ άρτια $\Leftrightarrow t$ άρτιος και σ περιττή $\Leftrightarrow t$ περιττός.
19. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7$.
    i) Εξετάστε αν η σ είναι περιττή.
    ii) Να βρεθούν όλοι οι $m \in \mathbb{Z}$ ώστε $< \sigma^m > \leq A_7$.
    iii) Αληθεύει ότι υπάρχει $\tau \in S_7$ με $\tau^{2020} = \sigma$;
    iv) Αληθεύει ότι $(13) \in < \sigma >$;
20. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & a & 1 & b & 6 & 7 & 3 \end{pmatrix} \in S_7$.
    i) Βρείτε τα a, b ώστε η σ να είναι άρτια.
    ii) Αν η σ είναι άρτια, αληθεύει ότι $(15)(56)(67) \in < \sigma >$;
21. Έστω $\sigma = (2345)(45167) \in S_7$.
    i) Βρείτε την τάξη της σ και εξετάστε αν η σ είναι άρτια.
    ii) Βρείτε την τάξη της ομάδας $< \sigma^{50} > \cap < \sigma^{33} >$.
    iii) Αληθεύει ότι η σ είναι γινόμενο δύο μεταθέσεων της S_7 που έχουν περιττές τάξεις;
    iv) Αληθεύει ότι υπάρχει $\tau \in S_7$ με $\tau\sigma\tau^{-1} = \sigma^2$;
22. Για ποια n η ομάδα A_n περιέχει κυκλική ομάδα τάξης 4;
23. Βρείτε, αν υπάρχουν, τα στοιχεία τάξης 6 στην A_6.
24. Στο Παράδειγμα 8.5(4) ορίσαμε το κέντρο $Z(G)$ ομάδας G. Δείξτε τα εξής.
    i) Η G είναι αβελιανή αν και μόνο αν $Z(G) = G$.
    ii) Για κάθε $n \geq 3$ είναι $Z(S_n) = \{1\}$.
    iii) $Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{R}) : a \in \mathbb{R}, a \neq 0 \right\}$.
25. $\star$ Έστω $n \geq 3$. Δείξτε ότι κάθε στοιχείο της A_n είναι γινόμενο κύκλων μήκους 3.
26. Για ποια n η ομάδα A_n είναι αβελιανή;
27. Έστω G αβελιανή υποομάδα που διαθέτει κυκλικές υποομάδες τάξης 4 και 6. Δείξτε ότι η G διαθέτει κυκλικές υποομάδες με τάξεις 2, 3, 4, 6, 12.
28. Πόσες υποομάδες τάξης 5 έχει μια ομάδα τάξης 25;
29. Έστω G ομάδα τέτοια ώστε $a^2b^2 = b^2a^2$ για κάθε $a, b \in G$. Δείξτε ότι τα στοιχεία της G που έχουν περιττή τάξη αποτελούν αβελιανή υποομάδα της G.
30. Μια ομάδα G είναι πεπερασμένη αν το πλήθος των υποομάδων της G είναι πεπερασμένο.
31. Δείξτε ότι $S_n = < (12), (23), (34), ..., (n-1n) >$
32. Έστω μη κενό $X \subseteq \{1, ..., n\}$. Μια υποομάδα H της S_n λέγεται **μεταβατική** επί του X αν για κάθε $i, j \in X$ υπάρχει $\sigma \in H$ με $\sigma(i) = j$. Δείξτε ότι για κάθε μη κενό $X \subseteq \{1, ..., n\}$ υπάρχει μεταβατική υποομάδα επί του X με $|H| = |X|$.
33. Γενικεύουμε εδώ την άσκηση 8.3i). Έστω G ομάδα (όχι αναγκαστικά πεπερασμένη) και $H \leq K \leq G$. Δείξτε ότι αν $[G : K], [K : H] < \infty$ τότε $[G : H] = [G : K][K : H]$.
34. Έστω F πεπερασμένο σώμα με $|F| = 2^n$, n περιττός. Δείξτε ότι αν
$$a^2 + ab + b^2 = 1,$$
όπου $a, b \in F$, τότε $a = b = 0$.
35. Έστω G ομάδα και $H, K \leq G$. Δείξτε ότι $H \cup K \leq G$ αν και μόνο αν $H \subseteq K$ ή $K \subseteq H$. Στη συνέχεια δείξτε ότι η G δεν είναι ένωση δύο γνήσιων υποομάδων της.
36. $\wr$ Έστω G πεπερασμένη ομάδα της οποίας η τάξη δεν είναι πολλαπλάσιο του 3. Δείξτε ότι αν $(ab)^3 = a^3b^3$ για κάθε $a, b \in G$, τότε η G είναι αβελιανή.

Υποδείξεις Ασκήσεων Κεφαλαίου 8

1. *Λύση.* Από το θεώρημα Lagrange έχουμε $|H \cap K| \mid m$ και $|H \cap K| \mid n$. Άρα
$$|H \cap K| \mid \mu\kappa\delta(m,n) \Rightarrow |H \cap K| = 1 \Rightarrow H \cap K = \{1\}.$$

2. *Λύση.* Πρώτα θεωρούμε την περίπτωση που οι m, n είναι σχετικά πρώτοι. Θα δείξουμε στην περίπτωση αυτή ότι το ab έχει τάξη mn. Για το σκοπό αυτό έστω $s = |ab|$. Παρατηρούμε ότι επειδή $ab = ba$, είναι
$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1 \cdot 1 = 1 \Rightarrow s|mn.$$
Επίσης,
$$1 = (ab)^s = a^s b^s \Rightarrow a^s = b^{-s} \in < a > \cap < b > \Rightarrow |a^s||m \text{ και } |a^s||n,$$
οπότε $|a^s| = 1$ γιατί οι m, n είναι σχετικά πρώτοι. Άρα $a^s = 1 \Rightarrow m|s$. Όμοια αποδεικνύεται ότι $n|s$ και συνεπώς $mn|s$ καθώς οι m, n είναι σχετικά πρώτοι. Άρα $s = mn$.

Στη συνέχεια θεωρούμε τη γενική περίπτωση. Για το $e = \varepsilon\kappa\pi(m,n)$ μπορούμε να γράψουμε $e = e_1e_2...e_t$, όπου οι ακέραιοι e_i είναι ανά δύο σχετικά πρώτοι και επιπλέον για κάθε i ισχύει $e_i|m$ ή $e_i|n$. Τότε για κάθε i το στοιχείο $a^{\frac{m}{e_i}}$ ή το $b^{\frac{n}{e_i}}$ έχει τάξη e_i. Επιλέγοντας ένα τέτοιο στοιχείο για κάθε i και σχηματίζοντας το γινόμενό τους, προκύπτει στοιχείο τάξης $e_1e_2...e_t$ σύμφωνα με το πρώτο μέρος της απόδειξης.

3. *Λύση.* i) Αφού $H \leq G$, $H \subseteq K$ και $K \leq G$ έπεται $H \leq K$. Από το θεώρημα του Lagrange έχουμε $[G:H] = \frac{|G|}{|H|}$, $[G:K] = \frac{|G|}{|K|}$ και $[K:H] = \frac{|K|}{|H|}$. Παρατηρούμε ότι
$$[G:K] = \frac{|G|}{|K|} = \frac{\frac{|G|}{|H|}}{\frac{|K|}{|H|}} = \frac{[G:H]}{[K:H]}.$$
Επομένως $[G:H] = [G:K][K:H]$.
ii)
iii) Από το ερώτημα i) έχουμε, $[G : H \cap K] = [G:H][H : H \cap K]$. Επομένως αρκεί να δείξουμε ότι $[H : H \cap K] \leq [G:K]$. Ορίζουμε την απεικόνιση
$$\varphi : \{h(H \cap K) : h \in H\} \to \{gK : g \in G\}, \ \ \varphi\left(h(H \cap K)\right) = hK.$$
Θα δείξουμε ότι η φ είναι καλώς ορισμένη και 1-1.

Πράγματι, έστω $h_1(H \cap K) = h_2(H \cap K)$. Τότε $h_2^{-1}h_1 \in H \cap K$. Άρα
$$h_2^{-1}h_1 \in K \Rightarrow h_1K = h_2K.$$
Άρα η φ είναι καλώς ορισμένη.

Έστω $h_1K = h_2K$ $(h_i \in H)$. Τότε $h_2^{-1}h_1 \in K$. Αλλά $h_2^{-1}h_1 \in H$, άρα $h_2^{-1}h_1 \in H \cap K$. Συνεπώς $h_1(H \cap K) = h_2(H \cap K)$. Άρα η φ είναι και 1-1.

4. *Λύση.* Από το θεώρημα του Lagrange, κάθε γνήσια υποομάδα της G θα έχει τάξη 1, p ή q. Η τετριμμένη υποομάδα είναι προφανώς κυκλική. Στις άλλες δύο περιπτώσεις η υποομάδα είναι κυκλική από το Πόρισμα 8.10.

5. *Λύση.* i) Από το θεώρημα του Lagrange $|H|||G|$. Αλλά ο μοναδικός διαιρέτης του 105 που είναι μεγαλύτερος του 35 είναι το 105. Άρα $|H| = |G|$ και επειδή $H \subseteq G$ με G πεπερασμένο, παίρνουμε $H = G$.
ii) Από την Πρόταση 8.11(2) έχουμε $g^{105} = 1$ και από την υπόθεση, $g^{39} = 1$. Καθώς ο μκδ των 105 και 39 είναι 3, υπάρχουν $x, y \in \mathbb{Z}$ με $3 = 105x + 39y$. Άρα $g^3 = (g^{105})^x(g^{39})^y = 1$.

6. *Λύση.* Έστω $g \in G, a \neq 1$. Τότε από την Πρόταση 8.11(2) έπεται ότι $|g| = p^i$ για κάποιο $i > 0$. Από το Θεώρημα 7.15(2) έχουμε ότι $|h| = p$, όπου $h = g^{p^{i-1}}$. Άρα η κυκλική υποομάδα $< h >$ έχει τάξη p.

7. *Λύση.* Σύμφωνα με τον ακόλουθο κατάλογο, για κάθε διαιρέτη d της τάξης $|S_4| = 24$ υπάρχει υποομάδα H της S_4 τάξης d.
   i) $d = 1, H =< 1 >$.
   ii) $d = 2, H =< (12) >$.
   iii) $d = 3, H =< (123) >$.
   iv) $d = 4, H =< (1234) >$.
   v) $d = 6, H = \{\sigma \in S_4 : \sigma(4) = 4\}$.
   vi) $d = 8, H = \{1, (12)(34), (14)(23), (24), (13), (1234), (13)(14), (1432)\}$. Βλ. Παράδειγμα 8.5(6).
   vii) $d = 12, H = A_4$.
   viii) $d = 24, H = S_4$.

8. *Λύση.* i) Επειδή $< a > \cap < b > \leq < a >$ και $| < a > | = p$, από το θεώρημα του Lagrange παίρνουμε,
$$| < a > \cap < b > | = 1 \text{ ή } p.$$
Αν $| < a > \cap < b > | = 1$, τότε $< a > \cap < b >= \{1\}$. Έστω $| < a > \cap < b > | = p$. Τότε $< a > \cap < b > \leq < a >$ και $| < a > \cap < b > | = | < a > |$. Άρα $< a > \cap < b >=< a >$, οπότε $< a > \subseteq < b >$. Άρα $< a >=< b >$.

   ii) Παρατηρούμε ότι αν $a \in G$ έχει τάξη p τότε κάθε στοιχείο $\neq 1$ της $< a >$ έχει τάξη p σύμφωνα με την Πρόταση 8.11(2). Έστω $G_p = \{g \in G : |g| = p\}$. Τότε από αυτό που παρατηρήσαμε παραπάνω έπεται ότι
$$G_p = \bigcup_{a \in G_p} (< a > -\{1\}).$$
Από το πρώτο ερώτημα έπεται η ύπαρξη ξένης ένωσης
$$G_p = \bigcup_{a \in A} (< a > -\{1\}),$$
όπου $A \subseteq G_p$. Επειδή το σύνολο $< a > -\{1\}$ έχει $p - 1$ στοιχεία, συνάγουμε ότι το πλήθος των στοιχείων του G_p είναι πολλαπλάσιο του $p - 1$.

   iii) Έστω $g \in G,\ g \neq 1$. Τότε $|g| \mid 33$, δηλαδή $|g| = 33, 11, 3$.

   Έστω ότι υπάρχει $g \in G$, με $|g| = 33$. Τότε το στοιχείο $h = g^{11}$ έχει τάξη $\frac{33}{\mu\kappa\delta(33,11)} = 3$.

   Έστω ότι κάθε $g \in G, g \neq 1$ έχει τάξη 11. Τότε από το δεύτερο ερώτημα, το πλήθος $|G \setminus \{1\}| =$ είναι πολλαπλάσιο του 10, άτοπο.

9. *Λύση* (1) και (2). Παρατήρηση.
   i) Αν $a, b \in G$ τότε $a = b \Leftrightarrow\ a^{-1} = b^{-1}$.
   ii) Αν $a \in G$ τότε $|a| = |a^{-1}|$.
   iii) Αν $a \in G$ τότε $a \neq a^{-1} \Leftrightarrow\ |a| > 2$.

   Έστω $A = \{g \in G : |g| > 2\}$. Από την παρατήρηση ii) $g \in A \Leftrightarrow\ g^{-1} \in A$. Από τις παρατηρήσεις i) και iii) έπεται ότι το A είναι ξένη ένωση συνόλων της μορφής $\{a, a^{-1}\}$ και άρα $|A| =$ άρτιος. Όμως το υποσύνολο B των στοιχείων τάξης 2 είναι το
$$B = \{g \in G : |g| = 2\} = G \setminus A \setminus \{1\}.$$
Άρα $|B| =$ περιττός.

   iii) Έστω ότι υπάρχουν $a, b \in G,\ a \neq b$ και $|a| = |b| = 2$. Θεωρούμε το σύνολο
$$H = \{1, a, b, ab\}.$$
Παρατηρούμε ότι $|H| = 4$ (για παράδειγμα αν $ab = a \Rightarrow b = 1$). Χρησιμοποιώντας το γεγονός ότι η G είναι αβελιανή, εύκολα επαληθεύεται ότι το πεπερασμένο σύνολο H είναι κλειστό στο G και άρα $H \leq G$. Από το θεώρημα του Lagrange έπεται ότι $4|2m$, άτοπο αφού ο m είναι περιττός.

Σημείωση. Στο ερώτημα (3) της άσκησης, αν η G δεν είναι αβελιανή η H δεν είναι αναγκαστικά υποομάδα της G. Για παράδειγμα, τα στοιχεία τάξης 2 της S_3 είναι $(12), (13), (23)$ και το σύνολο $\{1, (12), (13), (23)\}$ δεν είναι υποομάδα της S_3 (γιατί;).

10. *Λύση.* Επειδή το σύνολο $\{aH : a \in G\}$ έχει $[G : H] = n < \infty$ στοιχεία, ανάμεσα στα $H, gH, g^2H, \cdots, g^nH$ υπάρχουν δύο που είναι ίσα. Άρα $g^iH = g^jH$ για κάποια $0 \leq i,\ j \leq n,\ i > j$. Άρα $g^{i-j} \in H$ και $1 \leq i - j \leq n$.

11. *Λύση.* Έστω $G =< a >$ κυκλική ομάδα τάξης $n < \infty$. Ξέρουμε ότι $G = \{1, g, ..., g^{n-1}\}$. Το g^m είναι γεννήτορας της G αν και μόνο αν η τάξη του είναι n. Σύμφωνα με το Θεώρημα 7.17(2), αυτό ισοδυναμεί με $\frac{n}{\mu\kappa\delta(m,n)} = n \Leftrightarrow \mu\kappa\delta(m, n) = 1$. Το πλήθος των ακεραίων m με $1 \leq m \leq n - 1$ και $\mu\kappa\delta(m, n) = 1$ είναι η τιμή $\varphi(n)$ της συνάρτησης του Euler.
Θα δείξουμε ότι η $U(\mathbb{Z}_{4m})$, όπου m περιττός, έχει τουλάχιστον δύο στοιχεία τάξης 2. Επειδή $\varphi(2) = 1 \neq 2$, το προηγούμενο υποερώτημα δίνει το ζητούμενο. Από το Παράδειγμα 8.2(2), $U(\mathbb{Z}_{4m}) \simeq U(\mathbb{Z}_4) \times U(\mathbb{Z}_m)$. Παρατηρούμε ότι τα στοιχεία

$$([3]_4, [1]_m), ([3]_4, [-1]_m) \in U(\mathbb{Z}_4) \times U(\mathbb{Z}_m)$$

είναι διακεκριμένα (αφού m περιττός) και έχουν τάξη 2.

12. *Λύση.* Το ζητούμενο ισοδυναμεί με το να είναι επί η απεικόνιση $f : G \to G, a \mapsto a^m$. Επειδή $n < \infty$, αυτό ισοδυναμεί με το να είναι η f 1-1 . Έστω $a^m = b^m$ όπου $a, b \in G$. Ξέρουμε ότι $a^n = 1 = b^n$ καθώς $n = |G|$. Επειδή οι m, n είναι σχετικά πρώτοι, υπάρχουν $x, y \in \mathbb{Z}$ με $1 = mx + ny$. Έχουμε

$$a = a^1 = (a^m)^x(a^n)^y = (b^m)^x(b^n)^y = b^1 = b.$$

13. *Λύση.* Έστω G όπως στην εκφώνηση και $g \in G$. Τότε από την Πρόταση 8.11 έχουμε $g^n = 1$. Άρα $G \subseteq E_n$. Επειδή τα δύο σύνολα έχουν το αυτό πεπερασμένο πλήθος στοιχείων, συμπεραίνουμε ότι $G = E_n$.
Αν τώρα G είναι υποομάδα της $\mathbb{R} - \{0\}$ με τάξη n και $g \in G$, τότε όπως πριν έχουμε $g^n = 1$. Αλλά επειδή $g \in \mathbb{R}$, παίρνουμε $g = 1$ ή $g = -1$. Τελικά $G = \{1\} = E_1$ ή $G = \{1, -1\} = E_2$.

14. *Υπόδειξη.* Δείξτε ότι το σύνολο $G_2 = \{x \in G : x^2 = 1\}$ είναι υποομάδα της G και εφαρμόστε το θεώρημα του Lagrange.

15. *Υπόδειξη.* Κάθε στοιχείο της G τάξης d ανήκει σε κυκλική υποομάδα τάξης d. Έστω ότι $H_1, ..., H_m$ είναι οι διακεκριμένες κυκλικές υποομάδες της G τάξης d. Η καθεμιά έχει $\varphi(d)$ στοιχεία τάξης d. Δείξτε ότι για κάθε $i \neq j$, η τομή $H_i \cap H_j$ δεν περιέχει στοιχείο τάξης d. Από αυτό έπεται ότι το πλήθος των στοιχείων της G τάξης d ισούται με $m\varphi(d)$.

16. *Λύση.* Έστω $G \leq S_n$, $g \in G$ περιττή μετάθεση και $H = A_n \cap G$. Η απεικόνιση $f : H \to gH, h \mapsto gh$ είναι 1-1 γιατί αν $gh = gh'$, τότε $g^{-1}gh = g^{-1}gh'$, δηλαδή $h = h'$. Παρατηρούμε ότι το σύνολο H είναι το σύνολο των άρτιων μεταθέσεων της G. Επίσης, το σύνολο gH είναι το σύνολο των περιττών μεταθέσεων της G καθώς:
• Αν $h \in H$, τότε η h είναι άρτια μετάθεση στη G και άρα το γινόμενο gh είναι περιττή μετάθεση στη G.
• Αν x είναι περιττή μετάθεση στη G, τότε γράφοντας $x = g(g^{-1}x)$ έχουμε ότι η μετάθεση $g^{-1}x$ είναι άρτια (ως γινόμενο δύο περιττών) μετάθεση στη G και συνεπώς $x \in gH$.
Το ότι η f είναι 1-1 λέει ότι $|H| = |gH|$, δηλαδή ότι το πλήθος των άρτιων μεταθέσεων στη G ισούται με το πλήθος των περιττών μεταθέσεων στη G. Επειδή καμιά μετάθεση δεν μπορεί να είναι και άρτια και περιττή (Πρόταση 8.17), έχουμε ότι ακριβώς οι μισές από τις μεταθέσεις της G είναι περιττές.

17. *Λύση.* Δεν υπάρχει καθώς η μετάθεση σ^2 είναι άρτια για κάθε σ, ενώ η (12345678) είναι περιττή ως κύκλος με άρτιο μήκος.

18. *Λύση.* Είδαμε ότι $(a_1\ a_2 \cdots a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_3)(a_1\ a_2)$. Δηλαδή κάθε k- κύκλος είναι γινόμενο $(k - 1)$ αντιμεταθέσεων. Άρα αν σ όπως στην εκφώνηση, τότε $\sigma =$ γινόμενο αντιμεταθέσεων πλήθους $\sum_{i=1}^{m}(k_i - 1)$.

19. *Λύση.* i) Έχουμε $\sigma = (1427)(356)$. Άρα $\sigma = (17)(12)(14)(36)(35)$ περιττή, αφού έχουμε γινόμενο 5 αντιμεταθέσεων και ο 5 είναι περιττός.
ii) Παρατηρούμε ότι $< \sigma^m > \leq A_7 \Leftrightarrow < \sigma^m > \subseteq A_7 \Leftrightarrow \sigma^m \in A_7$. Επίσης,

$$\sigma^m \in A_7 \Leftrightarrow \sigma^m \text{ άρτια} \Leftrightarrow 5m \text{ άρτιος},$$

γιατί είδαμε πριν ότι $\sigma =$ γινόμενο $5m$ αντιμεταθέσεων. Άρα

$$< \sigma^m > \leq A_7 \Leftrightarrow m \text{ άρτιος.}$$

iii) Όχι. Στην ισότητα $\tau^{2020} = \sigma$, το αριστερό μέλος είναι άρτια μετάθεση επειδή ο 2020 είναι άρτιος, ενώ στο δεξί μέλος έχουμε περιττή μετάθεση. Αυτό είναι αδύνατο, λόγω της Πρότασης 8.17.

iv) Επειδή στο δεξί μέλος της $\sigma = (1427)(356)$ έχουμε ξένους κύκλους, αυτοί αντιμετατίθενται και επομένως για κάθε θετικό ακέραιο m, $\sigma^m = (1427)^m(356)^m$. Επειδή οι μεταθέσεις $(1427)^m, (356)^m$ παραμένουν ξένες, έχουμε ότι για κάθε m,

$$\sigma^m(1) \in \{1, 4, 2, 7\},$$

οπότε $\sigma^m(1) \neq 3$. Άρα δεν αληθεύει ότι $(13) \in < \sigma >$.

20. *Λύση.* i) Για το ζεύγος (a, b) έχουμε $(a, b) = (2, 4)$ ή $(a, b) = (4, 2)$.

Έστω $(a, b) = (2, 4)$. Τότε η ανάλυση της σ (μετά από λίγες στάνταρ πράξεις) είναι $\sigma = (15673)$. Έστω $(a, b) = (4, 2)$. Τότε $\sigma = (15673)(24)$. Παρατηρούμε ότι

$$(15673) = (13)(17)(16)(15) \in A_7, \text{ και}$$

$$(15673)(24) = (13)(17)(16)(15)(24) \notin A_7.$$

Άρα $a = 2,\ b = 4$.

ii) Επειδή $\sigma \in A_7$, έχουμε $< \sigma > \leq A_7$. Αλλά $(15)(56)(67)$ περιττή, δηλαδή $(15)(56)(67) \notin A_7$. Άρα δεν αληθεύει ότι $(15)(56)(67) \in < \sigma >$.

21. *Λύση.* Κατά τα γνωστά βρίσκουμε την ανάλυση της σ σε γινόμενο κύκλων ξένων ανά δύο, $\sigma = (1675)(234)$.

i) Έχουμε ότι $|\sigma| =$ εκπ(4,3)$= 12$.

ii) Επειδή $50 \equiv 2 \mod 12$, έχουμε $< \sigma^{50} > = < \sigma^2 > = \{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\}$. Με παρόμοιο τρόπο βρίσκουμε $< \sigma^{33} > = < \sigma^{-3} > = < \sigma^3 > = \{1, \sigma^3, \sigma^6, \sigma^9\}$. Άρα $< \sigma^{50} > \cap < \sigma^{33} > = \{1, \sigma^6\}$ και η ζητούμενη τάξη είναι 2.

iii) Όχι. Επειδή $\sigma = (1675)(234)$, έχουμε ότι η σ είναι γινόμενο μιας περιττής μετάθεσης και μιας άρτιας, άρα είναι περιττή μετάθεση. Είδαμε ότι κάθε μετάθεση με περιττή τάξη είναι άρτια στο Παράδειγμα 8.20(2). Συνεπώς αν είχαμε $\sigma = \sigma_1\sigma_2$, όπου σ_i έχουν περιττές τάξεις, τότε η σ θα ήταν και περιττή και άρτια. Αυτό είναι αδύνατο από την Πρόταση 8.17.

iv) Όχι. Το αριστερό σκέλος είναι περιττή διότι η σ είναι περιττή. Το δεξί είναι άρτια. Και πάλι αδύνατο από την Πρόταση 8.17.

22. *Λύση.* Η A_n περιέχει κυκλική υποομάδα τάξης 4 αν και μόνο αν περιέχει στοιχείο τάξης 4. Παρατηρούμε ότι για κάθε $n \geq 4$, η A_n περιέχει τον κύκλο (1234), που έχει τάξη 4 γιατί έχει μήκος 4. Η A_n για $n < 4$ δεν περιέχει υποομάδα τάξης 4, αφού $|A_n| < 4$ στις περιπτώσεις αυτές.

23. *Λύση.* Η A_6 δεν περιέχει στοιχείο τάξης 6. Πράγματι, από τη λύση της άσκησης 8.14, έπεται ότι κάθε στοιχείο της S_6 τάξης 6 είναι ή κύκλος μήκος 6 -άρα περιττή μετάθεση - ή γινόμενο ενός κύκλου μήκους 3 και ενός κύκλου μήκους 2 - άρα περιττή μετάθεση. Δηλαδή κάθε στοιχείο τάξης 6 της S_6 είναι περιττή μετάθεση.

24. ii) *Λύση.* Έστω $\sigma \in S_n - \{1\}$ όπου $n \geq 3$. Υπάρχει i με $\sigma(i) \neq i$. Επειδή $n \geq 3$, υπάρχει j ώστε τα $i, j, \sigma(i)$ είναι διακεκριμένα. Τώρα αν $\sigma(ij) = (ij)\sigma$, τότε στο αριστερό μέλος έχουμε $i \mapsto j \mapsto \sigma(j)$ και στο δεξί μέλος $i \mapsto \sigma(i) \mapsto \sigma(i)$. Άρα $\sigma(j) = \sigma(i) \Rightarrow i = j$, αδύνατο.

25. *Υπόδειξη.* Χρησιμοποιήστε τις εξής ισότητες. Αν a, b, c, d είναι διακεκριμένα, τότε
   i) $(ac)(ab) = (abc)$,
   ii) $(ab)(cd) = (abc)(bcd)$.

26. *Υπόδειξη.* Αν $n \geq 4$, παρατηρήστε ότι $(123)(124) \neq (124)(123)$.

27.

28. *Απάντηση.* 1 αν η ομάδα είναι κυκλική, 6 αν δεν είναι κυκλική.

29. *Υπόδειξη.* Έστω $a, b \in G$ περιττής τάξης. Δείξτε ότι η υπόθεση συνεπάγεται ότι $ab = ba$. Στη συνέχεια δείξτε ότι τα ab και ab^{-1} είναι περιττής τάξης.
30. *Υπόδειξη.* Θεωρήστε τις κυκλικές υποομάδες. Μπορεί κάποια από αυτές να είναι άπειρη;
31. *Υπόδειξη.* Ένας τρόπος είναι να χρησιμοποιήσουμε το Παράδειγμα 8.23(4) και τις σχέσεις
$$(1i) = (1\ i-1)(i-1\ i)(1\ i-1), i \geq 3.$$
32. *Υπόδειξη.* Θεωρήστε την ομάδα $< \sigma >$, $\sigma = (x_1\ x_2\ ...\ x_m)$, όπου $X = \{x_1, ..., x_m\}$.
33. *Υπόδειξη.* Αν $G/K = \{a_1K, ..., a_mK\}$ και $K/H = \{b_1H, ..., b_nH\}$, δείξτε ότι
$$G/H = \{a_ib_jH : 1 \leq i \leq m,\ \ 1 \leq j \leq n\}$$
και τα a_ib_jH είναι διακεκριμένα.
34. *Λύση.* Αν $b = 0$, τότε $a = 0$. Συνεπώς υποθέτουμε ότι $b \neq 0$. Πολλαπλασιάζοντας με b^{-2}, παίρνουμε $x^2 + x + 1 = 0$, όπου $x = ab^{-1}$. Με χρήση της παραπάνω σχέσης και του γεγονότος ότι η χαρακτηριστική του F είναι 2, εύκολα επαληθεύεται ότι τα στοιχεία $1, x, x+1$ είναι διακεκριμένα και ότι το υποσύνολο του F^*, $H = \{1, x, x+1\}$, είναι κλειστό ως προς τον πολλαπλασιασμό. Για παράδειγμα, $(x+1)^2 = x^2 + 2x + 1 = x^2 + 1 = x$. Άρα το H είναι υποομάδα της πολλαπλασιαστικής ομάδας F^* σύμφωνα με την Πρόταση 8.4(4). Από το θεώρημα του Lagrange έχουμε ότι $3|2^n - 1$. Άρα $(-1)^n \equiv 1 \mod 3 \Rightarrow n$ άρτιος, αδύνατο από την υπόθεση.
35. Έστω $G = H \cup K$, $x \in H - K, y \in K - H$. Τότε
$$xy \in G \Rightarrow xy \in H \text{ ή } xy \in K.$$
Στην πρώτη περίπτωση παίρνουμε $y = (x^{-1}x)y = x^{-1}(xy) \in H$ αφού το H είναι υποομάδα και $x, xy \in H$. Αυτό είναι άτοπο. Όμοια, έχουμε άτοπο και στη δεύτερη περίπτωση. Συνεπώς $H \subseteq K$ ή $K \subseteq H$.
Για το δεύτερο ερώτημα, παρατηρούμε ότι αν $G = H \cup K$, όπου H, K γνήσιες υποομάδες της G, τότε από το πρώτο ερώτημα έχουμε $H \subseteq K$ ή $K \subseteq H$. Αυτό σημαίνει ότι $G = K$ ή $G = H$, άτοπο.
36.

Ομομορφισμοί ομάδων

Στο κεφάλαιο αυτό θα δούμε ότι οι ομομορφισμοί ομάδων μας επιτρέπουν να συγκρίνουμε ομάδες. Αποδεικνύουμε το θεώρημα του Caley. Στη συνέχεια ταξινομούμε ως προς ισομορφισμό της κυκλικές ομάδες και προσδιορίζουμε τη δομή τους.

Βασικά σημεία

- ομομορφισμοί και ισομορφισμοί
- ταξινόμηση κυκλικών ομάδων
- υποομάδες κυκλικών ομάδων

9.1. Ομομορφισμοί

Ορισμός 9.1. *Έστω $(G,\cdot)$ και $(H,*)$ ομάδες. Μια απεικόνιση $f: G \to H$ λέγεται,*

(1) ***ομομορφισμός*** *αν $f(a\cdot b) = f(a) * f(b)$ για κάθε $a,b \in G$.,*
(2) ***μονομορφισμός*** *αν είναι ομομορφισμός και 1-1.*
(3) ***επιμορφισμός*** *αν είναι ομομορφισμός και επί,*
(4) ***ισομορφισμός*** *αν είναι ομομορφισμός, 1-1 και επί.*

Θα λέμε ότι οι ομάδες G και H είναι ***ισόμορφες*** *αν υπάρχει ισομορφισμός ομάδων $G \to H$. Στην περίπτωση αυτή θα γράφουμε $G \simeq H$.*

Στα επόμενα θα γράφουμε ab στην θέση του $a\cdot b$ και όμοια $f(a)f(b)$ στην θέση του $f(a) * f(b)$.

Παραδείγματα 9.2.

(1) **Ομομορφισμοί προσθετικών ομάδων δακτυλίων** Έστω $\varphi: R \to S$ ομομορφισμός δακτυλίων. Τότε η φ είναι ομομορφισμός ομάδων των αντίστοιχων προσθετικών ομάδων $(R,+) \to (S,+)$. Από τα Παραδείγματα 5.2 έχουμε:
   - Η απεικόνιση $\mathbb{Z} \to \mathbb{Z}_n,\ \ a \mapsto [a]$ είναι ομομορφισμός ομάδων.
   - Η απεικόνιση $\varphi: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ με $\varphi(a+b\sqrt{2}) = a - b\sqrt{2}$ είναι ισομορφισμός ομάδων.
   - Η απεικόνιση $\varphi: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, με $\varphi([a]_{mn}) = ([a]_m, [a]_n)$. είναι ομομορφισμός ομάδων. Αν επιπλέον ισχύει ότι $\mu\kappa\delta(m,n) = 1$, τότε είναι ισομορφισμός.

(2) **Ομομορφισμοί πολλαπλασιαστικών ομάδων δακτυλίων** Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων που έχουν μονάδες, τέτοιος ώστε $\varphi(1_R) = 1_S$. Τότε η φ είναι ομομορφισμός ομάδων των αντίστοιχων πολλαπλασιαστικών ομάδων $U(R) \to U(S)$ των αντιστρέψιμων στοιχείων. Βλ. άσκηση 6.7. Από τα Παραδείγματα 5.2(2) έχουμε:

- Έστω $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) : a, b \in \mathbb{R}, (a,b) \neq (0,0) \right\}$ και $H = \mathbb{C}^*$. Η απεικόνιση $\varphi : G \to H$ με $\varphi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + bi$ είναι ισομορφισμός ομάδων.
- Η απεικόνιση $\varphi : U(\mathbb{Z}_{mn}) \to U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$, με
$$\varphi([a]_{mn}) = ([a]_m, [a]_n).$$
είναι ομομορφισμός ομάδων. Αν επιπλέον ισχύει ότι $\mu\kappa\delta(m,n) = 1$, τότε είναι ισομορφισμός.

(3) Η απεικόνιση $\mathbb{Z} \to n\mathbb{Z}, a \mapsto an$, είναι ομομορφισμός ομάδων και αν $n \neq 0$, είναι ισομορφισμός.

Η απεικόνιση $\mathbb{Z} \to n\mathbb{Z}, a \mapsto 2an$, είναι ομομορφισμός ομάδων και αν $n \neq 0$ είναι μονομορφισμός (αλλά όχι επιμορφισμός).

(4) Η απεικόνιση $\varphi : \mathbb{Z} \to E_n$, $\varphi(a) = z^a$, όπου $z = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in E_n$ είναι επιμορφισμός ομάδων. Πράγματι, είναι ομομορφισμός
$$\varphi(a+b) = z^{a+b} = z^a \cdot z^b = \varphi(a)\varphi(b)$$
και επειδή $E_n =< z >$, η φ είναι επί.

(5) Η $\varphi : \mathbb{Z}_n \to E_n$ $(n > 0)$, $\varphi([a]) = z^a$, με z όπως στο (4) είναι (καλώς ορισμένη) ισομορφισμός ομάδων. Πράγματι, έστω
$$[a] = [b] \Rightarrow n \mid a - b \overset{(n=|E_n|)}{\Longrightarrow} z^{a-b} = 1 \Rightarrow z^a = z^b.$$
Η φ είναι προφανώς επί, αφού $E_n =< z >$. Τέλος η φ είναι ομομορφισμός ομάδων. Πράγματι,
$$\varphi([a+b]) = z^{a+b} = z^a z^b = \varphi([a])\varphi([b]).$$

(6) Η $\varphi : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$, $\varphi(x) = \ln(x)$ (λογάριθμος) είναι ομομορφισμός ομάδων αφού $\ln(xy) = \ln x + \ln y$ για κάθε $x, y \in \mathbb{R}_{>0}$. Μάλιστα είναι ισομορφισμός.

(7) Θεωρούμε την ομάδα $(\mathbb{C}^*, \cdot)$ των μη μηδενικών μιγαδικών αριθμών με πράξη τον πολλαπλασιασμό μιγαδικών. Η απεικόνιση $(\mathbb{C}^*, \cdot) \to (\mathbb{R}_{>0}, \cdot)$, $z \mapsto |z|$, (το μέτρο του z), είναι ομομορφισμός ομάδων αφού για κάθε $z_1, z_2 \in \mathbb{C}$ ισχύει $|z_1 z_2| = |z_1||z_2|$. Μάλιστα είναι επιμορφισμός.

(8) **Ορίζουσα** Έστω k σώμα. Λόγω της γνωστής πολλαπλασιαστικής ιδιότητας της ορίζουσας $det(AB) = det(A)det(B)$, η απεικόνιση
$$GL_n(k) \to (k*, \cdot), A \mapsto det(A),$$
είναι ομομορφισμός ομάδων. Μάλιστα είναι επιμορφισμός, καθώς αν $a \in \mathbb{R} \setminus \{0\}$, τότε
$$\det(diag(a, 1..., 1)) = a.$$

(9) **Πρόσημο μετάθεσης** Έστω $\sigma \in S_n$. Ορίζουμε,
$$\text{sign}(\sigma) = \begin{cases} 1, & \text{αν } \sigma \text{ άρτια} \\ -1, & \text{αν } \sigma \text{ περιττή} \end{cases}$$
Αφού κάθε $\sigma \in S_n$ είναι ή άρτια ή περιττή (όχι και τα δύο), έχουμε την απεικόνιση $\text{sign} : S_n \to \{1, -1\} = E_2$, η οποία είναι επιμορφισμός ομάδων $(n \geq 2)$. Πράγματι, το γινόμενο

i) δύο άρτιων μεταθέσεων είναι άρτια μετάθεση,
ii) δύο περιττών μεταθέσεων είναι άρτια μετάθεση,
iii) μιας άρτιας και μιας περιττής είναι περιττή (με οποιαδήποτε σειρά).

Παρατήρηση. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Ισχύουν τα εξής.

(1) $\varphi(1_G) = 1_H$.
(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$ για κάθε $a \in G$.
(3) $\varphi(a^m) = \varphi(a)^m$ για κάθε $m \in \mathbb{Z}$.

Πράγματι, για το (1), αν $a \in G$, έχουμε

$$a1_G = a \Rightarrow \varphi(a1_G) = \varphi(a) \Rightarrow \varphi(a)\varphi(1_G) = \varphi(a) \Rightarrow \varphi(1_G) = 1_H.$$

Για το (2), αν $a \in G$, έχουμε

$$aa^{-1} = 1_G \Rightarrow \varphi(aa^{-1}) = \varphi(1_G) \Rightarrow \varphi(a)\varphi(a^{-1}) = 1_H \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1}.$$

Αφήνουμε το (3) ως άσκηση στην επαγωγή.

Όπως στην περίπτωση των δακτυλίων, οι ομομορφισμοί ομάδων συμπεριφέρονται καλά ως προς τη σύνθεση απεικονίσεων. Η απόδειξη της ακόλουθης πρότασης ουσιαστικά περιέχεται στην απόδειξη της Πρότασης 5.5.

Πρόταση 9.3. *Έστω $\varphi : G \to H$ και $\psi : H \to K$ ομομορφισμοί ομάδων.*
(1) *Η σύνθεση $\psi \circ \varphi : G \to K$ είναι ομομορφισμός ομάδων. Ειδικά, αν οι φ, ψ είναι ισομορφισμοί, τότε ο $\psi \circ \varphi$ είναι ισομορφισμός.*
(2) *Αν ο φ είναι ισομορφισμός, τότε η αντίστροφη απεικόνιση $\varphi^{-1} : H \to G$ είναι ισομορφισμός.*

Ισόμορφες ομάδες έχουν πολλές κοινές ιδιότητες, κατ΄ αναλογία με την περίπτωση ισόμορφων δακτυλίων, όπως είδαμε στην Πρόταση 5.7. Για παράδειγμα:

Πρόταση 9.4. *Έστω $\varphi : G \to H$ ισομορφισμός ομάδων.*
(1) *Η G είναι πεπερασμένη αν και μόνο αν η H είναι πεπερασμένη.*
(2) *Η G είναι αβελιανή αν και μόνο αν η H είναι αβελιανή.*
(3) *Η G είναι κυκλική αν και μόνο αν η H είναι κυκλική.*
(4) *Για κάθε $g \in G$, τα στοιχεία g και $\varphi(g)$ έχουν την ίδια τάξη.*

Απόδειξη. Σε κάθε περίπτωση αρκεί να αποδείξουμε το ευθύ λόγω της Πρότασης 9.3(2). Αποδεικνύουμε ενδεικτικά το (3). Οι άλλες αποδείξεις αφήνονται στον αναγνώστη. Έστω $G =< g >= \{g^m : m \in \mathbb{Z}\}$. Επειδή η φ είναι επί, έχουμε

$$H = \varphi(G) = \{\varphi(g^m) : m \in \mathbb{Z}\}.$$

Επειδή η φ είναι ομομορφισμός, παίρνουμε $H = \{\varphi(g)^m : m \in \mathbb{Z}\}$, και συνεπώς $H =< \varphi(g) >$ που είναι κυκλική. □

Παρατήρηση. Τονίζουμε ότι στο παραπάνω επιχείρημα του ευθέος, δεν χρησιμοποιήσαμε ότι η φ είναι 1-1. Με άλλα λόγια, αν έχουμε επιμορφισμό ομάδων $\varphi : G \to H$ και η G είναι κυκλική, τότε και η H είναι κυκλική.

Παραδείγματα 9.5.

(1) Οι ομάδες $\mathbb{Z}_4$ και $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφες. Η πρώτη είναι κυκλική ενώ η δεύτερη δεν είναι κυκλική καθώς δεν διαθέτει στοιχείο τάξης 4.

(2) Οι ομάδες D_4 και $\mathbb{Z}_2 \times \mathbb{Z}_4$ δεν είναι ισόμορφες καθώς η πρώτη δεν είναι αβελιανή ενώ η δεύτερη είναι.

(3) Έστω R, S, T δακτύλιοι με μονάδες τέτοιοι ώστε υπάρχει ισομορφισμός δακτυλίων $\varphi : R \to S \times T$. Από την άσκηση 6.7 που με μεταφυσική, απόλυτη βεβαιότητα έχουμε λύσει γιατί φέρει αστεράκι, ο περιορισμός της φ στο υποσύνολο $U(R)$ των αντιστρέψιμων

στοιχείων του R, δίνει ισομορφισμό ομάδων $U(R) \simeq U(S \times T)$. Από την άσκηση 3.13 έχουμε $U(S \times T) = U(S) \times U(T)$, ώστε τελικά έχουμε ισομορφισμό ομάδων

$$U(R) \simeq U(S) \times U(T).$$

(4) Έστω $f(x) = x^3 + 2x^2 + x + 2 \in \mathbb{Z}_3[x]$. Θεωρούμε το κύριο ιδεώδες $I =< f(x) >$ του $\mathbb{Z}_3[x]$ και το δακτύλιο πηλίκο $R = \mathbb{Z}_3[x]/I$. Θα παραστήσουμε την ομάδα $U(R)$ των αντιστρέψιμων στοιχείων του R ως ευθύ γινόμενο δύο μη τετριμμένων ομάδων και θα εξετάσουμε αν η $U(R)$ είναι κυκλική.
Παρατηρούμε ότι το $1 \in \mathbb{Z}_3$ είναι ρίζα του $f(x)$ και κάνοντας την Ευκλείδεια διαίρεση βρίσκουμε $f(x) = (x-1)(x^2+1)$. Το x^2+1 δεν έχει ρίζα στο $\mathbb{Z}_3$ και επειδή έχει βαθμό 2 είναι ανάγωγο. Συνεπώς έχουμε βρει την ανάλυση του $f(x)$ σε γινόμενο ανάγωγων στο $\mathbb{Z}_3[x]$. Επειδή τα πολυώνυμα $x-1, x^2+1$ είναι σχετικά πρώτα και το $\mathbb{Z}_3$ σώμα, τα αντίστοιχα κύρια ιδεώδη είναι σχετικά πρώτα. Συνεπώς εφαρμόζει το Κινέζικο θεώρημα υπολοίπων, Θεώρημα 6.14, σύμφωνα με τι οποίο έχουμε ισομορφισμό δακτυλίων $R \simeq \mathbb{Z}_3[x]/ < x-1 > \times \mathbb{Z}_3[x]/ < x^2+1 >$, οπότε από το προηγούμενο παράδειγμα έχουμε ισομορφισμό ομάδων

$$U(R) \simeq U(\mathbb{Z}_3[x]/ < x-1 >) \times U(\mathbb{Z}_3[x]/ < x^2+1 >).$$

Ξέρουμε ότι έχουμε ισομορφισμό δακτυλίων $\mathbb{Z}_3[x]/ < x-1 > \simeq \mathbb{Z}_3$, Παράδειγμα 6.11(1), και επειδή ο $\mathbb{Z}_3$ είναι σώμα παίρνουμε

$$U(\mathbb{Z}_3[x]/ < x-1 >) \simeq \mathbb{Z}_3 - \{0\}$$

που είναι ομάδα τάξης 2. Επίσης ξέρουμε ότι ο δακτύλιος $\mathbb{Z}_3[x]/ < x^2+1 >$ είναι σώμα αφού το x^2+1 είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Επιπλέον, από την Πρόταση 6.5, ο $\mathbb{Z}_3[x]/ < x^2+1 >$ έχει $3^2 = 9$ στοιχεία. Άρα η ομάδα $U(\mathbb{Z}_3[x]/ < x^2+1 >)$ έχει 8 στοιχεία. (Μάλιστα είναι κυκλική από το Θεώρημα 8.14, αλλά αυτό δεν μας ενδιαφέρει εδώ.) Συνεπώς έχουμε την κατάσταση

$$U(R) \simeq H \times K, \ \ |H| = 2, \ \ |K| = 8.$$

Είναι σαφές ότι κάθε στοιχείο της ομάδας $H \times K$ έχει τάξη το πολύ 8 αφού $(h,k)^8 = (h^8, k^8) = (1_H, 1_K)$ Συμπερασματικά, $|U(R)| = 16$ και κάθε στοιχείο της $U(R)$ έχει τάξη το πολύ 8. Δηλαδή η $U(R)$ δεν έχει στοιχείο τάξης 16, ισοδύναμα δεν είναι κυκλική.

Ορισμός 9.6. *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Ορίζουμε,*

$$\ker \varphi = \{g \in G : \varphi(g) = 1\} \quad (\textit{ο } \textbf{πυρήνας της } \varphi),$$
$$\mathrm{Im}\varphi = \{\varphi(g) \in H : g \in G\} \quad (\textit{η } \textbf{εικόνα της } \varphi).$$

Πρόταση 9.7. *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε*
(1) $\ker \varphi \leq G$.
(2) $\mathrm{Im}\varphi \leq H$.
(3) *H φ είναι 1-1 αν και μόνο αν* $\ker \varphi = \{1\}$.

Απόδειξη. Ας δείξουμε ενδεικτικά το (2). Παρατηρούμε ότι $\mathrm{Im}\varphi \neq \emptyset$, αφού $\varphi(1_G) = 1_H$, δηλαδή $1_H \in \mathrm{Im}\varphi$. Έστω $a, b \in \mathrm{Im}\varphi$. Τότε $\varphi(g_a) = a$ και $\varphi(g_b) = b$ για κάποια $g_a, g_b \in G$. Επομένως $ab = \varphi(g_a)\varphi(g_b) = \varphi(g_a g_b) \in \mathrm{Im}\varphi$. Επίσης έχουμε $a^{-1} = (\varphi(g_a))^{-1} = \varphi(g_a^{-1}) \in \mathrm{Im}\varphi$. □

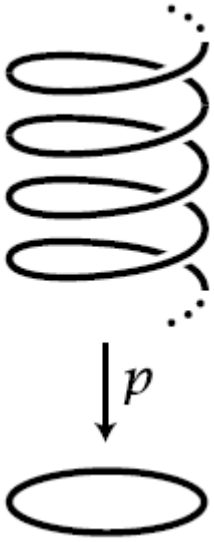
Παραδείγματα 9.8.

(1) Η απεικόνιση $\varphi : \mathbb{Z} \to E_n$ που είδαμε στο Παράδειγμα 9.2(4) έχει $\ker \varphi =< n >= n\mathbb{Z}$. Πράγματι, $z^a = 1 \Leftrightarrow |z| \mid a \Leftrightarrow n|a$.

(2) Με χρήση των ταυτοτήτων για το $cos(x+y)$ και $sin(x+y)$ εύκολα αποδεικνύεται ότι η απεικόνιση $p : \mathbb{R} \to \mathbb{C}^*$,

$$p(a) = \cos(2\pi a) + i\sin(2\pi a)$$

είναι ομομορφισμός ομάδων. Έχουμε $\mathrm{Im}p = E = \{z \in \mathbb{C} : |z| = 1\}$, όπου $|z|$ το μέτρο του $z \in \mathbb{C}$. Επίσης, $\ker p = \mathbb{Z}$. Γεωμετρικά η p "επιμηκύνει" τον άξονα $\mathbb{R}$ κατά 2π και τον "τυλίγει" γύρω από τον κύκλο, όπως δείχνει η εικόνα.



(3) Έστω $\varphi : \mathbb{Z}_{24} \to S_5, \quad \varphi([a]) = \sigma^a$, όπου $\sigma = (13)(245)$. Η φ είναι καλώς ορισμένη, ομομορφισμός ομάδων και $\ker\varphi =< [6] >$. Επίσης $\mathrm{Im}\varphi =< \sigma >$.

Πράγματι, παρατηρούμε ότι $|\sigma| = \text{εκπ}(2,3) = 6$ ($(13)(245)$ είναι γινόμενο ξένων κύκλων). Έστω $[a] = [b]$. Τότε

$$24 \mid a - b \Rightarrow 6 \mid a - b \Rightarrow \sigma^a = \sigma^b.$$

Η φ είναι ομομορφισμός ομάδων αφού $\sigma^{a+b} = \sigma^a\sigma^b$. Επίσης,

$$\ker\varphi = \{[a] \in \mathbb{Z}_{24} : \sigma^a = 1\} = \{[a] \in \mathbb{Z}_{24} : |6| \mid a\} = \{[6] \in \mathbb{Z}_{24} : \sigma \mid a\} =< [b] >$$

και $\mathrm{Im}\varphi = \{\sigma^a : [a] \in \mathbb{Z}_{24}\} = \{\sigma^a : a \in \mathbb{Z}\} =< \sigma > .$

Σύμφωνα με την επόμενη Πρόταση, το ευθύ γινόμενο ομάδων $G \times H$ περιέχει υποομάδα ισόμορφη με τη G και υποομάδα ισόμορφη με την H.

Πρόταση 9.9. *Έστω G, H ομάδες. Οι απεικονίσεις*

$$i_1 : G \to G \times H, g \mapsto (g, 1_H) \ \textit{και}\ i_2 : H \to G \times H, h \mapsto (1_G, h),$$

είναι μονομορφισμοί ομάδων και οι απεικονίσεις

$$\pi_1 : G \times H \to G, (g,h) \mapsto g \ \textit{και}\ \pi_2 : G \times H \to H, (g,h) \mapsto h,$$

είναι επιμορφισμοί ομάδων. Επιπλέον, $\ker\pi_1 = Im(i_2)$ *και* $\ker\pi_2 = Im(i_1)$

Απόδειξη. Άσκηση. □

Θα δούμε τώρα ότι οι συμμετρικές ομάδες περιέχουν αντίτυπα όλων των πεπερασμένων ομάδων.

Θεώρημα 9.10 (Cayley). *Έστω G πεπερασμένη ομάδα. Τότε η G είναι ισόμορφη με υποομάδα κάποιας S_n.*

Απόδειξη. Έστω $g \in G$. Θεωρούμε την απεικόνιση $L_g : G \to G$, με $L_g(a) = ga$ για κάθε $a \in G$. Θα δείξουμε ότι η L_g είναι 1-1 και επί. Πράγματι, αν $L_g(a) = L_g(a')$ Τότε

$$ga = ga' \Rightarrow a = a'.$$

Η L_g είναι επί αφού αν $a \in G$ Τότε $L_g(g^{-1}a) = g(g^{-1}a) = a$.) Άρα η L_g είναι μια μετάθεση του συνόλου G, δηλαδή $L_g \in S(G) =$ το σύνολο των μεταθέσεων του συνόλου G. Ορίζουμε τώρα την απεικόνιση

$$\varphi : G \to S(G), \;\; \varphi(g) = L_g.$$

Η φ είναι μονομορφισμός ομάδων (η $S(G)$ είναι ομάδα με πράξη την σύνθεση). Πράγματι, $\varphi(g_1g_2) = L_{g_1g_2}$ και $\varphi(g_1)\varphi(g_2) = L_{g_1}L_{g_2}$. Παρατηρούμε ότι

$$L_{g_1}L_{g_2}(a) = L_{g_1}(g_2a) = g_1(g_2a) = (g_1g_2)a = L_{g_1g_2}(a).$$

Επίσης έχουμε $\ker\varphi = \{g \in G : L_g = 1_{S(G)}\}$. Παρατηρούμε ότι

$$L_g = 1_{S(G)} \Leftrightarrow L_g(a) = 1_{S(G)}(a) \;\text{ για κάθε }\; a \in G \Leftrightarrow ga = a \Leftrightarrow g = 1_G.$$

Επομένως $\ker\varphi = \{1_G\}$. □

Παράδειγμα 9.11. Έστω $G =< g >$, $|G| = 3$. Δηλαδή $G = \{1, g, g^2\}$. Έχουμε

$$L_1 = \begin{pmatrix} 1 & g & g^2 \\ 1 & g & g^2 \end{pmatrix},\; L_g = \begin{pmatrix} 1 & g & g^2 \\ g & g^2 & 1 \end{pmatrix},\; L_{g^2} = \begin{pmatrix} 1 & g & g^2 \\ g^2 & 1 & g \end{pmatrix}.$$

$$G \simeq \left\{1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\} = A_3 \leq S_3.$$

9.2. Ταξινόμηση κυκλικών ομάδων

Θα δούμε εδώ ότι δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια τάξη. Κάτι αντίστοιχο στις αβελιανές ομάδες δεν ισχύει καθώς οι ομάδες $\mathbb{Z}_4$ και $\mathbb{Z}_2 \times \mathbb{Z}_2$ έχουν τάξη 4, αλλά δεν είναι ισόμορφες όπως είδαμε στο Παράδειγμα 9.5(1).

Θεώρημα 9.12 (Ταξινόμηση κυκλικών ομάδων)**.**
(1) *Κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την ομάδα* $\mathbb{Z}$.
(2) *Κάθε πεπερασμένη κυκλική ομάδα τάξης* n *είναι ισόμορφη με την* $\mathbb{Z}_n$.

Απόδειξη. (1) Έστω $G =< a >$ άπειρη κυκλική ομάδα. Θεωρούμε την απεικόνιση

$$\varphi : \mathbb{Z} \to G, \;\; \varphi(k) = a^k.$$

Η φ είναι ομομορφισμός ομάδων αφού $\varphi(k + k') = a^{k+k'} = a^k a^{k'} = \varphi(k)\varphi(k')$. Είναι σαφές ότι η φ είναι επί. Τέλος η φ είναι 1-1. Πράγματι έστω $k \in \ker\varphi$. Τότε $\varphi(k) = 1_G \Rightarrow a^k = 1_G$. Επειδή η τάξη του a είναι άπειρη, έχουμε $k = 0$. Επομένως $\ker\varphi = \{0\}$.

(2) Έστω $G =< a >$ πεπερασμένη κυκλική ομάδα τάξης n. Θεωρούμε την απεικόνιση

$$\varphi : \mathbb{Z}_n \to G, \;\; \varphi([k]) = a^k.$$

Η φ είναι καλώς ορισμένη. Πράγματι, αν $[k] = [k']$ τότε $k \equiv k' \mod n$ και άρα $a^k = a^{k'}$. Η φ είναι ομομορφισμός ομάδων, αφού $\varphi([k] + [k']) = a^{k+k'} = a^k a^{k'} = \varphi([k])\varphi([k'])$. Είναι σαφές ότι η φ είναι επί. Επίσης η φ είναι 1-1. Πράγματι,

$$[k] \in \ker\varphi \Leftrightarrow a^k = 1_G \Leftrightarrow n \mid k \;\text{ αφού }\; |a| = n.$$

Επομένως $\ker\varphi = \{[0]\}$, δηλαδή η φ είναι 1-1. □

Πόρισμα 9.13. *Δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια τάξη.*

Για παράδειγμα, αν $n \geq 1$, οι ακόλουθες ομάδες είναι κυκλικές τάξης n και άρα ισόμορφες ανά δύο,

$$\mathbb{Z}_n,\ E_n,\ <(12\cdots n)>,\ rot(D_n)$$

όπου $<(12\cdots n)>$ είναι η κυκλική υποομάδα της S_n που παράγεται από τον κύκλο $(12\cdots n)$ και $rot(D_n)$ είναι η υποομάδα της διεδρικής D_n που αποτελείται από τις περιστροφές.

9.3. Δομή κυκλικών ομάδων

Ξέρουμε από το θεώρημα του Lagrange ότι η τάξη κάθε υποομάδας πεπερασμένης ομάδας G διαιρεί την τάξη της G. Εδώ θα δούμε, μεταξύ των άλλων, ότι στις κυκλικές ομάδες ισχύει το αντίστροφο, δηλαδή για κάθε διαιρέτη m της τάξης πεπερασμένης κυκλικής ομάδας G, υπάρχει υποομάδα H της G τάξης m. Επιπλέον θα δούμε ότι για κάθε τέτοιο m υπάρχει μοναδική H.

Θεώρημα 9.14 (Οι υποομάδες κυκλικής ομάδας)**.**
(1) *Κάθε υποομάδα κυκλικής ομάδας είναι κυκλική.*
(2) *Για κάθε διαιρέτη m της τάξης μιας πεπερασμένης κυκλικής ομάδας G, υπάρχει μοναδική $H \leq G$ με $|H| = m$.*

Απόδειξη. (1) Έστω $G =< a >$ κυκλική ομάδα και $H \leq G,\ H \neq \{1_G\}$. Τότε υπάρχει $m \in \mathbb{Z}$ ώστε $a^m \in H,\ m \neq 0$. Άρα $a^{-m} \in H$. Επομένως υπάρχει ελάχιστος θετικός ακέραιος, έστω m, τέτοιος ώστε $a^m \in H$. Θα δείξουμε ότι $H =< a^m >$.
Πράγματι, $< a^m > \subseteq H$ αφού $a^m \in H$ και $H \leq G$.
Μένει να δείξουμε ότι $H \subseteq < a^m >$. Για το σκοπό αυτό, έστω $a^k \in H$. Από την Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{N}$ ώστε $k = qm + r,\ \ 0 \leq r < m$. Επομένως

$$a^r = a^k a^{-qm} = a^k (a^m)^{-q} \in H.$$

Από το ελάχιστο στον ορισμό του m, έπεται ότι $r = 0$. Άρα $k = qm$ και $a^k = (a^m)^q \in H$.
(2) Έστω $G =< a >$ πεπερασμένη κυκλική ομάδα, $|G| = n$ και $m|n$. Θα δείξουμε ότι υπάρχει $H \leq G$, με $|H| = m$. Θεωρούμε $H =< a^{n/m} >$. Από τον ορισμό της τάξης στοιχείου ($|a| = n$) έχουμε $|a^{n/m}| = m$. Επομένως $|H| = m$.
Έστω τώρα $K \leq G$, με $|K| = m$. Θα δείξουμε ότι $K =< a^{n/m} >$. Από το (1), η K είναι κυκλική, δηλαδή $K =< a^k >$, για κάποιο $k \in \mathbb{Z}$. Επειδή $|K| = m$, έχουμε

$$(a^k)^m = 1 \Rightarrow a^{km} = 1 \Rightarrow n \mid km \Rightarrow \frac{n}{m} \mid k \Rightarrow a^k \in < a^{n/m} > .$$

Επομένως $K \subseteq < a^{n/m} >$ και επειδή τα δύο σύνολα έχουν $m < \infty$, στοιχεία, έπεται ότι $K =< a^{n/m} >$. □

Παρατήρηση. Τονίζουμε ότι η προηγούμενη απόδειξη παρέχει μια συγκεκριμένη 1-1 και επί αντιστοιχία μεταξύ των θετικών διαιρετών m της τάξης n πεπερασμένης κυκλικής ομάδας $G =< g >$ και των υποομάδων της G ως εξής:

$$m \longleftrightarrow G_m =< g^{n/m} > .$$

Εδώ, η υποομάδα $G_m =< g^{n/m} >$ είναι η μοναδική υποομάδα της G τάξης m. Θα δούμε τώρα την αντιστοιχία αυτή σε δύο παραδείγματα.

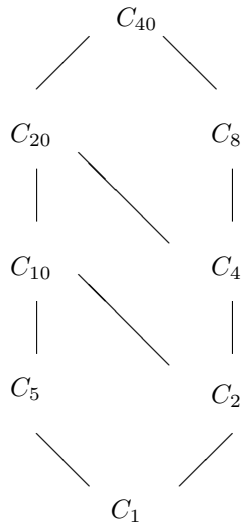
Διάγραμμα υποομάδων κυκλικών ομάδων

Το διάγραμμα υποομάδων πεπερασμένης ομάδας G ορίζεται ως εξής. Οι κορυφές του γραφήματος αντιστοιχούν στις υποομάδες της G. Δύο υποομάδες A, B της G συνδέονται με μία ακμή αν ισχύει $A \subset B$ ή $B \subset A$ και δεν υπάρχει υποομάδα C με $A \subset C \subset B$ ή

$B \subset C \subset A$. Στην περίπτωση αυτή, η υποομάδα που αντιστοιχεί στο άνω άκρο της ακμής περιέχει την υποομάδα που αντιστοιχεί στο κάτω άκρο.

Το διάγραμμα των υποομάδων μιας πεπερασμένης ***κυκλικής*** ομάδας G τάξης n, προσδιορίζεται πλήρως από την ανάλυση του n σε γινόμενο πρώτων, διότι
• για κάθε διαιρέτη m του n υπάρχει μοναδική υποομάδα C_m της G τάξης m (που από το Θεώρημα 9.14 οφείλει να είναι κυκλική), και
• $C_m \subseteq C_{m'} \Leftrightarrow m|m'$.

Για $G = C_{40}$ κυκλική ομάδα τάξης 40 το διάγραμμα υποομάδων είναι το εξής.



Για $G = C_{p^3}$ κυκλική τάξης p^3, όπου p πρώτος, το διάγραμμα υποομάδων της G είναι το ακόλουθο.

Καλό είναι να συγκριθούν τα διαγράμματα υποομάδων κυκλικών ομάδων και ιδεωδών του δακτυλίου $\mathbb{Z}_n$ που είδαμε στην Παράγραφο 6.3. Είναι σαφές ότι 'είναι τα ίδια';

Από το Θεώρημα 9.14 έπεται ότι μια κυκλική ομάδα άρτιας τάξης έχει *μοναδικό* στοιχείο τάξης 2. Γενικά έχουμε το εξής αποτέλεσμα.

Πρόταση 9.15. *Έστω G πεπερασμένη κυκλική ομάδα τάξης n. Τότε για κάθε διαιρέτη d του n, το πλήθος των στοιχείων της G που έχουν τάξη d είναι ίσο με $\varphi(d)$*

Απόδειξη. Πρώτα θα θεωρήσουμε την περίπτωση $d = n$. Ξέρουμε ότι

$$G = \{1, g, ..., g^{n-1}\}$$

για κάποιο g. Χρησιμοποιώντας το Θεώρημα 7.17(2), έχουμε ότι

$$|g^i| = n \Leftrightarrow \mu\kappa\delta(i, n) = 1.$$

Άρα το πλήθος των στοιχείων της G τάξης n είναι $\varphi(n)$.
Θεωρούμε τώρα τυχαίο θετικό διαιρέτη d του n. Κάθε στοιχείο της G τάξης d παράγει κυκλική υποομάδα της G τάξης d. Όμως από το Θεώρημα 9.14(2), η G διαθέτει μοναδική τέτοια υποομάδα, έστω G_d. Άρα όλα τα στοιχεία τάξης d της G περιέχονται στη G_d. Συνεπώς το πλήθος των στοιχείων τάξης d της G ισούται με το πλήθος των στοιχείων τάξης d της κυκλικής G_d. Από το πρώτο μέρος της απόδειξης, αυτό το πλήθος ισούται με $\varphi(d)$. □

Παραδείγματα 9.16.

(1) Έστω $G =< a >$ κυκλική τάξης 120 και $H =< a^{636} >$. Βρείτε τον ελάχιστο θετικό ακέραιο m με $a^m \in H$. Βρείτε τους γεννήτορες της H.
Καθώς η G είναι κυκλική, ξέρουμε ότι για κάθε διαιρέτη d της $|G|$ υπάρχει μοναδική υποομάδα της G τάξης d και αυτή είναι η $< a^{\frac{n}{d}} >$. Η τάξη της H ισούται με την τάξη του a^{636}, οπότε $|H| = \frac{120}{\mu\kappa\delta(120,636)} = 10$. Άρα $H = \{1, a^{12}, a^{24}, ..., a^{108}\}$ και $m = 12$.

Για να βρούμε τους γεννήτορες της H θέλουμε ισοδύναμα να βρούμε τα στοιχεία της H που έχουν τάξη ίση με $|H| = 10$. Για $i = 0, 1, ..., 9$, έχουμε

$$10 = |a^{12i}| = \frac{120}{\mu\kappa\delta(120, 12i)} = \frac{10}{\mu\kappa\delta(10, i)} \Leftrightarrow i = 1, 3, 7, 9.$$

Συνεπώς οι γεννήτορες της H είναι $a^{12}, a^{36}, a^{84}, a^{108}$.

(2) Έστω $\sigma = (12345)(4567) \in S_7$ και $G =< \sigma >$. Αληθεύει ότι η G περιέχει υποομάδα ισόμορφη με τη $U(\mathbb{Z}_{12})$; Με τη $U(\mathbb{Z}_5)$;
Έχουμε $= \{1, 5, 7, 11\}$ και εύκολα επαληθεύεται ότι κάθε στοιχείο της $U(\mathbb{Z}_{12})$ έχει τάξη 1 ή 2, πράγμα που σημαίνει ότι η $U(\mathbb{Z}_{12})$ δεν είναι κυκλική. Από την άλλη μεριά, ξέρουμε ότι κάθε υποομάδα κυκλικής είναι κυκλική. Συνεπώς η απάντηση στο πρώτο ερώτημα είναι αρνητική.
Για το δεύτερο ερώτημα, βρίσκουμε (κατά τα γνωστά) την ανάλυση σε γινόμενο ξένων κύκλων $\sigma = (1234)(567)$. Άρα $|G| = |\sigma| = 12$. Ξέρουμε ότι η ομάδα $U(\mathbb{Z}_5)$ είναι κυκλική τάξης 4 (Θεώρημα 8.14). [Φυσικά αυτό αποδεικνύεται στην συγκεκριμένη περίπτωση και με άμεσο υπολογισμό τάξεων, για παράδειγμα, η τάξη του $2 \in U(\mathbb{Z}_5)$ είναι 4]. Επειδή $4|12$, από το Θεώρημα 9.14(2), η απάντηση στο δεύτερο ερώτημα είναι καταφατική.

(3) Έστω G κυκλική ομάδα τάξης $n^5 - n$, $n > 1$. Δείξτε ότι υπάρχει $H \leq G$ με $|H| = 30$.

Επειδή η G είναι κυκλική, αρκεί να δείξουμε ότι $30 \mid |G|$, δηλαδή $30 \mid n^5 - n$. Πράγματι, επειδή $30 = 2 \cdot 3 \cdot 5$ και οι $2, 3, 5$ είναι ανά δύο σχετικά πρώτοι αρκεί να δείξουμε ότι

$$2 \mid n^5 - n, \;\; 3 \mid n^5 - n, \;\; 5 \mid n^5 - n.$$

Προφανώς $2 \mid n^5 - n$. Εφαρμόζοντας δύο φορές το μικρό θεώρημα του Fermat παίρνουμε την $3 \mid n^5 - n$ $(n^5 = n^3 n^2 \equiv nn^2 \equiv n^3 \equiv n \mod 3)$. Τέλος από το μικρό θεώρημα του Fermat για $p = 5$ παίρνουμε την $5 \mid n^5 - n$.

(4) Για κάθε θετικό ακέραιο n θεωρούμε το δακτύλιο $R_n = \dfrac{\mathbb{Z}_2[x]}{< (x+1)^n >}$ και την ομάδα $G_n = U(R_n)$. Θα δείξουμε τα εξής.
   i) $|G_n| = 2^{n-1}$.
   ii) Η G_3 είναι κυκλική.
   iii) Η G_4 δεν είναι κυκλική.

i) Πράγματι, συμβολίζοντας το ιδεώδες $< (x+1)^n >$ του $\mathbb{Z}_2[x]$ με I έχουμε ότι ένα στοιχείο $f(x)+I$ του R_n είναι αντιστρέψιμο, σύμφωνα με το Θεώρημα 6.6, αν και μόνο αν

$$\mu\kappa\delta((x+1)^n, f(x)) = 1 \Leftrightarrow \mu\kappa\delta(x+1, f(x)) = 1$$
$$\Leftrightarrow f(1) \neq 0 \Leftrightarrow f(1) = 1.$$

Από την Πρόταση 6.5, ξέρουμε ότι κάθε στοιχείο του R_n έχει μοναδική παράσταση της μορφής $a_n x^n + ... + a_1 x + a_0 + I, a_i \in \mathbb{Z}_2$. Από αυτό έπεται ότι το πλήθος των $f(x)+I$ που ικανοποιούν $f(1) = 1$ είναι 2^{n-1}.

ii) Επειδή $|G_3| = 4$, για να δείξουμε ότι η G_3 είναι κυκλική, αρκεί να δείξουμε ότι υπάρχει $g \in G$ με $g^2 \neq 1$, διότι τότε η τάξη του g, που διαιρεί το 4 σύμφωνα με την Πρόταση 8.11, θα είναι 4. Μια επιλογή για το g είναι $g = x + I$, καθώς $g^2 = x^2 + I \neq I$ αφού το $(x+1)^3$ δεν διαιρεί το x^2 στο $\mathbb{Z}_2[x]$.

iii) Θα δείξουμε ότι η G_4 έχει περισσότερα του ενός στοιχείου τάξης 2 και επομένως δεν είναι κυκλική λόγω της Πρότασης 9.15. Έστω $a = x^2 + I \in G_4$ και $b = x^3 + x + 1 + I \in G_4$. Είναι σαφές ότι $a \neq 1_{G_4}$ καθώς το $(x+1)^4$ δεν διαιρεί το x^2 στο $\mathbb{Z}_2[x]$. Έχουμε

$$a^2 = x^4 + I = 1 + I = 1_{G_4},$$

καθώς από το όνειρο του πρωτοετή, $I =< (x+1)^4 >=< x^4 + 1 >$. Άρα η τάξη του a είναι 2. Με παρόμοιο τρόπο έπεται ότι η τάξη του b είναι επίσης 2.

Ασκήσεις Κεφαλαίου 9

Ομάδα1: 1, 4, 6, 14, 15, 17, 23.
Ομάδα2: 2, 3, 5, 7-13, 16, 18, 20, 22, 24-26, 28.
Ομάδα3:19, 21, 27.

1. Αποδείξτε την Πρόταση 9.9.
2. Στις ακόλουθες περιπτώσεις εξετάστε αν οι ομάδες G, H είναι ισόμορφες.
   i) $G = \mathbb{Z}$ και $H = \mathbb{Z}_n, n > 0$.
   ii) $G = 2\mathbb{Z}$ και $H = 3\mathbb{Z}$.
   iii) $G = \mathbb{Z}$ και $H = \mathbb{Q}$.
   iv) $G = \mathbb{R}^*$ και $H = \mathbb{C}^*$.
   v) $G = \mathbb{R} \times \mathbb{R}$ και $H = \mathbb{C}$.
   vi) $G = \mathbb{R}$ και $H = (\mathbb{R}_{>0}, \cdot)$.
3. Έστω V η ομάδα συμμετριών του σχήματος Η. Η V είναι γνωστή ως η ομάδα του Klein.
   i) Δείξτε ότι $V \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
   ii) Δείξτε ότι η A_4 περιέχει υποομάδα ισόμορφη με τη V.
   iii) Αληθεύει ότι υπάρχει ομάδα G με $G \times V \simeq A_4$;
   iv) Αληθεύει ότι υπάρχει ομάδα G με $G \times V \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$;
4. Θεωρούμε κανονικό κυρτό εξάγωνο που οι κορυφές του έχουν χρωματισθεί εναλλάξ μπλε και κόκκινο. Ποια είναι η υποομάδα των συμμετριών του εξαγώνου που διατηρεί το χρωματισμό;
5. Δείξτε ότι για κάθε περιττό m οι ομάδες $U(\mathbb{Z}_m), U(\mathbb{Z}_{2m})$ είναι ισόμορφες.
6. Είναι σωστό ότι μια ομάδα είναι κυκλική αν κάθε γνήσια υποομάδα της είναι κυκλική;
7. Έστω $\varphi : G \to H$ ομομορφισμός πεπερασμένων ομάδων.
   i) Δείξτε ότι για κάθε $g \in G$, $|\varphi(g)| \mid |g|$.
   ii) Δείξτε ότι αν η φ είναι επί και η H έχει στοιχείο τάξης m, τότε η G έχει στοιχείο τάξης m.
   iii) Δείξτε ότι αν $\mu\kappa\delta(|G|, |H|) = 1$, τότε $\varphi(g) = 1_H$ για κάθε $g \in G$.
   iv) Έστω $G = S_6$ και $H = S_3$. Δείξτε ότι $\sigma \in \ker\varphi$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$.
8. Έστω $\varphi : \mathbb{Z}_{24} \to \mathbb{Z}_{20},\ \varphi([m]_{24}) = [5m]_{20}$. Δείξτε τα ακόλουθα.
   i) Η φ είναι καλώς ορισμένη.
   ii) Η φ είναι ομομορφισμός ομάδων.
   iii) $\ker\varphi =< [4]_{24} >$.
   iv) $\mathrm{Im}\varphi =< [5]_{20} >$.
9. Να βρεθούν όλοι οι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}$. Ποιοι από αυτούς είναι
   i) μονομορφισμοί ομάδων;
   ii) επιμορφισμοί ομάδων;
   iii) ισομορφισμοί ομάδων;
   iv) ομομορφισμοί δακτυλίων;
10. Έστω $\varphi : \mathbb{Q} \to \mathbb{Q}$ ομομορφισμός ομάδων. Δείξτε ότι υπάρχει $x \in \mathbb{Q}$ με $\varphi(a) = ax$ για κάθε $a \in \mathbb{Q}$. Ποιοι από τους προηγούμενους ομομορφισμούς ομάδων είναι ομομορφισμοί δακτυλίων;
11. Έστω G, H πεπερασμένες κυκλικές ομάδες με τάξεις m, n αντίστοιχα.
    i) Δείξτε ότι το πλήθος των ομομορφισμών ομάδων $G \to H$ είναι ίσο με $\mu\kappa\delta(m, n)$.
    ii) Έστω $G = \mathbb{Z}_{24}$ και $H = \mathbb{Z}_{20}$. Βρείτε όλους τους ομομορφισμούς ομάδων $G \to H$.
12. Βρείτε για ποια n υπάρχει
    i) επιμορφισμός ομάδων $G \to S_n$, όπου G αβελιανή,
    ii) μονομορφισμός ομάδων $S_n \to G$, όπου G αβελιανή,

iii) μονομορφισμός ομάδων $\mathbb{Z}_n \to S_n$,
iv) μονομορφισμός ομάδων $\mathbb{Z}_6 \to S_n$.

13. Έστω $n > 0$.
i) Πόσοι ομομορφισμοί ομάδων $\mathbb{Z}_n \to \mathbb{Z}$ υπάρχουν;
ii) Πόσοι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}_n$ υπάρχουν; Πόσοι από αυτούς είναι επί;

14. Δείξτε ότι η ομάδα $G = \{2^m \cdot 3^n \in \mathbb{Q} : m, n \in \mathbb{Z}\}$ με πράξη τον πολλαπλασιασμό είναι ισόμορφη με την ομάδα $\mathbb{Z} \times \mathbb{Z}$.

15. Δείξτε ότι η $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\varphi(x, y) = 28x + 49y$ είναι ομομορφισμός ομάδων. Ποια είναι η $\mathrm{Im}\varphi$;

16. $\star$ Έστω G μια πεπερασμένη κυκλική ομάδα και έστω $H, K \leq G$. Πόσα στοιχεία έχει η ομάδα $H \cap K$;

17. Έστω G κυκλική ομάδα τάξης 100, $G =< a >$
i) Αληθεύει ότι $< a^{28} >=< a^{36} >$;
ii) Βρείτε έναν γεννήτορα της ομάδας $< a^{22} > \cap < a^{55} >$.

18. Βρείτε όλες τις υποομάδες της ομάδας $G = \left\{ \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix} \in GL_2(\mathbb{Z}_{18}) \right\}$.

19. Ένας **αυτομορφισμός** μιας ομάδας G είναι ένας ισομορφισμός $G \to G$. Δείξτε ότι το σύνολο $Aut(G)$ των αυτομορφισμών της G είναι ομάδα με πράξη τη σύνθεση συναρτήσεων. Στη συνέχεια δείξτε τα εξής.
i) Η $Aut(\mathbb{Z})$ έχει τάξη 2.
ii) $Aut(\mathbb{Q}) \simeq \mathbb{Q}^*$.
iii) Για κάθε $n > 1$, $Aut(\mathbb{Z}_n) \simeq U(\mathbb{Z}_n)$.

20. Αληθεύει ότι αν $\varphi : S_4 \to G$ είναι ομομορφισμός ομάδων τέτοια ώστε 7 διαφορετικές άρτιες μεταθέσεις έχουν εικόνα το 1_G , τότε κάθε άρτια μετάθεση έχει εικόνα το 1_G;

21. Έστω G ομάδα. Δείξτε τα εξής.
i) Αν η G είναι αβελιανή, τότε η απεικόνιση $x \mapsto x^{-1}$ είναι αυτομορφισμός της G.
ii) Για κάθε $g \in G$, η απεικόνιση $x \mapsto g^{-1}xg$ είναι αυτομορφισμός της G.
iii) ≀ Αν $|G| > 2$, τότε υπάρχει μη τετριμμένος αυτομορφισμός $G \to G$.

22. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.
i) Υπάρχει ομάδα G ώστε $G \times \mathbb{Z}_4 \simeq \mathbb{Z}_{40} \times \mathbb{Z}_2$.
ii) Αν μια ομάδα έχει τουλάχιστον δύο στοιχεία τάξης 2, τότε δεν είναι κυκλική.

23. Έστω m περιττός ακέραιος. Δείξτε ότι η απεικόνιση $U(\mathbb{Z}_{2^n}) \to U(\mathbb{Z}_{2^n}), x \mapsto x^m$, είναι ισομορφισμός ομάδων.

24. Αληθεύει ότι για κάθε θετικό ακέραιο n το πλήθος των ανά δύο μη ισόμορφων ομάδων τάξης n είναι πεπερασμένο; Αν ναι, δώστε ένα άνω φράγμα.

Στις ασκήσεις που ακολουθούν, βρίσκουμε όλους τους n για τους οποίους η ομάδα $U(\mathbb{Z}_n), n > 1$, είναι κυκλική. Το τελικό αποτέλεσμα είναι ένα φημισμένο θεώρημα του Gauss:

Η ομάδα $U(\mathbb{Z}_n), n > 1$, είναι κυκλική αν και μόνο αν $n = 2, 4, p^m, 2p^m$, όπου p περιττός πρώτος. Ο παρακάτω τρόπος απόδειξης είναι αυτός του άρθρου D.R. Guichard, When is $U(\mathbb{Z}_n)$ cyclic? An algebraic approach, Mathematics Magazine 72(2) (1999), 139-142.

25. Δείξτε ότι η ομάδα $U(\mathbb{Z}_n)$ δεν είναι κυκλική αν το n διαιρείται από 2 διαφορετικούς περιττούς πρώτους αριθμούς.
Υπόδειξη: Έχουμε $n = ab$, όπου $a, b > 2$ και a, b σχετικά πρώτοι. Από το Παράδειγμα 9.2(2) έχουμε ισομορφισμό $U(\mathbb{Z}_{ab}) \simeq U(\mathbb{Z}_a) \times U(\mathbb{Z}_b)$.

26. Δείξτε ότι για κάθε $m \geq 3$, η ομάδα $U(\mathbb{Z}_{2^m})$ δεν είναι κυκλική.
Υπόδειξη: Αρκεί να δείξουμε ότι η $U(\mathbb{Z}_{2^m})$ έχει τουλάχιστον δύο στοιχεία τάξης 2. Δείξτε ότι τα στοιχεία $[-1]$ και $[2^{m-1} + 1]$ είναι διαφορετικά και έχουν τάξη 2.

27. ≀ Έστω p περιττός πρώτος. Στην άσκηση αυτή δείχνουμε ότι οι ομάδες $U(\mathbb{Z}_{p^m})$, $m \geq 2$, είναι κυκλικές χρησιμοποιώντας ότι η ομάδα $U(\mathbb{Z}_p)$ είναι κυκλική, βλ. Θεώρημα 8.14.
    i) Έστω $[a]_p$ ένας γεννήτορας της κυκλικής ομάδας $U(\mathbb{Z}_p)$. Δείξτε ότι τουλάχιστον ένα από τα στοιχεία $[a]_{p^2}, [a+p]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$. Άρα η ομάδα $U(\mathbb{Z}_{p^2})$ είναι κυκλική.
    ii) Δείξτε ότι αν το $[b]_{p^2}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^2})$, τότε το $[b]_{p^m}$ είναι γεννήτορας της $U(\mathbb{Z}_{p^m})$, $m \geq 3$. Άρα η ομάδα $U(\mathbb{Z}_{p^m})$ είναι κυκλική.
28. Η $U(\mathbb{Z}_n), n > 1$ είναι κυκλική αν και μόνο αν $n = 2, 4, p^m, 2p^m$, όπου p περιττός πρώτος.
29. ≀ Έστω G ομάδα με τάξη πρώτο αριθμό p. Πόσοι ισομορφισμοί ομάδων $G \times G \to G \times G$ υπάρχουν ;
30. Θεωρήστε τις επικαλύψεις του επιπέδου που αντιστοιχούν στα τρία σχήματα στο εξώφυλλο αυτών των σημειώσεων. Τι μπορείτε να πείτε για τις αντίστοιχες ομάδες συμμετριών;

Υποδείξεις Ασκήσεων Κεφαλαίου 9

1.

2. *Λύση.*
   i) Όχι. Η μία είναι άπειρη, η άλλη πεπερασμένη.
   ii) Ναι. Και οι δύο είναι άπειρες κυκλικές, Πόρισμα 9.13.
   iii) Όχι. Η μία είναι κυκλική, η άλλη δεν είναι.
   Ας δείξουμε ότι πράγματι η ομάδα $\mathbb{Q}$ δεν είναι κυκλική. Αν ήταν κυκλική, τότε θα υπήρχε $a/b \in \mathbb{Q}$, $(a, b \in \mathbb{Z})$ τέτοιος ώστε για κάθε $c \in \mathbb{Q}$ υπάρχει $m \in \mathbb{Z}$ με $c = m(a/b)$. Επιλέγοντας $c = 1/d$, όπου d ακέραιος που δεν διαιρεί το b, θα είχαμε $b = dma$, αδύνατο.
   iv) Όχι. Η μία έχει ένα στοιχείο τάξης 3, η άλλη έχει τρία στοιχεία τάξης 3.
   v) Ναι. Η απεικόνιση $(a, b) \mapsto a + bi$ είναι ισομορφισμός ομάδων.
   vi) Ναι. Η εκθετική απεικόνιση $x \mapsto e^x$ είναι ισομορφισμός ομάδων. Βλ. και το Παράδειγμα 9.2(6).

3. *Υποδείξεις.* Παρατηρούμε ότι η ομάδα $V = S(M)$ που είδαμε στο Παράδειγμα 7.2(4), έχει τάξη 4 και είναι αβελιανή.
   i) Με το συμβολισμό του Παραδείγματος 7.2(4), δείξτε ότι η απεικόνιση
   $$1 \mapsto (0,0),\ \rho_1 \mapsto (1,0)\ \rho_2 \mapsto (0,1),\ \sigma \mapsto (1,1)$$
   είναι ισομορφισμός ομάδων. Για την απόδειξη χρησιμοποιήστε τις σχέσεις που αναγράφονται στο ανωτέρω παράδειγμα.
   ii) Στο Παράδειγμα 7.2(4) είχαμε ότι $S(M) = \{1, \rho_1, \rho_2, \sigma\}$. Τοποθετώντας τους αριθμούς 1,2,3,4 στις κορυφές όπως ακριβώς στο παράδειγμα, δείξτε ότι το στοιχείο ρ_1 (ανάκλαση ως προς τον κατακόρυφο άξονα) αντιστοιχεί στη μετάθεση κορυφών $(12)(34)$. Κάνοντας το ίδιο για όλα τα στοιχεία της $S(M)$ δίνει το εξής υποσύνολο της A_4,
   $$H = \{1, (12)(34), (14)(23), (13)(24\}).$$
   Εύκολα αποδεικνύεται ότι το πεπερασμένο σύνολο H είναι κλειστό υποσύνολο της ομάδας A_4 και άρα υποομάδα σύμφωνα με την Πρόταση 8.4. Με παρόμοιο επιχείρημα με το (i) προκύπτει ότι $H \simeq V$.
   iii) Όχι. Διότι αν είχαμε $G \times V \simeq A_4$, τότε λαμβάνοντας τάξεις θα είχαμε $|G| \cdot |V| = |A_4| = 12$, οπότε η $|G| = 3$ που είναι πρώτος, και άρα η G θα ήταν αβελιανή σύμφωνα με το Πόρισμα 8.10. Τότε και η $G \times V$ θα ήταν αβελιανή, δηλαδή η A_4 θα ήταν αβελιανή, αδύνατο.
   iv) Όχι. Διότι αν είχαμε $G \times V \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$, τότε λαμβάνοντας τάξεις θα είχαμε $|G| = 2$. Τότε κάθε στοιχείο της ομάδας $G \times V$ θα είχε τάξη 1 ή 2. Όμως η ομάδα $\mathbb{Z}_4 \times \mathbb{Z}_2$ διαθέτει στοιχείο τάξης 4, για παράδειγμα το $(1, 0)$.

4. *Απάντηση.* Είναι ισόμορφη με τη D_3 (την ομάδα συμμετριών του μπλε τριγώνου, ή ισοδύναμα, του κόκκινου τριγώνου).

5. *Λύση.* Επειδή οι $2, m$ είναι σχετικά πρώτοι, από το Παράδειγμα 9.2(2) έχουμε
   $$U(\mathbb{Z}_{2m}) \simeq U(\mathbb{Z}_2) \times U(\mathbb{Z}_m).$$
   Όμως $U(\mathbb{Z}_2) = \{1\}$. Άρα $U(\mathbb{Z}_{2m}) \simeq \{1\} \times U(\mathbb{Z}_m) \simeq U(\mathbb{Z}_m)$.

6. *Λύση.* Όχι. Ένα αντιπαράδειγμα είναι η ομάδα S_3. Αυτή έχει τάξη 6 και άρα από το θεώρημα του Lagrange, κάθε γνήσια υποομάδα της έχει τάξη 1 ή 2 ή 3. Άρα κάθε γνήσια υποομάδα της είναι κυκλική από το Πόρισμα 8.10. Όμως η S_3 δεν είναι κυκλική καθώς δεν είναι αβελιανή.

7. *Λύση.* i) Έστω $|g| = n$ $(n < \infty$ αφού $|G| < \infty)$. Τότε
   $$g^n = 1_G \Rightarrow \varphi(g^n) = \varphi(1_G) = 1_H \Rightarrow \varphi(g)^n = 1_H \Rightarrow |\varphi(g)| \mid n.$$

ii) Έστω $h \in H$. Αφού η φ είναι επί υπάρχει $g \in G$ ώστε $h = \varphi(g)$. Από το πρώτο ερώτημα έπεται ότι $|h| \mid |g|$. Έστω $|g| = m|h|,\ m \in \mathbb{Z}_{>0}$. Για το g^m έχουμε

$$|g^m| = \frac{|g|}{\mu\kappa\delta(|g|, m)} = \frac{|g|}{m} = |h|.$$

iii) Έστω $g \in G$. Τότε από το πρώτο ερώτημα παίρνουμε $|\varphi(g)| \mid |g|$. Επειδή $|g| \mid |G|$, έπεται ότι $|\varphi(g)| \mid |G|$. Επίσης ισχύει $|\varphi(g)| \mid |H|$. Άρα

$$|\varphi(g)| \mid \mu\kappa\delta(|G|, |H|) \Rightarrow |\varphi(g)| \mid 1 \Rightarrow \varphi(g) = 1_H.$$

iv) Από την ανάλυση της σ σε γινόμενο ξένων κύκλων έχουμε $\sigma = (12345)$. Άρα $|\sigma| = 5$. Από το πρώτο παίρνουμε ότι $|\varphi(\sigma)| \mid 5$. Αλλά, $|\varphi(\sigma)| \mid |S_3| \Rightarrow |\varphi(\sigma)| \mid 6$. Επομένως $|\varphi(\sigma)| = 1 \Rightarrow \varphi(\sigma) = 1$.

8. *Λύση.* i) Έστω $[m]_{24} = [m']_{24}$. Τότε

$$24 \mid m - m' \Rightarrow 4 \mid m - m' \Rightarrow 20 \mid 5(m - m') \Rightarrow [5m]_{20} = [5m']_{20}.$$

ii) Έχουμε $\varphi([a]_{24} + [b]_{24}) = \varphi([a + b]_{24}) = [5(a + b)]_{20} = [5a]_{20} + [5b]_{20} = \varphi([a]_{24}) + \varphi([b]_{24})$.

iii) Ο πυρήνας της φ είναι

$\ker\varphi = \{[a]_{24} : [5a]_{20}) = [0]_{20}\} = \{[a]_{24} : 20|5a\} = \{[a]_{24} : 4|a\} =< [4]_{24} > .$

iv) Έχουμε $\mathrm{Im}\varphi = \{[5m]_{20} \in \mathbb{Z}_{20} : m \in \mathbb{Z}\} =< [5]_{20} > .$

9. *Λύση.* Έστω $\varphi : \mathbb{Z} \to \mathbb{Z}$ ομομορφισμός ομάδων. Ξέρουμε ότι $\varphi(m) = m\varphi(1)$, για κάθε $m \in \mathbb{Z}$. Άρα αν $\varphi : \mathbb{Z} \to \mathbb{Z}$ ομομορφισμός ομάδων υπάρχει $a \in \mathbb{Z}$ ώστε $\varphi(m) = ma$. Αντίστροφα, έστω $a \in \mathbb{Z}$. Ορίζουμε

$$\varphi_a : \mathbb{Z} \to \mathbb{Z},\ \ \varphi_a(m) = ma.$$

Τότε $\varphi_a(m+n) = (m+n)a = ma+na = \varphi_a(m)+\varphi_a(n)$, δηλαδή ο φ_a είναι ομομορφισμός ομάδων. Δείξαμε ότι οι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}$ είναι ακριβώς οι φ_a, όπου $a \in \mathbb{Z}$.

i) φ_a μονομορφισμός $\Leftrightarrow$ $\ker\varphi_a = \{0\}$ $\Leftrightarrow$ $a \neq 0$.
ii) φ_a επιμορφισμός $\Leftrightarrow$ $\mathrm{Im}\varphi_a = \mathbb{Z}$ $\Leftrightarrow$ $< a >= \mathbb{Z}$ $\Leftrightarrow$ $a = 1$ ή $a = -1$.
iii) φ_a ισομορφισμός $\Leftrightarrow$ φ_a μονομορφισμός και επιμορφισμός $\Leftrightarrow$ $a = 1$ ή $a = -1$.
iv) Παρατηρούμε ότι

$$\varphi_a(1 \cdot 1) = \varphi_a(1)\varphi_a(1) \Rightarrow a = a^2 \Rightarrow a = 0 \ \text{ ή } \ a = 1.$$

Συνεπώς, αν φ_a είναι ομομορφισμός δακτυλίων, τότε $a = 0$ ή $a = 1$. Αντίστροφα, αν $a = 0$ ή $a = 1$ η φ , τότε η είναι φ_a είναι μηδενική απεικόνιση ή η ταυτοτική που είναι ασφαλώς ομομορφισμοί δακτυλίων.

10. *Λύση.* Έστω $m, n \in \mathbb{Z}, n \neq 0$, και $\varphi : \mathbb{Q} \to \mathbb{Q}$ ομομορφισμός ομάδων. Τότε

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

και επομένως $\varphi(\frac{m}{n}) = m\varphi(\frac{1}{n}) = m\frac{1}{n}\varphi(1) = \frac{m}{n}\varphi(1)$. Θέτοντας $x = \varphi(1)$ έχουμε ότι $\varphi(a) = ax$ για κάθε $a \in \mathbb{Q}$.
Ο παραπάνω φ είναι ομομορφισμός δακτυλίων αν και μόνο για κάθε $a, b \in \mathbb{Q}$,

$$\varphi(ab) = \varphi(a)\varphi(b) \Leftrightarrow abx = abx^2 \Leftrightarrow x^2 = x \Leftrightarrow x = 0, 1.$$

11. *Λύση.* i) Έστω $G =< g >, H =< h >$ με αντίστοιχες τάξεις m, n και έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Έχουμε $\varphi(g) = h^a,\ \ 0 \leq a < n$ αφού $H = \{1, h, h^2, \ldots, h^{n-1}\}$. Ξέρουμε ότι $g^m = 1_G$. Άρα $\varphi(g)^m = \varphi(g^m) = \varphi(1_G) = 1_H \Rightarrow h^{am} = 1_H$. Επομένως $n \mid am$. Έστω $d = \mu\kappa\delta(m, n)$. Τότε $\frac{n}{d} \mid a\frac{m}{d}$. Επειδή οι $\frac{n}{d}, \frac{m}{d}$ είναι σχετικά πρώτοι παίρνουμε $\frac{n}{d} \mid a$. Άρα

$$a = \frac{n}{d} \cdot i,\ \ i = 0, 1, 2, \ldots, d - 1. \tag{9.1}$$

Για κάθε $i = 0, 1, 2, \ldots, (d-1)$ ορίζουμε την απεικόνιση

$$\varphi_i(g^k) = h^{\frac{n}{d}ik}, \ \ (k \in \mathbb{Z}).$$

• Η φ_i είναι καλώς ορισμένη. Πράγματι, έστω $g^k = g^{k'}$. Τότε

$$m \mid k - k' \Rightarrow m\frac{n}{d} \mid \frac{n}{d}i(k-k') \Rightarrow \frac{m}{d}n \mid \frac{n}{d}i(k-k') \Rightarrow n \mid \frac{n}{d}i(k-k').$$

Επομένως $h^{\frac{n}{d}ik} = h^{\frac{n}{d}ik'}$.

• Εύκολα επαληθεύεται ότι η φ_i είναι ομομορφισμός ομάδων.

• $\varphi_i \neq \varphi_j$ για κάθε $i \neq j$, $0 \leq i, j \leq d-1$. Πράγματι, έστω $\varphi_i = \varphi_j$, $0 \leq i, j \leq d-1$. Τότε

$$\varphi_i(g) = \varphi_j(g) \Rightarrow h^{\frac{n}{d}i} = h^{\frac{n}{d}\xi} \Rightarrow n \mid \frac{n}{d}(i-j) \Rightarrow i = j,$$

αφού $0 \leq i, j \leq d-1$.

• Κάθε ομομορφισμός ομάδων $G \to H$ είναι ένας από τους φ_i. Πράγματι, έστω $\varphi_i : G \to H$ ομομορφισμός ομάδων. Τότε από την (9.1), $\varphi = \varphi_i$ για κάποιο $i = 0, 1 \cdots, d-1$, αφού

$$\varphi(g^k) = h^{ak} = h^{n/d \cdot ik}.$$

ii) Με τον συμβολισμό της λύσης του πρώτου ερωτήματος, έχουμε $m = 24, n = 20, d = \mu\kappa\delta(24, 20) = 4, \frac{n}{d} = \frac{20}{4} = 5$. Επίσης $i = 0, 1, 2, 3$. Σύμφωνα με την λύση, υπάρχουν ακριβώς 4 ομομορφισμοί ομάδων $\mathbb{Z}_{24} \to \mathbb{Z}_{20}$, οι εξής.

$$\begin{aligned} \varphi_0 &: \quad \varphi_0([k]_{24}) = [0]_{20} \\ \varphi_1 &: \quad \varphi_1([k]_{24}) = [5k]_{20} \\ \varphi_2 &: \quad \varphi_2([k]_{24}) = [10k]_{20} \\ \varphi_3 &: \quad \varphi_3([k]_{24}) = [15k]_{20} \end{aligned}$$

Σημείωση. Στην άσκηση 8 είχαμε $\varphi = \varphi_1$.

12. *Λύση.*

Παρατήρηση. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων.

1. Αν φ επί και G αβελιανή, τότε η H είναι αβελιανή.
2. Αν φ 1-1 και H αβελιανή, τότε η ομάδα G είναι αβελιανή.

Ας δείξουμε το 1. Έστω $h, h' \in H$. Αφού η G είναι επί, υπάρχουν $g, g' \in G$ με $h = \varphi(g)$, $h' = \varphi(g')$. Επομένως

$$hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g')\varphi(g) = h'h.$$

Επομένως η H είναι αβελιανή.

i) Από την παρατήρηση 1, αν $\varphi : G \to S_n$ επιμορφισμός και G αβελιανή τότε S_n αβελιανή. Άρα $n = 1, 2$.

ii) Από την παρατήρηση 2, η S_n είναι αβελιανή, άρα $n = 1, 2$.

iii) Για κάθε n επαληθεύεται ότι η απεικόνιση $\varphi : \mathbb{Z}_n \to S_n, [m] \mapsto \sigma^m$,όπου $\sigma = (12 \cdots n)$, είναι καλά ορισμένη και μονομορφισμός ομάδων. Πράγματι,

$$[m] = [m'] \Leftrightarrow m \equiv m' \mod n \Leftrightarrow \sigma^m = \sigma^{m'},$$

όπου η δεύτερη ισοδυναμία έπεται από το γεγονός ότι $|\sigma| = n$. Για κάθε $[m_1], [m_2] \in \mathbb{Z}_n$ είναι

$$\varphi([m_1] + [m_2]) = \varphi([m_1 + m_2]) = \sigma^{m_1+m_2} = \sigma^{m_1}\sigma^{m_2} = \varphi([m_1])\varphi([m_2]).$$

Το πρώτο επιχείρημα δείχνει ότι η φ είναι μονομορφισμός (λόγω των ισοδυναμιών).

iv) Έστω $\varphi : \mathbb{Z}_6 \to S_n$ μονομορφισμός ομάδων. *Παρατήρηση.* Εύκολα επαληθεύεται ότι αν $\psi : G \to H$ είναι μονομορφισμός ομάδων, τότε τα στοιχεία g και $\psi(g)$ έχουν την ίδια τάξη, αφού $g^n = 1_G \Leftrightarrow \psi(g^n) = \psi(1_G) \Leftrightarrow \psi(g)^n = 1_H$. Έστω $\varphi : \mathbb{Z}_6 \to S_n$ μονομορφισμός ομάδων. Επειδή η ομάδα $\mathbb{Z}_6$ περιέχει στοιχείο τάξης 6, το ίδιο συμβαίνει με την ομάδα S_n από την παρατήρηση. Εύκολα επαληθεύεται θεωρώντας εκπ μηκών κύκλων σε γινόμενα ξένων κύκλων, ότι η S_n, $n \leq 4$, δεν έχει στοιχείο τάξης 6. Επομένως λαμβάνουμε την αναγκαία συνθήκη $n \geq 5$.

Η S_n, $n \geq 5$, έχει στοιχείο σ τάξης 6 (για παράδειγμα το $(123)(45)$). Εύκολα επαληθεύεται (όπως στο προηγούμενο υποερώτημα) ότι η απεικόνιση $\mathbb{Z}_6 \to S_n, [m] \mapsto \sigma^m$, είναι μονομορφισμός ομάδων. Συνεπώς η απάντηση είναι $n \geq 5$.

13. i) *Λύση.* Έστω $\varphi : \mathbb{Z}_n \to \mathbb{Z}$ ομομορφισμός ομάδων. Τότε αφού

$$0 = \varphi([0]) = \varphi(n[1]) = n\varphi([1]) \Rightarrow \varphi([1]) = 0.$$

Άρα για κάθε $[a] \in \mathbb{Z}_n$ έχουμε $\varphi([a]) = \varphi(a[1]) = a\varphi([1]) = 0$. Συνεπώς υπάρχει μοναδικός ομομορφισμός ομάδων $\varphi : \mathbb{Z}_n \to \mathbb{Z}$, ο μηδενικός . ii) *Υπόδειξη:* Αν $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ είναι ομομορφισμός ομάδων, τότε ο φ καθορίζεται από την τιμή στο 1, αφού για κάθε $m \in \mathbb{Z}$ είναι $\varphi(m) = \varphi(1)$. *Απάντηση:* Οι ομομορφισμοί ομάδων $\mathbb{Z} \to \mathbb{Z}_n$ είναι οι $\varphi_i(m) = [im]$, όπου $i = 0, 1, ..., n-1$ Το ζητούμενο πλήθος των επιμορφισμών είναι ίσο με το πλήθος των προηγούμενων i που είναι αντιστρέψιμα $\bmod n$, δηλαδή ισούται με την τιμή της συνάρτησης του Euler στο n.

14. *Λύση.* Θεωρούμε την απεικόνιση,

$$\varphi : G \to \mathbb{Z} \times \mathbb{Z}, \;\; \varphi(2^m \cdot 3^n) = (m, n).$$

Η φ είναι καλώς ορισμένη. Πράγματι, έστω

$$2^m \cdot 3^n = 2^{m'} \cdot 3^{n'} \Rightarrow 2^{m-m'} = 3^{n'-n} \Rightarrow m = m', \; n = n' \Rightarrow (m, n) = (m', n').$$

Η φ είναι ομομορφισμός ομάδων. Πράγματι,

$$\begin{aligned} \varphi(2^m 3^n \cdot 2^{m'} 3^{n'}) &= \varphi(2^{m+m'} 3^{n+n'}) = (m + m', n + n') \\ &= (m, n) + (m', n') = \varphi(2^m 3^n)\varphi(2^{m'} 3^{n'}). \end{aligned}$$

Είναι σαφές ότι η φ είναι επί. Τέλος η φ είναι 1-1. Πράγματι,

$$\ker \varphi = \{2^m 3^n : (m, n) = (0, 0)\} = \{1\}.$$

Άρα $G \simeq \mathbb{Z} \times \mathbb{Z}$.

15. *Λύση.* Παρατηρούμε ότι

$$\begin{aligned} \varphi\left((x, y) + (x', y')\right) &= \varphi(x + x', y + y') \\ &= 28(x + x') + 49(y + y') \\ &= (28x + 49y) + (28x' + 49y') \\ &= \varphi(x, y) + \varphi(x', y'). \end{aligned}$$

Για την εικόνα έχουμε $\mathrm{Im}\varphi = \{28x + 49y : x, y \in \mathbb{Z}\} =< d >$, όπου $d = \mu\kappa\delta(28, 49) = 7$. Δηλαδή, $\mathrm{Im}\varphi =< 7 >= 7\mathbb{Z}$.

16. *Λύση.* Θα δείξουμε ότι $|H \cap K| = d$, όπου $d = \mu\kappa\delta(|H|, |K|)$.
Από το Θεώρημα 9.14 ξέρουμε ότι αν $m \mid n$, τότε υπάρχει μοναδική υποομάδα $H_m \leq G$ με $|H_m| = m$.
Επειδή $H \cap K \leq H$, από το θεώρημα του Lagrange έχουμε ότι $|H \cap K| \mid |H|$. Ομοίως $|H \cap K| \mid |K|$. Επομένως $|H \cap K| \mid \mu\kappa\delta(|H|, |K|)$. Άρα $H \cap K \leq H_d$, όπου $d = \mu\kappa\delta(m, n)$. Επειδή $d \mid |H|$ έχουμε $H_d \subseteq H$. Ομοίως $H_d \subseteq K$ και $H_d \subseteq H \cap K$. Τελικά $H \cap K = H_d$.

17. *Λύση.* (i) Αφού G κυκλική από το Θεώρημα 9.14 έχουμε ότι

$$\begin{aligned} < a^{28} > &= < a^{36} > \Leftrightarrow | < a^{28} > | = | < a^{36} > | \Leftrightarrow \\ \frac{100}{\mu\kappa\delta(100, 28)} &= \frac{100}{\mu\kappa\delta(100, 36)} \Leftrightarrow 25 = 25. \end{aligned}$$

Άρα αληθεύει ότι $< a^{28} >=< a^{36} >$.

(ii) Από την προηγούμενη άσκηση παίρνουμε, $| < a^{22} > \cap < a^{55} > | = \mu\kappa\delta(| < a^{22} > |, | < a^{55} > |)$. Όμως,

$$| < a^{22} > | = \frac{100}{\mu\kappa\delta(100, 22)} = 50 \quad \text{και} \quad | < a^{55} > | = \frac{100}{\mu\kappa\delta(100, 55)} = 20.$$

Επομένως $| < a^{22} > \cap < a^{55} > | = 10$. Τότε $< a^{22} > \cap < a^{55} >=< a^{\frac{100}{10}} >=< a^{10} >$.

18. *Λύση.* Θεωρούμε την απεικόνιση $\varphi : \mathbb{Z}_{18} \to G, \quad \varphi([m]) = \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix}$. Εύκολα επαληθεύεται ότι η φ είναι ισομορφισμός ομάδων. Επομένως $G \simeq \mathbb{Z}_{18}$ κυκλική τάξης 18. Άρα οι υποομάδες της G είναι οι
$$\left\{ \begin{pmatrix} [1] & [m] \\ [0] & [1] \end{pmatrix} \in G : [m] \in H \right\}, \text{ όπου } H \leq \mathbb{Z}_{18}.$$
Ξέρουμε ότι οι υποομάδες της κυκλικής ομάδας $\mathbb{Z}_{18}$ είναι οι ακόλουθες
$$H = \mathbb{Z}_{18}, \ <[2]>, <[3]>, <[6]>, <[9]>, <[0]> .$$

19. Οι i) και ii) έγιναν στις ασκήσεις (7) και (8) ουσιαστικά.
iii) *Υπόδειξη:* Παρατηρήστε αρχικά ότι κάθε ομομορφισμός ομάδων $\mathbb{Z}_n \to \mathbb{Z}_n$, είναι πολλαπλασιασμός με το $\varphi([1])$. Δείξτε ότι αν $\varphi \in Aut(\mathbb{Z}_n)$, τότε $\varphi([1]) \in U(\mathbb{Z}_n)$. Στη συνέχεια, δείξτε ότι η απεικόνιση $Aut(\mathbb{Z}_n) \to U(\mathbb{Z}_n), \varphi \mapsto \varphi([1])$, είναι ισομορφισμός ομάδων.

20. *Λύση.* Αληθεύει. Επειδή $|A_4| = 12$, από την υπόθεση έπεται ότι η υποομάδα $A_4 \cap \ker\varphi$ της A_4 έχει δείκτη στην A_4 μικρότερο του 2. Άρα $A_4 \cap \ker\varphi = A_4 \Rightarrow A_4 \subseteq \ker\varphi$.

21. *Υπόδειξη. iii)* Χρησιμοποιώντας τα προηγούμενα υποερωτήματα, δείξτε ότι μπορούμε να υποθέσουμε ότι κάθε στοιχείο της G διάφορο από το ουδέτερο έχει τάξη 2. Στη συνέχεια δείξτε ότι με την υπόθεση αυτή, η G είναι διανυσματικός χώρος υπεράνω του σώματος $\mathbb{Z}_2$. Αν $\dim G > 1$ βρείτε μια γραμμική απεικόνιση $G \to G$ διάφορη της ταυτοτικής.

22. Λύση. i) Έστω ότι υπάρχει τέτοια G. Τότε $|G \times \mathbb{Z}_4| = |\mathbb{Z}_{40} \times \mathbb{Z}_2|$, δηλαδή $|G| = 20$. Επομένως κάθε στοιχείο της $G \times \mathbb{Z}_4$ έχει τάξη ≤ 20 (αφού $4 \mid 20$). Αλλά το στοιχείο $([1]_{40}, [0]_2) \in \mathbb{Z}_{40} \times \mathbb{Z}_2$ έχει τάξη 40, το οποίο είναι άτοπο, αφού αν $\varphi : H \to K$ ισομορφισμός ομάδων τότε για κάθε $h \in H$, $|h| = |\varphi(h)|$.
ii)

23.

24. Αληθεύει. Για παράδειγμα, για τον πίνακα πολλαπλασιασμού της ομάδας υπάρχουν πεπερασμένου πλήθους δυνατότητες. Ένα άνω φράγμα είναι $(n!)^n$ καθώς κάθε γραμμή του πίνακα είναι μετάθεση των στοιχείων της ομάδας.

25. *Υπόδειξη.* Δείξτε ότι το πρόβλημα ισοδυναμεί με την εύρεση του πλήθους των πινάκων $A \in M_2(\mathbb{Z}_p)$ που ικανοποιούν $det(A) \neq 0$.
Η πρώτη γραμμή του A μπορεί να είναι οτιδήποτε εκτός από τη μηδενική, άρα έχουμε για αυτή $p^2 - 1$ επιλογές. Η δεύτερη μπορεί να είναι οποιαδήποτε εκτός από πολλαπλάσιο της πρώτης (δικαιολογήστε το), άρα $p^2 - p$ επιλογές για αυτή. Συνεπώς η απάντηση είναι $(p^2 - 1)(p^2 - p)$.

26.

27.

28.

29.

30. Είναι ισόμορφες ανά δύο.

Κανονικές υποομάδες, ομάδα πηλίκο

Στο κεφάλαιο αυτό των σημειώσεων εισάγουμε την έννοια της κανονικής υποομάδας και μελετάμε την ομάδα πηλίκο. Ως εφαρμογή αποδεικνύουμε το θεώρημα του Cauchy για αβελιανές ομάδες. Επίσης εξετάζουμε το εσωτερικό ευθύ γινόμενο υποομάδων.

Βασικά σημεία

- κανονικές υποομάδες
- ομάδα πηλίκο
- πρώτο θεώρημα ισομορφισμών
- εσωτερικό ευθύ γινόμενο υποομάδων

10.1. Κανονικές υποομάδες

Ξέρουμε ότι το σύνολο $\mathbb{Z}_n = \{[a] : a \in \mathbb{Z}\}$ είναι ομάδα με πράξη

$$\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n,\ ([a],[b]) \mapsto [a+b].$$

Έχουμε $[a] = \{a + kn : k \in \mathbb{Z}\} = a + n\mathbb{Z}$. Τότε η πράξη παίρνει τη μορφή

$$(a + n\mathbb{Z}, b + n\mathbb{Z}) \mapsto (a+b) + n\mathbb{Z}.$$

Ερώτηση. Έστω G ομάδα, $H \leq G$ και $G/H = \{aH : a \in G\}$. Αληθεύει ότι η αντιστοιχία

$$G/H \times G/H \to G/H,\ \ (aH, bH) \mapsto abH \tag{10.1}$$

καθιστά το σύνολο G/H ομάδα; Θα δούμε ότι η (10.1) δεν είναι γενικά απεικόνιση, αλλά στην περίπτωση που είναι απεικόνιση, τότε εφοδιάζει το σύνολο G/H με τη δομή ομάδας. Έτσι θα εξετάσουμε ισοδύναμες συνθήκες ώστε να είναι απεικόνιση.

Ορισμός 10.1. *Έστω G ομάδα, $S \subseteq G$ και $a, b \in G$. Θέτουμε $aSb = \{asb \in G : s \in S\}$.*

Παρατηρούμε ότι αν $b = 1_G$ και $S \leq G$, τότε έχουμε την κλάση aS της S στη G.

Πρόταση 10.2. *Έστω $H \leq G$. Τα ακόλουθα είναι ισοδύναμα.*
(1) *Η αντιστοιχία (10.1) είναι απεικόνιση.*
(2) *Για κάθε $g \in G$ ισχύει, $g^{-1}Hg \subseteq H$.*
(3) *Για κάθε $g \in G$ ισχύει, $g^{-1}Hg = H$.*
(4) *Για κάθε $g \in G$ ισχύει, $gH = Hg$.*

Απόδειξη. (1) $\Rightarrow$ (2). Έστω $a_1H = a_2H$ και $b_1H = b_2H$. Τότε $a_1b_1H = a_2b_2H$. Ισοδύναμα,

$$a_2^{-1}a_1 \in H \text{ και } b_2^{-1}b_1 \in H \Rightarrow b_2^{-1}a_2^{-1}a_1b_1 \in H. \tag{10.2}$$

Έστω $g \in G$ και $h \in H$. Θα δείξουμε ότι $g^{-1}hg \in H$. Από την (10.2) για $a_2^{-1}a_1 = h$ και $b_1 = b_2 = g$ έχουμε $g^{-1}hg \in H$.

(2) $\Rightarrow$ (3). Έστω $g^{-1}Hg \subseteq H$ για κάθε $g \in G$. Τότε για g^{-1} στην θέση του g παίρνουμε,

$$(g^{-1})^{-1}Hg^{-1} \subseteq H \Rightarrow gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg \Rightarrow H \subseteq g^{-1}Hg.$$

Επομένως $g^{-1}Hg = H$.

(3) $\Rightarrow$ (4). Έπεται άμεσα.

(4) $\Rightarrow$ (1). Επειδή $a_2^{-1}a_1 \in H$ και $gH = Hg$ για κάθε $g \in G$, υπάρχει $h \in H$ ώστε

$$b_2^{-1}(a_2^{-1}a_1) = h \cdot b_2^{-1}.$$

Επομένως

$$b_2^{-1}a_2^{-1}a_1b_1 = hb_2^{-1} \cdot b_1 \in H,$$

αφού $h \in H$, $b_2^{-1}b_1 \in H$ και $H \leq G$. Επομένως ισχύει η (3.4.3), άρα η (3.4.2) είναι πράγματι απεικόνιση. □

Προσοχή. Η σχέση $gH = Hg$ δεν σημαίνει αναγκαστικά ότι $gh = hg$ για κάθε $g \in G$ και για κάθε $h \in H$. Το σωστό είναι ότι για κάθε $g \in G$ και για κάθε $h \in H$ υπάρχει $h' \in H$ ώστε $gh = h'g$.

Ορισμός 10.3. *Έστω G ομάδα και $H \leq G$. Η H λέγεται* ***κανονική*** *υποομάδα της G (συμβολισμός $H \trianglelefteq G$) αν αληθεύουν οι συνθήκες της Πρότασης 10.2.*

Παραδείγματα 10.4.

(1) Αν η G είναι αβελιανή, τότε κάθε $H \leq G$ είναι κανονική.

(2) Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε $\ker\varphi \trianglelefteq G$.
Πράγματι, έστω $g \in G$ και $h \in \ker\varphi$. Θα δείξουμε ότι $g^{-1}hg \in \ker\varphi$. Παρατηρήστε ότι

$$\begin{aligned}\varphi(g^{-1}hg) &= \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})1_H\varphi(g)\\ &= \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = 1_H.\end{aligned}$$

Άρα $g^{-1}hg \in \ker\varphi$.

(3) Η υποομάδα A_n των άρτιων μεταθέσεων της συμμετρικής ομάδας S_n είναι κανονική υποομάδα, $A_n \trianglelefteq S_n$.
Γνωρίζουμε ότι $A_n \leq S_n$. Έστω $\sigma \in S_n$ και $\tau \in A_n$. Η μετάθεση $\sigma^{-1}\tau\sigma$ είναι άρτια αφού οι σ^{-1}, σ είναι ή και οι δύο άρτιες ή και οι δύο περιττές. Δηλαδή $\sigma^{-1}\tau\sigma \in A_n$ για κάθε $\sigma \in S_n$ και για κάθε $\tau \in A_n$. Άρα $A_n \trianglelefteq S_n$.
Σημείωση. Το γεγονός ότι $A_n \trianglelefteq S_n$ προκύπτει και από το Παράδειγμα (2). Πράγματι, $A_n = \ker(\mathrm{sign})$, όπου $\mathrm{sign} : S_n \to \{-1, 1\}$ ο ομομορφισμός προσήμου, Παράδειγμα 9.2(9).

(4) Η υποομάδα $H = \{1, (1\ 2)\}$ της S_3 δεν είναι κανονική.
Αρκεί να δείξουμε ότι $\sigma^{-1}(1\ 2)\sigma \notin H$ για κάποιο $\sigma \in S_3$. Για παράδειγμα θεωρήστε το $\sigma = (1\ 3)$. Τότε

$$(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H.$$

(5) Η υποομάδα $H =< \sigma >$ της S_4, όπου $\sigma = (1\ 2\ 3\ 4)$ δεν είναι κανονική.
Αρκεί να δείξουμε ότι $g^{-1}\tau g \notin H$ για κάποιο $g \in S_4$ και $\tau \in H$. Παρατηρούμε ότι για $g = (1\ 2)$ και $\tau = \sigma = (1\ 2\ 3\ 4)$,

$$(1\ 2)^{-1}(1\ 2\ 3\ 4)(1\ 2) = (2\ 1\ 3\ 4).$$

Έχουμε $H =< \sigma >= \{1, \sigma, \sigma^2, \sigma^3\}$ αφού η σ έχει τάξη 4. Επίσης, $\sigma^2 = (1\ 3)(2\ 4)$, $\sigma^3 = (4\ 3\ 2\ 1)$. Επομένως $(2\ 1\ 3\ 4) \notin H$ και η H δεν είναι κανονική.

(6) Η υποομάδα $H = \{\sigma \in S_4 : \sigma(4) = 4\}$ της S_4 δεν είναι κανονική.
Έστω $h \in H$. Επιλέγουμε $h \in H$ με $h(1) \neq 1$ και θέτουμε $\tau = (1\ 4)h(1\ 4)$. Αν $\tau(4) = 4$, τότε

$$(1\ 4)(4) = h(1\ 4)(4) \Rightarrow 1 = h(1),$$

αδύνατο. Άρα $\tau \notin H$.

(7) Η υποομάδα $H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}$ της $GL_2(\mathbb{R})$ δεν είναι κανονική.
Πράγματι, για $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ και $\eta = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ έχουμε

$$g^{-1}hg = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} \notin H.$$

(8) Έστω k σώμα. Η $SL_n(k) = \{A \in GL_n(k) : \det(A) = 1\}$ είναι κανονική υποομάδα της $GL_n(k)$ ως πυρήνας του ομομορφισμού ομάδων

$$GL_n(k) \to (k*, \cdot), A \mapsto det(A),$$

του Παραδείγματος 9.2(8).

(9) Έστω G ομάδα. Εύκολα επαληθεύεται ότι το κέντρο της G,

$$Z(G) = \{a \in G : ag = ga \ \ \forall g \in G\},$$

είναι κανονική υποομάδα της G.

10.2. Ομάδα πηλίκο

Έστω G ομάδα και $H \trianglelefteq G$. Δείξαμε στην προηγούμενη παράγραφο ότι η αντιστοιχία

$$G/H \times G/H \to G/H, \ \ (aH, bH) \mapsto abH$$

είναι απεικόνιση. Θα δούμε ότι με αυτή την πράξη το G/H είναι ομάδα. Η ουσιαστική δουλειά έγινε πριν και μένει τώρα η τυπική επαλήθευση.

Θεώρημα 10.5. *Έστω $H \trianglelefteq G$. Τότε το σύνολο G/H είναι ομάδα με την πράξη*

$$G/H \times G/H \to G/H, \ \ (aH, bH) \mapsto abH.$$

Απόδειξη. Παρατηρούμε ότι

$$\begin{aligned} (aH)\left((bH)(cH)\right) &= (aH)(bcH) = a(bc)H \\ \left((aH)(bH)\right)(cH) &= (ab)H(cH) = (ab)cH. \end{aligned}$$

Επειδή $a(bc) = (ab)c$, ισχύει η προσεταιριστική ιδιότητα στο G/H.

Για κάθε $aH \in G/H$ έχουμε, $(aH)(1_GH) = aH = (1_GH)(aH)$ αφού $1_Ga = a = a1_G$. Δηλαδή το ουδέτερο στοιχείο είναι το $1_GH = H$.

Τέλος, για κάθε $a \in H$,

$$(aH)(a^{-1}H) = aa^{-1}H = H \text{ και } (a^{-1}H)(aH) = aa^{-1}H = H.$$

Δηλαδή, το αντίστροφο του aH είναι το $a^{-1}H$. □

Παραδείγματα 10.6.

(1) Αν $G = \mathbb{Z}$ και $H =< n >= n\mathbb{Z}$, τότε $G/H = \mathbb{Z}_n$.

(2) Έστω $G = \mathbb{Q}$ και $H = \mathbb{Z}$. Επειδή η G είναι αβελιανή, έχουμε $H \trianglelefteq G$ και επομένως το σύνολο $\mathbb{Q}/\mathbb{Z} = \{a + \mathbb{Z} : a \in \mathbb{Q}\}$ είναι ομάδα με πράξη $(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) + \mathbb{Z}$. Εδώ έχουμε

$$a + \mathbb{Z} = b + \mathbb{Z} \Leftrightarrow a - b \in \mathbb{Z}.$$

Άρα τα ακόλουθα στοιχεία του $\mathbb{Q}/\mathbb{Z}$,

$$\mathbb{Z},\ \frac{1}{2} + \mathbb{Z},\ \frac{1}{3} + \mathbb{Z},\ \cdots$$

είναι διακεκριμένα. Αυτό σημαίνει ότι η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρη. Σημειώνουμε ότι κάθε στοιχείο αυτής έχει πεπερασμένη τάξη καθώς

$$n(\frac{m}{n} + \mathbb{Z}) = m + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}.$$

(3) Έστω $G = (\mathbb{R}^*, \cdot)$ και $H = \mathbb{R}_{>0}$. Είναι σαφές ότι $H \trianglelefteq G$. Εδώ $G/H = \{H, (-1)H\}$, όπου $(-1)H = \mathbb{R}_{<0}$.

(4) **Αβελιανοποίηση ομάδας** Έστω G ομάδα. Κάθε στοιχείο της G της μορφής

$$x^{-1}y^{-1}xy$$

λέγεται **μεταθέτης** και συμβολίζεται με $[x, y]$. Η ονομασία δικαιολογείται από τη σχέση $xy = yx[x, y]$. Είναι σαφές ότι τα x, y αντιμετατίθενται αν και μόνο αν $[x, y] = 1$. Με $[G, G]$ συμβολίζουμε την υποομάδα της G που παράγεται από τους μεταθέτες (βλ. Παράγραφο 8.6 για υποομάδα που παράγεται από στοιχεία). Καλείται **υποομάδα μεταθετών** της G ή **παράγουσα υποομάδα** της G. Πρόκειται περί κανονικής υποομάδας αφού για κάθε $g \in G$ έχουμε

$$g[x, y]g^{-1} = gx^{-1}y^{-1}xyg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1})$$

$$= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}] \in [G, G].$$

Άρα το πηλίκο $G/[G, G]$ είναι ομάδα κατά το συνήθη τρόπο. Παρατηρούμε ότι η $G/[G, G]$ είναι αβελιανή, καθώς για κάθε $x, y \in G$ έχουμε

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

Μάλιστα η $[G, G]$ είναι η μικρότερη κανονική υποομάδα N της G που το πηλίκο G/N είναι αβελιανή ομάδα, καθώς αν $xyN = yxN$ για κάθε $x, y \in G$, τότε

$$(yx)^{-1}xy \in N \Rightarrow [x, y] \in N \Rightarrow [G, G] \subseteq N.$$

Η ομάδα $G/[G, G]$ λέγεται η **αβελιανοποίηση** της G. Αν πάρετε μάθημα θεωρίας ομάδων ή αλγεβρικής τοπολογίας ή θεωρίας αναπαραστάσεων θα έχετε την ευκαιρία να εκτιμήσετε τις χάρες της. Για παράδειγμα, αν $n > 2$, τότε (άσκηση 10.22) $[S_n, S_n] = A_n$ και $S_n/[S_n, S_n] \simeq \mathbb{Z}_2$.

Θεώρημα 10.7 (Πρώτο θεώρημα ισομορφισμών ομάδων). *Έστω $\varphi : G \to H$ ομομορφισμός ομάδων. Τότε η απεικόνιση*

$$\psi : G/\ker\varphi \to \mathrm{Im}\varphi,\ \ \psi(g\ \ker\varphi) = \varphi(g)$$

είναι ισομορφισμός ομάδων.

Απόδειξη. Γνωρίζουμε ότι $\ker\varphi \trianglelefteq G$. Άρα $G/\ker\varphi$ είναι ομάδα με πράξη

$$(g_1 \ker\varphi)(g_2 \ker\varphi) = g_1 g_2 \ker\varphi.$$

Η ψ είναι καλώς ορισμένη. Πράγματι,

$$g_1 \ker\varphi = g_2 \ker\varphi \Leftrightarrow g_2^{-1} g_1 \in \ker\varphi \Leftrightarrow \varphi(g_2^{-1} g_1) = 1_H \Leftrightarrow \varphi(g_2)^{-1}\varphi(g_1) = 1_H$$
$$\Leftrightarrow \varphi(g_1) = \varphi(g_2).$$

Η ψ είναι ομομορφισμός ομάδων. Πράγματι,

$$\psi\left((g_1 \ker\varphi)(g_2 \ker\varphi)\right) = \psi(g_1 g_2 \ker\varphi) = \varphi(g_1 g_2)$$
$$= \varphi(g_1)\varphi(g_2) = \psi(g_1 \ker\varphi)\psi(g_1 \ker\varphi).$$

Η ψ είναι 1-1 αφού οι συνεπαγωγές στο επιχείρημα ότι η ψ είναι καλά ορισμένη αντιστρέφονται. □

Πόρισμα 10.8. *Έστω $N \trianglelefteq G$. Τότε το N είναι ο πυρήνας κάποιου ομομορφισμού ομάδων $\psi : G \to G'$.*

Απόδειξη. Έστω $\psi : G \to G/N$, $\psi(g) = gN$. Τότε ψ είναι ομομορφισμός ομάδων και $\ker\psi = N$. □

Θα δούμε εδώ μια εφαρμογή που δείχνει ότι το πέρασμα στο πηλίκο είναι χρήσιμη τεχνική σε συνδυασμό με επαγωγή.

Θεώρημα 10.9 (Cauchy για αβελιανές ομάδες)**.** *Έστω G πεπερασμένη αβελιανή ομάδα και $p \mid |G|$, όπου p πρώτος. Τότε υπάρχει $g \in G$ ώστε $|g| = p$.*

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στη $|G|$. Αν $|G| = 1$, δεν υπάρχει κάτι να δείξουμε Έστω ότι $|G| > 1$ και το θεώρημα ισχύει για κάθε αβελιανή ομάδα με τάξη $< |G|$. Έστω p πρώτος, με $p \mid |G|$. Έστω $a \in G$, $a \neq 1$ και $m = |a|$. Διακρίνουμε τις ακόλουθες δύο περιπτώσεις.

1. Έστω $p \mid m$. Τότε το $g = a^{\frac{m}{p}}$ έχει τάξη p.

2. Έστω $p \nmid m$. Θεωρούμε την ομάδα G/N, όπου $N =< a >$ (είναι ομάδα, αφού G αβελιανή). Παρατηρούμε ότι

$$|G/N| < |G| \ \ (\text{αφού} \ \ a \neq 1).$$

Επίσης η G/N είναι αβελιανή και $p \mid |G/N|$, αφού $p \mid |G|$ και $p \nmid m = |N|$. Από την επαγωγική υπόθεση υπάρχει $bN \in G/N$ τάξης p. Άρα

$$(bN)^p = N \ \ \Rightarrow \ \ b^p \in N.$$

Έστω $n = |b|$. Επειδή $(bN)^n = N$, η Πρόταση 8.11(2) δίνει ότι $p|n$. Το $b^{\frac{n}{p}}$ έχει τάξη p. □

Σημείωση. Το συμπέρασμα του θεωρήματος 10.9 ισχύει και χωρίς την υπόθεση ότι η G είναι αβελιανή. Το αποτέλεσμα αυτό είναι γνωστό ως το θεώρημα του Cauchy στις ομάδες. Δεν θα το αποδείξουμε εδώ. Αυτό και άλλα ωραία πράγματα μπορείτε να δείτε στο μάθημα Θεωρία Ομάδων.

Παραδείγματα 10.10.

(1) Θεωρούμε την ομάδα του κύκλου $E = \{z \in \mathbb{C} : |z| = 1\}$ (με πράξη τον πολλαπλασιασμό μιγαδικών). Ισχυριζόμαστε ότι $\mathbb{R}/\mathbb{Z} \simeq E$.
Πράγματι, αυτό προκύπτει άμεσα από το πρώτο θεώρημα ισομορφισμών εφαρμοζόμενο στην ομομορφισμό του Παραδείγματος 9.8(2).

(2) Στο Παράδειγμα 10.4(8) είδαμε ότι αν k είναι σώμα, η υποομάδα $SL_n(k)$ της $GL_n(k)$ είναι κανονική καθώς είναι ο πυρήνας του ομομορφισμού ομάδων $GL_n(k) \to k^*, A \mapsto \det(A)$. Η απεικόνιση αυτή είναι επί και επομένως από το πρώτο θεώρημα ισομορφισμών έπεται ότι $GL_n(k)/SL_n(k) \simeq k^*$.

(3) Έστω k σώμα και $B(k)$, $U(k)$ και $T(k)$ οι υποομάδες της $GL_n(k)$ των άνω τριγωνικών πινάκων, των άνω τριγωνικών πινάκων με όλα τα διαγώνια στοιχεία ίσα με 1 και των διαγώνιων πινάκων αντίστοιχα. Εύκολα επαληθεύεται ότι η απεικόνιση

$$B(k) \to T(k), (a_{ij}) \mapsto diag(a_{11}, ..., a_{nn})$$

είναι επιμορφισμός ομάδων με πυρήνα την υποομάδα $U(k)$. Άρα η $U(k)$ είναι κανονική στη $B(k)$ και $B(k)/U(k) \simeq T(k)$.

10.3. Γινόμενο υποομάδων, εσωτερικό ευθύ γινόμενο

Έστω A, B υποσύνολα ομάδας G. Ορίζουμε το σύνολο

$$AB = \{ab \in G : a \in A, b \in B\}.$$

Είναι σαφές ότι οι αριστερές και δεξιές κλάσεις είναι ειδικές περιπτώσεις όταν το A (αντίστοιχα, το B) είναι μονοσύνολο και το B (αντίστοιχα, το A) υποομάδα. Ακόμα και αν οι A, B είναι υποομάδες της G δεν είναι απαραίτητο το AB να είναι ομάδα. Ένα παράδειγμα είναι $G = S_3, A =< (12) >, B =< (13) >$ καθώς τότε το σύνολο $AB = \{1, (12), (13), (132)\}$ έχει 4 στοιχεία και το 4 δεν διαιρεί το 6.

Πρόταση 10.11. *Έστω G ομάδα και $H, K \leq G$. Ισχύουν τα εξής.*
(1) *$HK \leq G \Leftrightarrow HK = KH$.*
(2) *Αν $H \trianglelefteq G$ ή $K \trianglelefteq G$, τότε $HK \leq G$.*

Απόδειξη. (1) Έστω $HK \leq G$. Για κάθε $k \in K, h \in H$ έχουμε $kh = (h^{-1}k^{-1})^{-1} \in HK$ γιατί $HK \leq G$. Άρα $KH \subseteq HK$. Συνεπώς δεδομένων των k, h υπάρχουν $k_1 \in K, h_1 \in H$ με $k^{-1}h^{-1} = h_1k_1 \Rightarrow hk = k_1^{-1}h_1^{-1} \in KH$. Άρα $HK \subseteq KH$. Αντίστροφα, αν $HK = KH$, τότε για κάθε $h_1, h_2 \in H$ και $k_1, k_2 \in K$ έχουμε

$$(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2^{-1}) = h_1h_3k_3 \in HK$$

για κάποια $h_3 \in H$ και $k_3 \in K$. Άρα $HK \leq G$.
(2) Αν $H \trianglelefteq G$, τότε για κάθε $k \in K, Hk = kH$ και άρα $HK = KH$. Από το (1), $HK \leq G$. Η απόδειξη με την υπόθεση $K \trianglelefteq G$ είναι παρόμοια. □

Σημειώνουμε ότι αν $H, K \leq G$ και το σύνολο HK είναι υποομάδα της G, τότε η HK είναι η υποομάδα της G που παράγεται από το σύνολο $H \cup K$. Αυτό έπεται από το (1) της προηγούμενης πρότασης.

Σε επιχειρήματα αριθμητικού τύπου με γινόμενα πεπερασμένων υποομάδων, η ακόλουθη πρόταση είναι συχνά χρήσιμη. Θα δούμε τέτοια επιχειρήματα στα παραδείγματα και εφαρμογές που ακολουθούν.

Πρόταση 10.12. *Αν G ομάδα και H, K πεπερασμένες υποομάδες της G, τότε*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Απόδειξη. Θεωρούμε την απεικόνιση

$$f : H \times K \to HK, f(h, k) = hk.$$

Είναι σαφές ότι είναι επί. Αρκεί να δείξουμε ότι η αντίστροφή εικόνα κάθε $y \in HK$ έχει $|H \cap K|$ στοιχεία. Για το σκοπό αυτό θα δείξουμε ότι

$$f^{-1}(hk) = \{(hx, x^{-1}k) : x \in H \cap K\}.$$

Πράγματι, η σχέση $\supseteq$ είναι σαφής. Έστω $(h_1, k_1) \in f^{-1}(hk)$, οπότε $h_1k_1 = hk$. Τότε $h^{-1}h_1 = kk_1^{-1} \in H \cap K$ αφού H, K υποομάδες. Θέτοντας $x = h^{-1}h_1 = kk_1^{-1}$, έχουμε ότι $(h_1, k_1) = (hx, x^{-1}k)$. □

Πρόταση 10.13. *Έστω G ομάδα και $H, K \leq G$ έτσι ώστε:*
(1) *Οι H, K είναι κανονικές στη G,*
(2) *$H \cap K = \{1\}$,*
(3) *$HK = G$.*
Τότε η απεικόνιση $H \times K \to G, (h, k) \mapsto G$, είναι ισομορφισμός.

Απόδειξη. Πρώτα θα δείξουμε ότι από τις υποθέσεις (1) και (2) έπεται ότι $hk = kh$ για κάθε $h \in H, k \in K$. Πράγματι, έχουμε $(hkh^{-1})k^{-1} \in K$ αφού K κανονική στη G και όμοια $h(kh^{-1}k^{-1}) \in H$ αφού H κανονική στη G. Άρα

$$hkh^{-1}k^{-1} \in H \cap K = \{1\} \Rightarrow hk = kh.$$

Θεωρούμε την απεικόνιση

$$f : H \times K \to G, f(h, k) = hk.$$

Από την υπόθεση (3) είναι επί. Είναι ομομορφισμός ομάδων καθώς

$$f((h, k)(h', k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h, k)f(h', k').$$

Τέλος η f είναι 1-1 καθώς έχει τετριμμένο πυρήνα. Πράγματι,

$$hk = 1 \Rightarrow h = k^{-1} \in H \cap K = \{1\} \Rightarrow (h, k) = (1, 1).$$

Συνεπώς η f είναι ισομορφισμός. □

Όταν ισχύουν οι υποθέσεις τις Πρότασης 10.13 θα λέμε ότι η G είναι το **εσωτερικό ευθύ γινόμενο** των H, K. Στην περίπτωση αυτή, μιλώντας ελεύθερα, έχουμε πετύχει μια διάσπαση της G σε απλούστερα κομμάτια, $G = H \times K$, πράγμα που διευκολύνει τη μελέτη της G.

Επισημαίνουμε ότι ισχύει το αντίστροφο της Πρότασης 10.13 (βλ. άσκηση 10.27).

Παραδείγματα 10.14.

(1) Αν $G = S_3, K = A_3$ και H οποιαδήποτε υποομάδα της G τάξης 2, τότε $G = HK$ αλλά δεν αληθεύει ότι η G είναι το εσωτερικό ευθύ γινόμενο των H, K καθώς η H δεν είναι κανονική στην S_3. Εξάλλου αν ίσχυε το συμπέρασμα της Πρότασης 10.13 για το συγκεκριμένο παράδειγμα θα είχαμε $S_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$ που είναι αβελιανή, αδύνατο.

(2) Έστω G κυκλική ομάδα τάξης mn, όπου m, n είναι σχετικά πρώτα ακέραιοι. Ξέρουμε ότι η G έχει υποομάδες G_m, G_n τάξεων m, n αντίστοιχα. Τότε η G είναι το εσωτερικό ευθύ γινόμενο των G_m, G_n. Πράγματι οι υποομάδες αυτές είναι κανονικές καθώς η G είναι αβελιανή. Επειδή οι m, n είναι σχετικά πρώτοι, έχουμε ότι $G_m \cap G_n = \{1\}$ σύμφωνα με την άσκηση 8.1. Τέλος από την Πρόταση 10.12 έχουμε $|G_mG_n| = mn$ και άρα $G_mG_n = G$.

Εφαρμογή 10.15. *Έστω G πεπερασμένη ομάδα και $H \leq G$ με $[G : H] = p$. Αν p είναι ο μικρότερος πρώτος που διαιρεί την τάξη της G, τότε η $H \trianglelefteq G$*

Απόδειξη. Πράγματι, έστω $x \in G$ και $K = x^{-1}Hx \neq H$. Τότε $|K| = |H|$ και από την Πρόταση 10.12 έπεται ότι

$$|HK| = |H|\frac{|H|}{|H \cap K|}.$$

Επειδή $K \neq H$, έχουμε $\frac{|H|}{|H \cap K|} > 1$ και επειδή ο ακέραιος $\frac{|H|}{|H \cap K|}$ διαιρεί τον $|G|$, έχουμε $\frac{|H|}{|H \cap K|} \geq p$ λόγω του ελαχίστου του p. Συνεπώς $|HK| \geq |H|p = |G|$ που σημαίνει ότι $G = HK$. Άρα υπάρχουν $h, h' \in H$ με

$$x = h(x^{-1}h'x) \Rightarrow 1 = hx^{-1}h' \Rightarrow x \in H \Rightarrow K = H,$$

άτοπο. □

Εφαρμογή 10.16. *Κάθε ομάδα G τάξης p^2, όπου p πρώτος, είναι ισόμορφη με τη $\mathbb{Z}_{p^2}$ ή $\mathbb{Z}_p \times \mathbb{Z}_p$. Ειδικά η G είναι αβελιανή.*

Απόδειξη. Πράγματι, έστω ότι η G δεν είναι κυκλική. Επειδή η τάξη της είναι p^2, κάθε στοιχείο της διάφορο του 1 έχει τάξη p. Επειδή $|G| > p$, είναι σαφές ότι υπάρχουν $a, b \in G - \{1\}$ με $a \notin < b >$. Έστω $H = < a >, K = < b >$.

(1) Οι H, K είναι κανονικές στη G από το προηγούμενο παράδειγμα.

(2) Ισχύει ότι $H \cap K = \{1\}$ καθώς από το θεώρημα του Lagrange έχουμε $|H \cap K||p$ και έχουμε $H \cap K \subsetneq H$.

(3) Ισχύει $G = HK$ καθώς από την Πρόταση 10.12, $|HK| = p^2$.

Από την Πρόταση 10.13 παίρνουμε $G \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Ασκήσεις Κεφαλαίου 10

Ομάδα1: 4, 8, 9, 14-16.
Ομάδα2: 1, 2, 3, 5-7, 10-13, 17-21, 25-26, 29, 30, 31.
Ομάδα3: 22, 23, 27, 28, 32.

1. $\star$ Δείξτε ότι κάθε υποομάδα δείκτη 2 είναι κανονική.
2. Δείξτε ότι αν H είναι υποομάδα της G με δείκτη 2, τότε η H περιέχει κάθε στοιχείο της G που έχει περιττή τάξη. Στη συνέχεια δείξτε ότι η A_4 δεν περιέχει υποομάδα τάξης 6 και επομένως δεν αληθεύει γενικά το αντίστροφο του θεωρήματος του Lagrange.
3. Έστω $G =< a >$ κυκλική τάξης 12 και $H =< a^{1821} >$. Βρείτε τον ελάχιστο θετικό ακέραιο m με $a^m \in H$.
4. Έστω $H \leq Z(G)$, όπου G ομάδα και $Z(G) = \{a \in G : ag = ga \quad \text{για κάθε} \quad g \in G\}$ το κέντρο της ομάδας της G. Τότε $H \trianglelefteq G$.
5. $\star$ Έστω $H \leq Z(G)$. Αν G/H κυκλική, τότε G αβελιανή.
6. Έστω G ομάδα με $|G| = pq$, όπου p, q διακεκριμένοι πρώτοι. Δείξτε ότι αν $Z(G) \neq \{1\}$, τότε η G είναι κυκλική.
7. Έστω $|G| = 210,\ N \trianglelefteq G,\ |N| = 7$.
   i) Δείξτε ότι $g^{30} \in N$ για κάθε $g \in G$.
   ii) Δείξτε ότι αν $g^7 \in N$, τότε $g \in N$.
8. $\star$Έστω $H \trianglelefteq G,\ K \trianglelefteq G$.
   i) Δείξτε ότι $H \cap K \trianglelefteq G$.
   ii) Αν $H \cap K = \{1\}$, δείξτε ότι $hk = kh$ για κάθε $h \in H$ και για κάθε $k \in K$.
9. Δείξτε ότι κάθε αβελιανή ομάδα τάξης pq, όπου p, q είναι διακεκριμένοι πρώτοι, είναι κυκλική. Διατυπώστε και αποδείξτε μια γενίκευση.
10. Αληθεύει ότι υπάρχει ομομορφισμός $\varphi : S_5 \to G$ με $\ker\varphi =< \sigma >$, όπου $\sigma = (2345)$;
11. Θεωρούμε την πολλαπλασιαστική ομάδα $\mathbb{R}^* = \mathbb{R} - \{0\}$.
   i) Δείξτε ότι $\mathbb{R}_{>0} \leq \mathbb{R}^*$ και $[\mathbb{R}^* : \mathbb{R}_{>0}] = 2$.
   ii) Δείξτε ότι η $\mathbb{R}^*$ έχει μοναδική υποομάδα δείκτη 2.
12. Έστω G ομάδα και $m \in \mathbb{Z}_{>0}$ τέτοια ώστε υπάρχει μοναδική $H \leq G$ με $|H| = m$. Τότε $H \trianglelefteq G$.
13. Έστω G ομάδα και $m \in \mathbb{Z}_{>0}$ τέτοια ώστε υπάρχει $H \leq G$ με $|H| = m$. Δείξτε ότι η τομή όλων των υποομάδων της G τάξης m είναι κανονική υποομάδα της G.
14. Δείξτε ότι η $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ είναι κανονική υποομάδα της $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$ και $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}$.
15. Έστω $m, n \in \mathbb{Z}_{>0}$. Τότε $\mathbb{Z}_n/ < [m] > \simeq \mathbb{Z}_m$.
16. Έστω G_1, G_2 ομάδες και $N_i \trianglelefteq G_i$. Δείξτε ότι $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ και
$$\frac{G_1 \times G_2}{N_1 \times N_2} \simeq \frac{G_1}{N_1} \times \frac{G_2}{N_2}.$$
17. Έστω G ομάδα και $a, b \in G$. Δίνεται η απεικόνιση $f : \mathbb{Z} \times \mathbb{Z} \to G, f(x, y) = a^x b^y$.
   i) Βρείτε και αποδείξτε ικανή και αναγκαία συνθήκη στα a, b ώστε η f να είναι ομομορφισμός ομάδων.
   ii) Έστω ότι η G είναι αβελιανή και ότι οι τάξεις των a, b είναι πεπερασμένες και σχετικά πρώτες. Βρείτε το $\ker f$ και την τάξη της εικόνας Img.
18. Έστω G ομάδα και $D = \{(g, g) \in G \times G : g \in G\}$. Δείξτε τα εξής.
   i) $D \leq G \times G$.
   ii) $D \trianglelefteq G \times G \Leftrightarrow G$ αβελιανή.

19. i) Έστω $\varphi : G \to H$ ομομορφισμός ομάδων και $K \trianglelefteq H$. Τότε το σύνολο $\varphi^{-1}(K) = \{g \in G : \varphi(g) \in K\}$ είναι κανονική υποομάδα της G.
    ii) Έστω $\varphi : G \to \mathbb{Z}_n$ επιμορφισμός ομάδων. Τότε για κάθε θετικό διαιρέτη d του n υπάρχει $N \trianglelefteq G$ με $[G : N] = d$.
20. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων.
    i) Αν η φ είναι επί και όχι 1-1 και $|G| = 77$, τότε η H είναι αβελιανή.
    ii) Αν $|G| = 20$, $|H| = 26$, τότε $|\mathrm{Im}\varphi| = 1$ ή 2.
21. Αν G ομάδα και $a \in G$, θέτουμε $\varphi_a : G \to G$, $\varphi_a(g) = a^{-1}ga$. Να αποδείξετε τα ακόλουθα.
    i) φ_a ισομορφισμός ομάδων.
    ii) Το $\mathrm{Inn}G = \{\varphi_a : a \in G\}$ είναι ομάδα ως προς την σύνθεση απεικονίσεων.
    iii) $G/Z(G) \simeq \mathrm{Inn}G$ $(Z(G) = \{a \in G : ag = ga\ \forall g \in G\})$.
22. Έστω G ομάδα που διαθέτει δύο διαφορετικές υποομάδες H, K δείκτη 2. Δείξτε ότι $H \cap K \trianglelefteq G$ και $\dfrac{G}{H \cap K} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
23. Δείξτε ότι η παράγουσα υποομάδα της S_n είναι η A_n, $n > 2$.
24. Θεωρούμε τη διεδρική ομάδα $D_n = \{1, r, ..., r^{n-1}, s, sr, ..., sr^{n-1}\}$ με το συμβολισμό του Παραδείγματος 7.4(10). Δείξτε ότι η υποομάδα $H =< r >$ των περιστροφών είναι κανονική και $D_n/H \simeq \mathbb{Z}_2$.
25. Με το συμβολισμό του Παραδείγματος 7.4(10) δείξτε ότι η παράγουσα υποομάδα της διεδρικής D_n είναι η $< r^2 >$. Βρείτε την αβελιανοποίηση της D_n.
26. Δίνονται τα στοιχεία $\rho = (12345), \sigma = (25)(35) \in S_5$ και η παραγόμενη υποομάδα $G =< \rho, \sigma >$. Δείξτε τα εξής.
    i) $\sigma\rho = \rho^{-1}\sigma$
    ii) $< \rho > \trianglelefteq G$.
    iii) $G \simeq D_5$.
27. Δείξτε ότι η A_n, $n > 1$, είναι η μοναδική υποομάδα της S_n δείκτη 2.
28. ≀ Δείξτε ότι αν N είναι κανονική υποομάδα της $A_n, n \geq 3$ που περιέχει ένα κύκλο μήκους 3, τότε $N = A_n$.
29. Δείξτε το αντίστροφο της Πρότασης 10.13.
30. Έστω $H \leq G$ τέτοια ώστε $x^2 \in H$ για κάθε $x \in G$. Δείξτε ότι $H \trianglelefteq G$.
31. Έστω $\varphi : G \to H$ ομομορφισμός ομάδων, όπου η H είναι αβελιανή. Δείξτε ότι κάθε υποομάδα της G που περιέχει τον πυρήνα $ker\varphi$ είναι κανονική υποομάδα της G.
32. Έστω G πεπερασμένη ομάδα και $N \trianglelefteq G$ με $\mu\kappa\delta(|N|, [G : N]) = 1$. Δείξτε ότι η N είναι η μοναδική υποομάδα της G τάξης $|N|$.
33. Έστω G πεπερασμένη ομάδα και$N \trianglelefteq G$ με $\mu\kappa\delta(|G|, Aut(G)) = 1$, όπου $Aut(G)$ είναι η ομάδα των αυτομορφισμών της G, δηλαδή η ομάδα των ισομορφισμών $G \to G$ με πράξη τη σύνθεση απεικονίσεων. Δείξτε ότι η N περιέχεται στο κέντρο της G.

Υποδείξεις Ασκήσεων Κεφαλαίου 10

1. *Λύση.* Έστω $[G:H]=2$. Τότε αν $g\in G-H$, έχουμε τις ξένες ενώσεις $G=H\cup gH$ και $G=H\cup Hg$. Άρα $gH=G-H=Hg$. Αν $g\in H$, τότε φυσικά πάλι $gH=H=Hg$.

2. *Υπόδειξη.* Από την προηγούμενη άσκηση η H είναι κανονική στη G και άρα μπορούμε να θεωρήσουμε το φυσικό ομομορφισμό $G\to G/H$. Δείξτε ότι ο πυρήνας περιέχει κάθε στοιχείο της G που έχει περιττή τάξη.

   Για το δεύτερο ερώτημα, παρατηρούμε ότι αν H είναι υποομάδα της A_4 τάξης 6, τότε η H περιέχει κάθε κύκλο μήκους 3 σύμφωνα με το πρώτο ερώτημα. Όμως το πλήθος αυτών είναι $8>6$, άτοπο.

3. *Λύση.* Η τάξη της H ισούται με την τάξη του a^{1821}, οπότε $|H|=\frac{12}{\mu\kappa\delta(1821,12)}=4$. Γνωρίζουμε ότι για κάθε διαιρέτη $d\mid|G|$ υπάρχει μοναδική υποομάδα της G τάξης d (γιατί G κυκλική) και αυτή είναι η $<a^{\frac{n}{d}}>$. Άρα $H=<a^{\frac{12}{4}}>=<a^3>$. Άρα $m=3$.

4. *Λύση.* $Z(G)\leq G$. Αφού $H\leq Z(G)$, έπεται $H\leq G$. Έστω $g\in G$ και $h\in H$. Τότε $g^{-1}hg=hg^{-1}g=h\in H$. Άρα $H\trianglelefteq G$.

5. *Λύση.* Από την προηγούμενη άσκηση, $H\trianglelefteq G$, άρα η G/H είναι ομάδα. Έστω $G/H=<aH>$. Έστω $g_1,g_2\in G$. Θα δείξουμε ότι $g_1g_2=g_2g_1$. Παρατηρούμε ότι $g_1H\in G/H$, άρα $g_1H=a^mH$ για κάποιο $m\in\mathbb{Z}_{>0}$. Επομένως $g_1=a^mh_1$, για κάποιο $h_1\in H$. Ομοίως $g_2=a^nh_2$, για κάποιο $h_2\in H$. Τότε

$$g_1g_2=a^mh_1a^nh_2\overset{H\leq Z(G)}{=}a^ma^nh_1h_2=a^{m+n}h_1h_2.$$

   Ομοίως $g_2g_1=a^{m+n}h_1h_2$. Άρα $g_1g_2=g_2g_1$.

6. *Υπόδειξη.* Χρησιμοποιώντας την προηγούμενη άσκηση δείξτε ότι η G είναι αβελιανή. Μετά εφαρμόστε την άσκηση 8.2.

7. *Λύση.* i) Αφού $N\trianglelefteq G$, η G/N είναι ομάδα με την συνήθη πράξη και $|G/N|=\frac{|G|}{|N|}=\frac{210}{7}=30$. Επομένως για κάθε $g\in G$, $(gN)^{30}=1_{G/N}\Rightarrow g^{30}N=N\Rightarrow g^{30}\in N$.

   ii) Παρατηρούμε ότι

$$g^7\in N\Rightarrow g^7N=N\Rightarrow(gN)^7=N=1_{G/N}.$$

   Επομένως στην ομάδα G/N, $|gN|\mid 7$. Όμως έχουμε και $|gN|\mid 30$ καθώς $|G/N|=30$. Αφού $\mu\kappa\delta(7,30)=1$, $|gN|=1\Rightarrow gN=1_{G/N}=N\Rightarrow g\in N$.

8. *Λύση.* 1. Έχουμε $H\leq G$ και $K\leq G$. Ξέρουμε ότι $H\cap K\leq G$. Έστω $a\in H\cap K$ και $g\in G$. Τότε $a\in H$ και αφού $H\trianglelefteq G$, παίρνουμε $g^{-1}ag\in H$. Ομοίως $g^{-1}ag\in K$, οπότε $g^{-1}ag\in H\cap K$. Δηλαδή, $H\cap K\trianglelefteq G$.

   2. Έστω $h\in H$ και $k\in K$. Τότε $k^{-1}hk\in H$, αφού $H\trianglelefteq G\quad(k\in K)$. Άρα $h^{-1}(k^{-1}hk)\in H$, αφού $H\leq G$. Ομοίως, $h^{-1}k^{-1}hk\in K$ (αφού $h^{-1}k^{-1}h\in K$). Επομένως

$$h^{-1}k^{-1}hkk\in H\cap K=\{1\}\Rightarrow h^{-1}k^{-1}hk=1\Rightarrow hk=kh.$$

9. *Λύση.* Από το Θεώρημα 10.9 η G έχει στοιχεία a,b τάξης p,q αντίστοιχα. Από την άσκηση 8.2, η G έχει στοιχείο τάξης pq, άρα είναι κυκλική.
   Γενίκευση: Κάθε πεπερασμένη αβελιανή ομάδα με τάξη που δεν διαιρείται από το τετράγωνο φυσικού αριθμού >1 είναι κυκλική.

10. *Λύση.* Όχι. Θα δείξουμε ότι η $<\sigma>$ δεν είναι κανονική στην S_5. Παρατηρούμε ότι $(12)^{-1}(2345)(12)=(1345)\notin<\sigma>$,αφού, για παράδειγμα, κάθε $\tau\in<\sigma>$ έχει την ιδιότητα $\tau(1)=1$ (κι εδώ δεν ισχύει) ή αλλιώς $<\sigma>=\{1,\sigma,\sigma^2,\sigma^3\}$, όπου $\sigma^2=(24)(35)$, $\sigma^3=\sigma^{-1}=(5432)$.

11. *Λύση.* *ii*). Έστω H υποομάδα της αβελιανής ομάδας $\mathbb{R}^*$ με δείκτη 2. Τότε η ομάδα $\mathbb{R}^*/H$ έχει τάξη 2 και συνεπώς $(xH)^2=H$, δηλαδή $x^2\in H$ για κάθε $x\in\mathbb{R}^*$. Άρα $\mathbb{R}_{>0}\subseteq$

H. Συνεπώς, αν το H περιέχει αρνητικό πραγματικό αριθμό, τότε λόγω κλειστότητας θα περιείχε κάθε αρνητικό πραγματικό, οπότε $H = \mathbb{R}^*$, αδύνατο. Άρα $H = \mathbb{R}_{>0}$.

12. *Λύση.* Παρατηρούμε ότι αν $g \in G$, τότε $g^{-1}Hg \leq G$ και $|g^{-1}Hg| = |H|$. Πράγματι, $g^{-1}Hg \neq \emptyset$, αφού $H \neq \emptyset$. Έστω $g^{-1}h_1g,\ g^{-1}h_2g \in g^{-1}Hg$. Τότε

$$g^{-1}h_1gg^{-1}h_2g = g^{-1}(h_1h_2)g \in g^{-1}Hg,$$

αφού $H \leq G$. Επίσης,

$$(g^{-1}h_1g)^{-1} = g^{-1}h_1^{-1}(g^{-1})^{-1} = g^{-1}h_1^{-1}g \in g^{-1}Hg,$$

αφού $H \leq G$. Η απεικόνιση $f : H \to g^{-1}Hg,\ \ f(h) = g^{-1}hg$ είναι 1-1 και επί. Πράγματι, έστω $f(h_1) = f(h_2)$. Τότε $g^{-1}h_1g = g^{-1}h_2g \Rightarrow h_1 = h_2$. Δηλαδή η f είναι 1-1. Από τον ορισμό της f είναι άμεσο ότι είναι επί. Επομένως αφού $g^{-1}Hg \leq G$ και $|g^{-1}Hg| = |H|$ και από την μοναδικότητα της υπόθεσης έπεται ότι $g^{-1}Hg = H$ για κάθε $g \in G$. Δηλαδή $H \trianglelefteq G$.

13. *Υπόδειξη.* Έστω $g \in G$. Δείξτε ότι καθώς το H διατρέχει τις υποομάδες της G τάξης m, το ίδιο συμβαίνει με τις υποομάδες gHg^{-1}.

14. *Λύση.* Η απεικόνιση ορίζουσας $\det : GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$, είναι ομομορφισμός ομάδων αφού $\det AB = (\det A)(\det B)$. Επειδή $\ker det = SL_n(\mathbb{R})$, έχουμε $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$. Επίσης η απεικόνιση det είναι επί. Πράγματι, αν $a \in \mathbb{R} \setminus \{0\}$ Τότε $\det diag(a, 1, ..., 1) = a$. Από το πρώτο θεώρημα ισομορφισμών ομάδων παίρνουμε ότι $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R} \setminus \{0\}$.

15. *Λύση. Πρώτος τρόπος.* Θεωρούμε την απεικόνιση $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m,\ \ [a]_n \mapsto [a]_m$. Η φ είναι καλώς ορισμένη. Πράγματι, $[a]_n = [b]_n \Rightarrow n \mid a - b \Rightarrow m \mid a - b \Rightarrow [a]_m = [b]_m$.

Η φ είναι ομομορφισμός ομάδων. Πράγματι,

$$\varphi([a]_n + [b]_n) = \varphi([a + b]_n) = [a + b]_m = [a]_m + [b]_m = \varphi([a]_n) + \varphi([b]_n).$$

Είναι σαφές ότι η φ είναι επί. Παρατηρούμε ότι

$$\ker \varphi = \{[a]_n : [a]_m = [0]_m\} = \{[a]_n : m \mid a\} =< [m]_n > .$$

Επομένως από το πρώτο θεώρημα ισομορφισμών ομάδων, $\mathbb{Z}_n/ < [m] > \simeq \mathbb{Z}_m$.

Δεύτερος τρόπος. Η $\mathbb{Z}_m$ είναι κυκλική ομάδα.

Ισχυρισμός. Αν G κυκλική και $N \leq G$, τότε G/N κυκλική. Πράγματι, η G είναι αβελιανή άρα $N \trianglelefteq G$. Αν $G =< a >$, τότε $G/N =< aN >$. Πράγματι, αν $g \in G$ τότε $g = a^k$ για κάποιο $k \in \mathbb{Z}$. Άρα $gN = a^kN = (aN)^k$.

Επομένως από τον ισχυρισμό έπεται ότι η $\mathbb{Z}_n/ < [m] >$ είναι κυκλική. Όμως δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια τάξη. Επειδή,

$$\left|\frac{\mathbb{Z}_n}{< [m] >}\right| = \frac{n}{\frac{n}{m}} = m = |\mathbb{Z}_m|,$$

το ζητούμενο έπεται.

16. *Υπόδειξη.* Θεωρήστε την απεικόνιση $(g_1, g_2) \mapsto (g_1N_1, g_2N_2)$ και εφαρμόστε το πρώτο θεώρημα ισομορφισμών.

17. *Υπόδειξη.*
    i) Δείξτε ότι η f να είναι ομομορφισμός ομάδων αν και μόνο αν $ab = ba$.
    ii) Δείξτε ότι $\ker f = m\mathbb{Z} \times n\mathbb{Z}$, όπου m, n είναι οι τάξεις των a, b αντίστοιχα. Για το σκοπό αυτό, η άσκηση 2.1 είναι χρήσιμη. Δείξτε ότι

$$\frac{\mathbb{Z} \times \mathbb{Z}}{m\mathbb{Z} \times n\mathbb{Z}} \simeq \mathbb{Z}_m \times \mathbb{Z}_n.$$

18. *Λύση. ii).* Έστω $a, b, g \in G$. Παρατηρούμε ότι

$$(a, b)(g, g)(a, b)^{-1} = (a, b)(g, g)(a^{-1}, b^{-1}) = (aga^{-1}, bgb^{-1}).$$

Άρα η D είναι κανονική στη $G \times G$ αν και μόνο

$$aga^{-1} = bgb^{-1}, \tag{10.3}$$

για κάθε $a, b, g \in G$. Θέτοντας $b = 1$ στη (10.3) έπεται ότι $ag = ga$ για κάθε $a, g \in G$, δηλαδή η G είναι αβελιανή. Αντίστροφα, αν η G είναι αβελιανή, τότε σαφώς ισχύει η (10.3).

19. *Λύση. i)* Πρώτα θα δείξουμε ότι $\varphi^{-1}(K) \leq G$. Πράγματι, $\varphi^{-1}(K) \neq \emptyset$, αφού $\varphi(1_G) = 1_H \in K$. Έστω $a, b \in \varphi^{-1}(K)$, δηλαδή $\varphi(a), \varphi(b) \in K$. Τότε

$$\varphi(a)\varphi(b) \in K \overset{(K \leq H)}{\Rightarrow} \varphi(ab) \in K \Rightarrow ab \in \varphi^{-1}(K).$$

Επίσης,

$$\varphi(a) \in K \overset{K \leq H}{\Rightarrow} \varphi(a)^{-1} \in K \Rightarrow \varphi(a^{-1}) \in K \Rightarrow a^{-1} \in \ \varphi^{-1}(K).$$

Συνεπώς $\varphi^{-1}(K) \leq G$.
Έστω $a \in \varphi^{-1}(K)$. Τότε $\varphi(a) \in K$. Για κάθε $g \in G$ έχουμε

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) \in K,$$

αφού $K \trianglelefteq H$. Άρα $g^{-1}ag \in \varphi^{-1}(K)$, δηλαδή $\varphi^{-1}(K) \trianglelefteq G$.

ii) Επειδή $\mathbb{Z}_n$ κυκλική και το $\frac{n}{d} \mid n$, υπάρχει $K \leq \mathbb{Z}_n$ ώστε $|K| = \frac{n}{d}$. Έστω $N = \varphi^{-1}(K)$. Από το ερώτημα 1 έχουμε $N \trianglelefteq G$ (αφού $K \trianglelefteq \mathbb{Z}_n$ γιατί $\mathbb{Z}_n$ αβελιανή). Θα δείξουμε ότι $[G : N] = d$.

Για το σκοπό αυτό αρκεί να δειχθεί ότι η ακόλουθη απεικόνιση είναι 1-1 και επί,

$$\psi : G/N \to \mathbb{Z}_n/K, gN \mapsto \varphi(g)K.$$

Η ψ είναι καλά ορισμένη και 1-1 γιατί

$$gN = hN \Leftrightarrow h^{-1}g \in N \Leftrightarrow \varphi(h^{-1}g) = \varphi(h)^{-1}\varphi(g) \in K \Leftrightarrow \varphi(g)K = \varphi(h)K.$$

Είναι σαφές ότι η ψ είναι επί αφού η φ είναι επί. (*Σημείωση.* Η ψ είναι ισομορφισμός ομάδων).

20. *Λύση. i)* Από το πρώτο θεώρημα ισομορφισμών ομάδων, $G/\ker\varphi \simeq \mathrm{Im}\varphi = H$. Η φ δεν είναι 1-1, άρα $|\ker\varphi| > 1$. Επομένως $|G/\ker\varphi| = 1, 7, 11$. Δηλαδή $|H| = 1, 7, 11$, άρα H κυκλική (οι $7, 11$ είναι πρώτοι), οπότε H αβελιανή.
ii) Παρατηρούμε ότι $\mathrm{Im}\varphi \leq H$, άρα από το θεώρημα του Lagrange παίρνουμε,

$$|\mathrm{Im}\varphi| \mid |H| \Rightarrow |\mathrm{Im}\varphi| \mid 26.$$

Επειδή $G/\ker\varphi \simeq \mathrm{Im}\varphi$ έπεται ότι

$$|\mathrm{Im}\varphi| \mid |G| \Rightarrow |\mathrm{Im}\varphi| \mid 20.$$

Επομένως $|\mathrm{Im}\varphi| = 1$ ή 2.

21. *Λύση. i)* Παρατηρούμε ότι

$$\varphi_a(g_1g_2) = a^{-1}(g_1g_2)a = (a^{-1}g_1a)(a^{-1}g_2a) = \varphi_a(g_1)\varphi_a(g_2),$$

δηλαδή η φ είναι ομομορφισμός ομάδων.

Η φ_a είναι 1-1. Πράγματι, έστω $g \in \ker\varphi_a$. Τότε

$$a^{-1}ga = 1_G \Rightarrow g = 1_G \Rightarrow \ker\varphi_a = \{1_G\}.$$

Δηλαδή η φ είναι 1-1.

Η φ_a είναι επί. Πράγματι, έστω $g' \in G$. Τότε $\varphi_a(ag'a^{-1}) = g'$.
ii) Θα δείξουμε ότι $\mathrm{Inn}G \leq Aut(G)$. Είναι σαφές ότι $\mathrm{Inn}G \neq \emptyset$. Έστω $\varphi_a, \varphi_b \in \mathrm{Inn}G$. Τότε

$$\begin{aligned}(\varphi_a \circ \varphi_b)(g) &= \varphi_a(\varphi_b(g)) = \varphi_a(b^{-1}gb) \\ &= a^{-1}b^{-1}gba = (ba)^{-1}gba = \varphi_{ba}(g)\end{aligned}$$

για κάθε $g \in G$. Επομένως $\varphi_a \circ \varphi_b = \varphi_{ba} \in \mathrm{Inn}(G)$.
Έστω $\varphi_a \in \mathrm{Inn}(G)$. Τότε $\varphi_a^{-1} = \varphi_{a^{-1}} \in \mathrm{Inn}G$. Πράγματι, για κάθε $g \in G$ έχουμε

$$\begin{aligned}\varphi_a(\varphi_a^{-1}(g)) &= g \Rightarrow a^{-1}\varphi_a^{-1}(g)a = g \Rightarrow \\ \varphi_a^{-1}(g) &= aga^{-1} = (a^{-1})^{-1}ga^{-1} = \varphi_{a^{-1}}(g).\end{aligned}$$

iii) Θα δείξουμε ότι η απεικόνιση $\psi : G \to \mathrm{Inn}G,\ \ \psi(a) = \varphi_{a^{-1}}$ είναι επιμορφισμός ομάδων με $\ker\psi = Z(G)$. Παρατηρούμε ότι

$$\psi(ab) = \varphi_{(ab)^{-1}} = \varphi_{b^{-1}a^{-1}} = \varphi_{a^{-1}}\varphi_{b^{-1}} = \psi(a)\psi(b).$$

Η ψ είναι επί ($\psi(a^{-1}) = \varphi_a$). Τέλος έχουμε,$\ker\psi = \{a \in G : \varphi_{a^{-1}} = I_G\}$, όπου $I_G : G \to G,\ I_G(a) = a$. Παρατηρούμε ότι $\varphi_{a^{-1}} = I_G \Leftrightarrow \varphi_{a^{-1}}(g) = g$ για κάθε $g \in G \Leftrightarrow aga^{-1} = g \Leftrightarrow a \in Z(G)$. Από το πρώτο θεώρημα ισομορφισμών ομάδων έπεται ότι $G/Z(G) \simeq \mathrm{Inn}G$.

22.

23. *Υπόδειξη.* Η σχέση $[S_n, S_n] \subseteq A_n$ είναι σαφής αφού κάθε μεταθέτης είναι της μορφής $x^{-1}y^{-1}xy$, δηλαδή άρτια μετάθεση. Για την άλλη σχέση χρησιμοποιήστε ότι $(ij)(kl) = [(ij),(jl)(ik)]$.

24. Λύση. Έπεται άμεσα από την άσκηση 10.1 αφού $[D_n : H] = 2n/n = 2$.

25.

26. *Υπόδειξη iii*). Με το συμβολισμό της εκφώνησης και του Παραδείγματος 7.4(10), θεωρήστε απεικόνιση $G \to D_5$ με την ιδιότητα $r \mapsto \rho$ και $s \mapsto \sigma$.

27. *Λύση. 1ος τρόπος.* Αν $H \leq S_n$ με $[S_n : H] = 2$, τότε από την άσκηση 10.1 η H είναι κανονική στη S_n. Επειδή η ομάδα S_n/H έχει τάξη 2, έχουμε $\sigma^2 \in H$ για κάθε $\sigma \in S_n$. Ειδικά, αν το σ είναι κύκλος μήκους 3, τότε

$$\sigma^2 = \sigma^{-1} \in H \Rightarrow \sigma \in H$$

αφού $H \leq S_n$. Επειδή η A_n παράγεται από τους κύκλους μήκους 3 (άσκηση 8.25), έχουμε $A_n \subseteq H$. Από αυτό έπεται ότι $A_n = H$ αφού $|A_n| = |H| < \infty$.

2ος τρόπος. Αν $H \leq S_n$ με $[S_n : H] = 2$, τότε από την άσκηση 10.1 η H είναι κανονική στη S_n και $S_n/H \simeq C_2$ κυκλική ομάδα τάξης 2. Έστω $\varphi : S_n \to S_n/H$ ο φυσικός επιμορφισμός. Επειδή η ομάδα S_n/H είναι αβελιανή, από τη σχέση

$$(st) = (si)(tj)(ij)(tj)^{-1}(si)^{-1},$$

έπεται ότι η φ παίρνει την ίδια τιμή σε όλες τις αντιμεταθέσεις. Επομένως σε κάθε γινόμενο αντιμεταθέσεων με άρτιο πλήθος παραγόντων παίρνει την τιμή $1 \in C_2$. Αυτό σημαίνει ότι $A_n \subseteq \ker\varphi = H$. Από αυτό έπεται ότι $A_n = H$ αφού $|A_n| = |H| < \infty$.

28.

29.

30. *Λύση.* Έστω $g \in G, h \in H$. Τότε

$$ghg^{-1} \in H \Leftrightarrow g^{-2}ghg^{-1} \in H \Leftrightarrow hg^{-2}ghg^{-1} \in H \Leftrightarrow (hg^{-1}) \in H$$

που ισχύει.

31. *Λύση.* Αν $g \in G$ και $a \in N$, τότε $\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(a)$ διότι η H είναι αβελιανή. Άρα

$$g^{-1}aga^{-1} \in ker\varphi \subseteq N.$$

Από την τελευταία σχέση έπεται ότι $g^{-1}ag \in G$.

32. *Υπόδειξη.* Έστω $H \leq G$ με $|H| = |N|$. Θεωρώντας το φυσικό επιμορφισμό, $\pi : G \to G/N$, δείξτε ότι η τάξη της $\pi(H)$ διαιρεί το $|N|$ και το $[G : N]$. Άρα $\pi(H) = 1$. Αυτό σημαίνει ότι $H \subseteq ker\pi = N$. Επειδή $|H| = |N| < \infty$, έπεται ότι $H = N$.

33. Δείξτε ότι ο πυρήνας του ομομορφισμού ομάδων $G \to Aut(N)$, $g \mapsto f_g$, όπου $f_g(x) = xgx^{-1}$, είναι η G.

Επαναληπτικές Ασκήσεις: Κεφάλαια 7-10

1. i) Διατυπώστε το θεώρημα του Lagrange για πεπερασμένες ομάδες και δείξτε ότι κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική. Αληθεύει το αντίστροφο τοπου θεωρήματος του Lagrange;
   ii) Δείξτε ότι κάθε κυκλική ομάδα είναι αβελιανή. Αληθεύει το αντίστροφο;
   iii) Έστω G ομάδα τάξης p, όπου p περιττός πρώτος. Δείξτε ότι η απεικόνιση $\varphi : G \to G, a \mapsto a^2$ είναι αυτομορφισμός της G.
2. Πέντε φοιτητές περιμένουν στη ουρά στις ώρες γραφείου της Βασικής Άλγεβρας με τη διάταξη Α,Β,Γ,Δ,Ε. Κάθε λεπτό, ακριβώς δύο φοιτητές από αυτούς εναλλάσσουν τις θέσεις τους. Είναι δυνατό μετά από ακριβώς 15 λεπτά να έχει προκύψει η διάταξη Ε,Δ,Γ,Β,Α ;
3. Έστω G πεπερασμένη ομάδα τάξης n η οποία έχει τουλάχιστον δύο στοιχεία a, b τάξης 2.
   i) Δώστε παράδειγμα τέτοιας ομάδας G.
   ii) Αληθεύει ότι ο n είναι άρτιος;
   iii) Δείξτε ότι αν $ab = ba$, τότε ο n είναι πολλαπλάσιος του 4.
   iv) Αληθεύει ότι η G είναι κυκλική;
   v) Είναι δυνατό η G να έχει ακριβώς δύο στοιχεία τάξης 2;
   vi) Αν $\varphi : G \to H$ είναι ομομορφισμός ομάδων και η H έχει περιττή τάξη, δείξτε ότι $|ker\varphi| \geq 4$.
4. i) Αληθεύει ότι η ομάδα $(\mathbb{Q}, +)$ είναι κυκλική;
   ii) Δείξτε ότι η ομάδα $G = \{2^m \cdot 3^n \in \mathbb{Q} : m, n \in \mathbb{Z}\}$ με πράξη τον πολλαπλασιασμό είναι ισόμορφη με την προσθετική ομάδα του δακτυλίου $\mathbb{Z}[i]$.
5. Έστω G ομάδα με τάξη το πολύ 15 που περιέχει στοιχεία r, s με τάξεις $5, 2$ αντίστοιχα.
   i) Βρείτε την τάξη της G.
   ii) Δώστε παράδειγμα τέτοιας G που δεν είναι αβελιανή.
   iii) Δείξτε ότι αν η G είναι αβελιανή, τότε η G είναι κυκλική.
   iv) Βρείτε την τάξη του στοιχείου $r^{-1}sr$. Στη συνέχεια δείξτε ότι αν η G έχει μοναδικό στοιχείο τάξης 2, τότε είναι κυκλική.
   v) Δείξτε ότι κάθε στοιχείο της G γράφεται μοναδικά στην μορφή $r^i s^j$, όπου $i \in \{0, 1, 2, 3, 4\}$ και $j \in \{0, 1\}$.
6. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7$.
   i) Βρείτε την ανάλυση σε γινόμενο ανά δύο ξένων κύκλων, την τάξη και το πρόσημο των σ και σ^{2019}.
   ii) Βρείτε τους γεννήτορες της ομάδας $< \sigma^{2019} >$.
   iii) Αληθεύει ότι υπάρχει $\tau \in S_7$ με $\tau^{2020} = \sigma$;
   iv) Αληθεύει ότι $(13) \in < \sigma >$;
   v) Βρείτε τους ακέραιους m ώστε η ομάδα $< \sigma^m >$ να περιέχει στοιχείο τάξης 6.
7. Έστω $\varphi : S_5 \to H$ ομομορφισμός ομάδων.
   i) Δείξτε ότι $(12345) \in ker\varphi$ αν $|H| = 12$.
   ii) Δείξτε ότι $(123) \in ker\varphi$ αν η H είναι αβελιανή.
8. Έστω $f(x) = (x^2 + x + 1)(x^3 + x + 1) \in \mathbb{Z}_2[x]$. Θεωρούμε το κύριο ιδεώδες $I =< f(x) >$ του $\mathbb{Z}_2[x]$ και το δακτύλιο πηλίκο $R = \mathbb{Z}_2[x]/I$.
   i) Παραστήστε την ομάδα $U(R)$ των αντιστρέψιμων στοιχείων του R ως ευθύ γινόμενο δύο μη τετριμμένων ομάδων.
   ii) Ποια είναι η τάξη της $U(R)$;
   iii) Αληθεύει ότι η $U(R)$ είναι κυκλική;

Ενδεικτικές Λύσεις Επαναληπτικών Ασκήσεων

1. Τα πρώτα δύο υποερωτήματα είναι γνωστά από τη θεωρία. Για το τρίτο υποερώτημα σημειώνουμε αρχικά ότι η G είναι αβελιανή (από τα προηγούμενα υποερωτήματα). Άρα για κάθε $a, b \in G$,

$$\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b),$$

όπου στη δεύτερη ισότητα χρησιμοποιήσαμε ότι $ab = ba$. Αν $a \in ker\varphi$, δηλαδή $a^2 = 1_G$, τότε η τάξη του a διαιρεί το 2. Επίσης, επειδή $a \in G$, η τάξη του a διαιρεί την τάξη της G που είναι περιττή. Άρα η τάξη του a ισούται με 1 και $a = 1_G$. Άρα ο ομομορφισμός φ είναι 1-1. Τέλος έχουμε μια 1-1 απεικόνιση από πεπερασμένο σύνολο G στο G. Αυτή είναι αναγκαστικά επί.

2. Υποθέτοντας ότι η αρχική διάταξη των φοιτητών είναι 12345, τότε μετά από ακριβώς t εναλλαγές θέσεων, θα προκύψει διάταξη που δίνεται από μετάθεση της μορφής $(i_1j_1)(i_2j_2)...(i_tj_t)$, (γινόμενο αντιμεταθέσεων που το πλήθος τους είναι t). Αν το t είναι περιττός, μια τέτοια μετάθεση είναι περιττή. Όμως η διάταξη 54321 αντιστοιχεί στη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

η οποία είναι άρτια καθώς $\sigma = (15)(24)$. Επειδή δεν υπάρχει μετάθεση που να είναι και άρτια και περιττή, συμπεραίνουμε ότι η διάταξη 54321 δεν μπορεί να επιτευχθεί μετά ακριβώς t λεπτά αν ο t είναι περιττός.

3. i) Η S_3 έχει ακριβώς τρία στοιχεία τάξης 2, τα $(12), (13), (23)$.
   ii) Ναι, καθώς κάθε στοιχείο πεπερασμένης ομάδας τάξης n έχει τάξη διαιρέτη του n.
   iii) Ναι, καθώς αν $ab = ba$, τότε το πεπερασμένο σύνολο $H = \{1, a, b, ab\}$ έχει 4 στοιχεία (δείξτε ότι τα $1, a, b, ab$ είναι διακεκριμένα) και είναι κλειστό ως προς τον πολλαπλασιασμό της G (δείξτε το). Άρα είναι υποομάδα της G και από το θεώρημα του Lagrange έχουμε $4||G|$.
   iv) Ξέρουμε ότι κάθε πεπερασμένη κυκλική ομάδα έχει το πολύ ένα στοιχείο τάξης 2 (κανένα αν είναι περιττής τάξης από το θεώρημα του Lagrange, ακριβώς ένα αν είναι άρτιας τάξης από το θεώρημα 9.14). Συνεπώς η G δεν είναι κυκλική.
   v) Όχι. Θα δούμε ότι κάθε ομάδα G άρτιας τάξης έχει περιττό πλήθος στοιχείων τάξης 2.
   Πράγματι, ξέρουμε ότι για κάθε $a \in G$, τα a, a^{-1} έχουν την ίδια τάξη. Επίσης ξέρουμε ότι ένα $a \in G$ έχει τάξη 2 αν και μόνο αν $a = a^{-1}$ και $a \neq 1_G$. Άρα το υποσύνολο A της G που αποτελείται από τα στοιχεία που έχουν τάξη μεγαλύτερη του 2 έχει άρτιο πλήθος στοιχείων. Από την ξένη ένωση $G = \{1_G\} \cup G_2 \cup A$, όπου G_2 είναι το υποσύνολο των στοιχείων τάξης 2, συμπεραίνουμε ότι $|G| = 1 + |G_2| + |A|$, και επειδή οι ακέραιοι $|G|, |A|$ είναι άρτιοι, παίρνουμε ότι ο $|G_2|$ είναι περιττός.
   vi) Για κάθε $a \in G$ το στοιχείο $\varphi(g) \in H$ έχει τάξη που διαιρεί την τάξη της H και άρα έχει περιττή τάξη. Αν το $a \in G$ έχει τάξη 2, τότε από τη σχέση

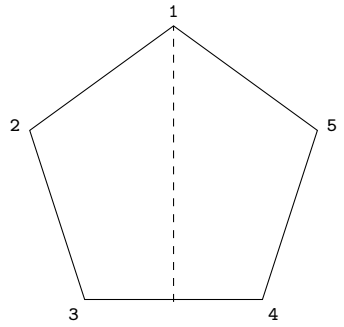
$$\varphi(a^2) = \varphi(1_G) \Rightarrow \varphi(a)^2 = 1_H,$$

συμπεραίνουμε ότι το $\varphi(a)$ έχει τάξη διαιρέτη του 2. Συνεπώς για κάθε στοιχείο a τάξης 2 της G, το $\varphi(g)$ έχει τάξη 1, δηλαδή $\varphi(g) = 1_H$, ισοδύναμα $g \in ker\varphi$. Από το προηγούμενο υποερώτημα η G διαθέτει τουλάχιστον 3 στοιχεία τάξης 2 και άρα αυτά ανήκουν στον πυρήνα $ker\varphi$. Μαζί με το 1_G έχουμε τουλάχιστον 4 στοιχεία στο $ker\varphi$

4. i) Βλ. άσκηση $9.2iii$).
   ii) Δείξτε ότι η απεικόνιση $\mathbb{Z}[i] \to G, a + bi \mapsto 2^a \cdot 3^b$ είναι ισομορφισμός ομάδων.

5. i) Η τάξη της G είναι πολλαπλάσιο και του 2 και του 5, άρα του 10, και μικρότερη ή ίση του 15. Άρα $|G| = 10$.

   ii) Ένα παράδειγμα είναι η διεδρική ομάδα D_5 (συμμετρίες του κανονικού πενταγώνου). Εδώ μια επιλογή για το στοιχείο r είναι η περιστροφή του επιπέδου κατά γωνία $2\pi/5$ και μια επιλογή για το στοιχείο s είναι ανάκλαση γύρω από ευθεία που διέρχεται από κορυφή και είναι κάθετη στην απέναντι πλευρά.



   Με τις παραπάνω επιλογές, στο διάγραμμα η r αντιστοιχεί στο κύκλο (12345) και η s στη μετάθεση $(25)(34)$. Εύκολα επαληθεύεται ότι $(12345)(25)(34) \neq (34)(25)(12345)$ και άρα η D_5 δεν είναι αβελιανή.
   Ξέρουμε ότι $|D_5| = 2 \cdot 5 = 10$.

   iii) Επειδή $rs = sr$ και οι τάξεις των r, s είναι σχετικά πρώτες, έπεται από άσκηση που κάναμε στο μάθημα ότι η τάξη του rs ισούται με $5 \cdot 2 = 10$. Επειδή $|G| = 10$, η G είναι κυκλική. (Σημείωση. Σε γραπτό εξετάσεων πρέπει να υπάρχει η απόδειξη της άσκησης αυτής. Βλ. πρώτο μέρος της λύσης της άσκησης 8.2).

   iv) Επειδή $(r^{-1}sr)^2 = r^{-1}s^2r = r^{-1}1_Gr = 1_G$, η τάξη του $r^{-1}sr$ είναι 1 ή 2. Αν $r^{-1}sr = 1_G$, τότε $s = rr^{-1} = 1_G$ αδύνατο, αφού το s έχει τάξη 2. Συνεπώς η τάξη του $r^{-1}sr$ ισούται με 2.
   Αν η G έχει μοναδικό στοιχείο τάξης 2, τότε $r^{-1}sr = s$, δηλαδή $rs = sr$. Είδαμε στο προηγούμενο υποερώτημα ότι το rs έχει τάξη 10 και άρα η G είναι κυκλική.

   v) Παρόμοιο επιχείρημα με το Παράδειγμα $8.8(1)ii)$, όπου $H =< r >, K =< s >$.

6. i) Υπολογίζοντας κατά τα γνωστά βρίσκουμε ότι η ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων είναι $\sigma = (1427)(356)$. Ως κύκλος με άρτιο μήκος, η μετάθεση (1427) είναι περιττή. Ως κύκλος με περιττό μήκος, η μετάθεση (356) είναι άρτια. Άρα το γινόμενο $\sigma = (1427)(356)$ είναι περιττή. Από την ανάλυση της σ σε γινόμενο ξένων ανά δύο κύκλων $\sigma = (1427)(356)$, έχουμε ότι η τάξη της είναι $\varepsilon\kappa\pi(4, 3) = 12$.
   Επειδή η σ είναι περιττή μετάθεση και ο ακέραιος 2019 είναι περιττός, η μετάθεση σ^{2019} είναι περιττή. Επειδή $2019 \equiv 3 \mod 12$, έχουμε

$$\sigma^{2019} = \sigma^3 = (1427)^3(356)^3 = (1724),$$

   όπου στη δεύτερη ισότητα χρησιμοποιήσαμε ότι οι κύκλοι $(1427), (356)$ αντιμετατίθενται. Αυτή είναι η ζητούμενη ανάλυση της σ^{2019}. Άρα η σ^{2019} έχει τάξη 4.

   ii) Είδαμε πριν ότι η σ^{2019} έχει τάξη 4. Άρα η κυκλική ομάδα $H =< \sigma^{2019} >$ έχει τάξη 4. Επειδή η H είναι υποομάδα τάξης 4 της κυκλικής ομάδας $< \sigma >$ που έχει τάξη 12, η ταξινόμηση των υποομάδων κυκλικής ομάδας (βλ. Θεώρημα 9.14), δίνει ότι $H =< \sigma^{12/4} >= \{1, \sigma^3, \sigma^6, \sigma^9\}$. Υπολογίζοντας τάξεις στοιχείων, βλέπουμε ότι τα σ^3, σ^9 είναι τα στοιχεία της H που έχουν τάξη 4. Άρα τα στοιχεία αυτά είναι οι ζητούμενοι γεννήτορες.

   iii) Δεν αληθεύει, καθώς η μετάθεση τ^{2020} είναι άρτια (ο ακέραιος 2020 είναι άρτιος), ενώ είδαμε ότι η σ είναι περιττή. Ξέρουμε ότι δεν υπάρχει μετάθεση που να είναι και άρτια και περιττή.

   iv) Η ομάδα $< \sigma >$ είναι κυκλική και έχει άρτια τάξη από το πρώτο υποερώτημα. Ως τέτοια, περιέχει μοναδικό στοιχείο τάξης 2, το σ^6. Εύκολα επαληθεύεται ότι $\sigma^6(1) = 2$. Άρα

$\sigma^6 \neq (13)$ και $(13) \notin < \sigma >$. [Για διαφορετικό επιχείρημα, βλ. λύση της άσκησης $8.19iv$)]

v) Ξέρουμε ότι μια πεπερασμένη κυκλική ομάδα τάξης n περιέχει στοιχείο τάξης d αν και μόνο αν $d > 0$ και $d|n$. Στη συγκεκριμένη περίπτωση, αυτό ισοδυναμεί με το 6 να διαιρεί την τάξη της ομάδας $< \sigma^m >$ δηλαδή το $12/\mu\kappa\delta(12, m)$. Θεωρώντας $m = 0, 1, ..., 11$, βλέπουμε ότι $m = 1, 2, 5, 7, 9, 10, 11$. Οι ζητούμενοι ακέραιοι είναι οι $m \equiv 1, 2, 5, 7, 9, 10, 11 \mod 12$.

7. i) Επειδή η $\sigma = (12345)$ είναι κύκλος μήκος 5, έχουμε $\sigma^5 = 1$ και άρα $\varphi(\sigma)^5 = 1_H$, αφού φ ομομορφισμός ομάδων. Επομένως η τάξη του $\varphi(\sigma)$ είναι διαιρέτης του 5. Από την άλλη μεριά, επειδή $|H| = 12$, η τάξη του $\varphi(\sigma)$ είναι διαιρέτης του 12, και άρα ισούται με 1. Δηλαδή $\varphi(\sigma) = 1_H$.

ii) Έχουμε

$$\varphi(123) = \varphi((13)(12)) = \varphi(13)\varphi(12) = \varphi(12)\varphi(13)$$
$$= \varphi((12)(13)) = \varphi((123)^2) = \varphi(123)^2,$$

όπου στην τρίτη ισότητα χρησιμοποιήσαμε ότι η H είναι αβελιανή. Άρα $\varphi(123) = 1_H$ δηλαδή $(123) \in ker\varphi$.

8. Παρόμοιο με το Παράδειγμα 9.5(4).

Δράσεις ομάδων και τα θεωρήματα Sylow

Ένας ιδιαίτερα αποτελεσματικός τρόπος μελέτης μιας ομάδας είναι μέσω των δράσεων της σε σύνολα. Στο κεφάλαιο αυτό εισάγουμε την έννοια της δράσης. Στη συνέχεια αποδεικνύουμε τα φημισμένα θεωρήματα Sylow που είναι από τα πιο σημαντικά αποτελέσματα στη θεωρία των πεπερασμένων ομάδων.

Βασικά σημεία

- δράσεις ομάδων
- τροχιές και σταθεροποιούσες υποομάδες
- εξίσωση κλάσεων
- θεωρήματα Sylow και εφαρμογές

11.1. Ορισμοί και παραδείγματα

Ορισμός 11.1. *Έστω G μια ομάδα και X ένα σύνολο. Μια δράση της G στο X είναι μια απεικόνιση*

$$\cdot : G \times X \to X, (g, x) \mapsto g \cdot x,$$

τέτοια ώστε

(1) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ *για κάθε* $g_1, g_2 \in G, x \in X$,
(2) $1 \cdot x = x$ *για κάθε* $x \in G$, *όπου* 1 *είναι το ουδέτερο στοιχείο της* G.

Δεδομένης της παραπάνω δράσης, θα λέμε συχνά ότι το X είναι G-σύνολο ή ότι η G δρα στο X μέσω της $\cdot$.

Παραδείγματα 11.2.

(1) Η συμμετρική ομάδα S_n δρα στο $X = \{1, 2, ..., n\}$ με $\sigma \cdot i = \sigma(i)$.
Η επαλήθευση των δύο ιδιοτήτων του ορισμού είναι άμεση, η πρώτη ιδιότητα έπεται από τον ορισμό της σύνθεσης απεικονίσεων και η δεύτερη από το γεγονός ότι το ουδέτερο στοιχείο της S_n είναι η ταυτοτική απεικόνιση $\{1, 2, ..., n\} \to \{1, 2, ..., n\}$.

(2) Η γενική γραμμική ομάδα $GL(2,\mathbb{R})$ των 2×2 αντιστρέψιμων πινάκων δρα στο $\mathbb{R}^2$ μέσω γινομένου πινάκων

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}.$$

Η πρώτη ιδιότητα του ορισμού έπεται από την προσεταιριστική ιδιότητα του γινομένου πινάκων.

Στη συνέχεια θα δούμε μερικά γενικά παραδείγματα δράσεων που θα εμφανιστούν συχνά παρακάτω.

(3) **Δράση της G στη G μέσω αριστερού πολλαπλασιασμού.** Η G δρα στο σύνολο $X=G$ μέσω της

$$G\times X\to X, (g,x)\mapsto gx,$$

όπου το gx είναι το γινόμενο των g,x στη G. Η πρώτη ιδιότητα του παραπάνω ορισμού είναι η προσεταιριστική ιδιότητα της ομάδας και η δεύτερη είναι ο ορισμός του ουδέτερου στοιχείου.

(4) **Δράση της G στη G μέσω συζυγίας.** Η G δρα στο σύνολο $X=G$ μέσω της

$$G\times X\to X, (g,x)\mapsto gxg^{-1}.$$

Άμεσα επαληθεύονται οι ιδιότητας του ορισμού, καθώς έχουμε για κάθε $g_1,g_2\in G$,

$$g_1(g_2xg_2^{-1})g_1^{-1}=(g_1g_2)x(g_1g_2)^{-1} \text{ και } g_1 1 g_1^{-1}=1.$$

(5) **Δράση της G στη στο σύνολο των υποομάδων της μέσω συζυγίας.** Εδώ θεωρούμε το σύνολο X των υποομάδων της G. Η G δρα στο X μέσω της

$$G\times X\to X, (g,K)\mapsto gKg^{-1}.$$

(6) **Δράση της G στο G/H μέσω αριστερού πολλαπλασιασμού.** Θεωρούμε υποομάδα H της G και το σύνολο $X=G/H$ των αριστερών κλάσεων της H στη G. Η G δρα στο $X=G/H$ μέσω της

$$G\times X\to X, (g,aH)\mapsto (ga)H.$$

Στα δύο τελευταία παραδείγματα αφήνουμε ως άσκηση την επαλήθευση ότι πράγματι έχουμε δράσεις (μη ξεχάσετε στο τελευταίο να ελέγξετε ότι η απεικόνιση είναι καλά ορισμένη).

(7) **Περιορισμός δράσης σε υποομάδα.** Έστω ότι η ομάδα G δρα στο σύνολο X και έστω H υποομάδα της G. Θεωρώντας τον περιορισμό της απεικόνισης

$$G\times X\to X, (g,x)\mapsto g\cdot x,$$

στο υποσύνολο $H\times X$ του $G\times X$, είναι σαφές ότι έχουμε δράση της H στο X.

Παρατήρηση. (Σχέση δράσης με μεταθέσεις) Έστω X ένα G-σύνολο με αντίστοιχη δράση

$$\cdot : G\times X\to X, (g,x)\mapsto g\cdot x.$$

Θυμίζουμε ότι έχουμε την ομάδα $S(X)$ των μεταθέσεων του X, τα στοιχεία της οποίας είναι οι 1-1 και επί απεικονίσεις $X\to X$ και η πράξη είναι η σύνθεση συναρτήσεων. Θα δούμε εδώ ότι από την προηγούμενη δράση επάγεται με φυσικό τρόπο ομομορφισμός ομάδων $G\to S(X)$.

Πράγματι, για κάθε $g\in G$ ορίζεται η απεικόνιση

$$\alpha_g : X\to X, x\mapsto g\cdot x.$$

Εύκολα επαληθεύεται η α_g είναι 1-1 και επί: Για το 1-1 παρατηρούμε ότι

$$\begin{aligned} & g \cdot x_1 = g \cdot x_2 \Rightarrow \\ & g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2) \Rightarrow \\ & (g^{-1}g) \cdot x_1 = (g^{-1}g) \cdot x_2 \\ & 1 \cdot x_1 = 1 \cdot x_2 \\ & x_1 = x_2. \end{aligned}$$

Για το επί σημειώνουμε ότι αν $y \in G$, τότε θέτοντας $x = g^{-1} \cdot y$ έχουμε:

$$\begin{aligned} g \cdot x &= g \cdot (g^{-1} \cdot y) \\ &= (g^{-1}g) \cdot x \\ &= 1 \cdot x \\ &= x. \end{aligned}$$

Έτσι λαμβάνουμε μια απεικόνιση

$$\alpha : G \to S(X), g \mapsto \alpha_g$$

και είναι υπόθεση ρουτίνας η απόδειξη ότι αυτή είναι ομομορφισμός ομάδων.

Στην απόδειξη ποίου θεωρήματος του Κεφαλαίου 9 χρησιμοποιήσαμε την προηγούμενη ιδέα;

Θα δούμε τώρα και ένα αποτέλεσμα στην αντίστροφη κατεύθυνση. Έστω ότι G είναι ομάδα και X σύνολο (όχι αναγκαστικά G-σύνολο). Έστω ότι έχουμε έναν ομομορφισμό ομάδων $\alpha : G \to S(X)$. Ορίζουμε την απεικόνιση

$$G \times X \to X, (g, x) \mapsto \alpha(g)(x).$$

Αφήνουμε ως άσκηση την επαλήθευση ότι πρόκειται περί δράσης της G στο X και επίσης ότι ο ομομορφισμός ομάδων που επάγεται από αυτή είναι ο αρχικός $\alpha : G \to S(X)$.

Μιλώντας πρόχειρα, το συμπέρασμα της παρατήρησης είναι ότι είτε μιλάμε για δράση ομάδας G σε σύνολο X είτε για ομομορφισμό ομάδων από τη G στις μεταθέσεις του X, είναι το ίδιο πράγμα.

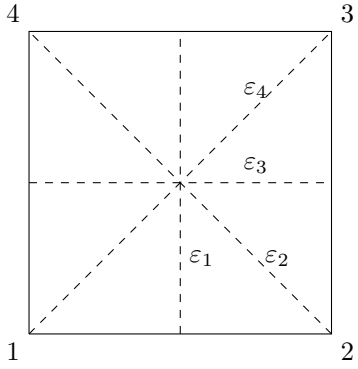
Ας δούμε δύο παραδείγματα όπου χρησιμοποιείται η προηγούμενη ιδέα.

Παραδείγματα 11.3.

(1) Θεωρούμε τη διεδρική ομάδα D_4, δηλαδή την ομάδα των συμμετριών του τετραγώνου. Από το Παράδειγμα 7.4 (10), ξέρουμε ότι

$$D_4 = \{1, r_1, r_2, r_3, s_1, s_2, s_3, s_4\},$$

όπου r_i είναι η περιστροφή κατά γωνία $\frac{\pi}{2}i$ και s_j είναι η ανάκλαση ως προς τον άξονες συμμετρίας ε_j που φαίνεται στο σχήμα. Η D_4 δρα στο σύνολο $X = \{1, 2, 3, 4\}$ των κορυφών του τετραγώνου με $f \cdot P = f(P)$, όπου $f \in D_4$ και $P \in X$.



Για παράδειγμα $r_1 \cdot 1 = 2$, $r_1 \cdot 2 = 3$, $r_1 \cdot 3 = 4$, $r_1 \cdot 4 = 1$. Σύμφωνα με την Παρατήρηση που είδαμε πριν, για τον αντίστοιχο ομομορφισμό ομάδων

$$\alpha : D_4 \to S(X)$$

έχουμε

$$\alpha_1 = 1, \alpha_{r_1} = (1234), \alpha_{r_2} = (13)(24), \alpha_{r_3} = (1432),$$
$$\alpha_{s_1} = (12)(34), \alpha_{s_2} = (13), \alpha_{s_3} = (14)(23), \alpha_{s_4} = (24).$$

Παρατηρούμε ότι εδώ ο ομομορφισμός α είναι μονομορφισμός. Μας επιτρέπει να βλέπουμε την ομάδα D_4 ως συγκεκριμένη υποομάδα της S_4. Καλό είναι το συγκριθεί το παραπάνω με το Παράδειγμα 8.5 (6).

(2) Το δεύτερο παράδειγμα αφορά άπειρες ομάδες. Έστω ομάδα G που έχει γνήσια υποομάδα K πεπερασμένου δείκτη. Θα δείξουμε ότι η G έχει γνήσια κανονική υποομάδα πεπερασμένου δείκτη.

Θεωρούμε τη δράση της G στο $X = G/K$ μέσω αριστερού πολλαπλασιασμού. Σύμφωνα με την παρατήρηση που είδαμε πριν, έχουμε ομομορφισμό ομάδων $\alpha : G \to S_X$. Επειδή το X είναι πεπερασμένο σύνολο, η ομάδα S_X είναι πεπερασμένη. Ο πυρήνας $ker\alpha$ είναι κανονική υποομάδα της G και επιπλέον έχει πεπερασμένο δείκτη στη G διότι από το πρώτο θεώρημα ισομορφισμών ομάδων έπεται ότι η ομάδα $G/ker\alpha$ είναι ισόμορφη με υποομάδα της πεπερασμένης S_X.

11.2. Τροχιές και σταθεροποιούσες υποομάδες

Έστω G μια ομάδα και X ένα G σύνολο. Ορίζουμε την ακόλουθη σχέση στο X

$$x \sim x' \Leftrightarrow \exists g \in G, g \cdot x = x'.$$

Εύκολα επαληθεύεται ότι είναι σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του x είναι $[x] = \{g \cdot x \in X : g \in G\}$ και τη συμβολίζουμε συνήθως με $\mathcal{O}_x$

Ορισμός 11.4. *Έστω G μια ομάδα, X ένα G σύνολο και $x \in X$.*

(1) *Η **τροχιά** του x είναι το σύνολο*

$$\mathcal{O}_x = \{g \cdot x \in X : g \in G\}.$$

(2) *Η **σταθεροποιούσα υποομάδα** G_x που αντιστοιχεί στο x είναι το σύνολο*

$$G_x = \{g \in G : g \cdot x = x\}.$$

Αφήνουμε ως άσκηση την επαλήθευση ότι το G_x είναι πράγματι υποομάδα της G.

Παρατήρηση. Από την Παράγραφο 2.2 ξέρουμε ότι δύο τροχιές ή ταυτίζονται ή είναι ξένα σύνολα και ότι το X μπορεί να παρασταθεί ως ξένη ένωση τροχιών.

Παραδείγματα 11.5.

(1) Έστω

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 9 & 8 & 6 & 7 & 1 \end{pmatrix} \in S_9$$

και έστω $G =< \sigma >$ η κυκλική υποομάδα της S_9 που παράγεται από το σ. Η G δρα στο σύνολο $X = \{1, 2, ..., 9\}$ με $\sigma \cdot i = \sigma(i)$. Για την τροχιά του $1 \in X$ έχουμε

$$\sigma(1) = 3,\ \sigma^2(1) = \sigma(3) = 5,\ \sigma^3(1) = \sigma(5) = 9,\ \sigma^4(1) = \sigma(9) = 1$$

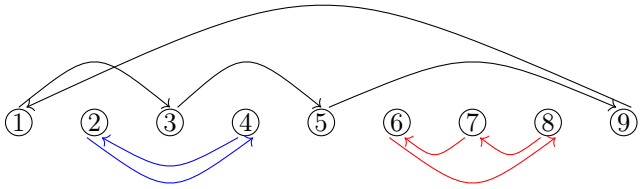
και άρα

$$\mathcal{O}_1 = \{1, 3, 5, 9\}$$

Όμοια έχουμε

$$\mathcal{O}_2 = \{2, 4\}, \mathcal{O}_6 = \{6, 8, 7\}$$

Εποπτικά, η δράση της G και οι τρεις τροχιές φαίνονται στο ακόλουθο σχήμα.



Έχουμε την ξένη ένωση

$$X = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_6.$$

Σημειώνουμε ότι οι τροχιές αντιστοιχούν στην ανάλυση της σ σε γινόμενο κύκλων ξένων ανά δύο

$$\sigma = (1359)(24)(678)$$

που είδαμε στο Παράδειγμα 7.14 (1).

Εύκολα επαληθεύεται ότι έχουμε τις σταθεροποιούσες υποομάδες

$$G_1 = G_3 = G_5 = G_9 =< \sigma^4 >= \{1, \sigma^4, \sigma^8\},$$
$$G_2 = G_4 =< \sigma^2 >= \{1, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\},$$
$$G_6 = G_7 = G_8 =< \sigma^3 >= \{1, \sigma^3, \sigma^6, \sigma^9\}.$$

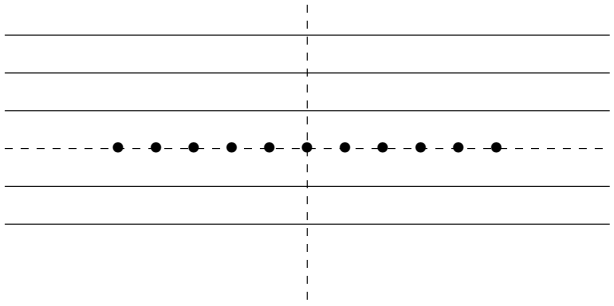
(2) Θεωρούμε την ομάδα $G = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{R}\}$ με πράξη τον πολλαπλασιασμό πινάκων. Η G δρα στο επίπεδο $\mathbb{R}^2$ όπως στο Παράδειγμα 11.2(2),

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} c_1 + ac_2 \\ c_2 \end{pmatrix}.$$

Εδώ οι τροχιές είναι δύο ειδών,

η τροχιά ενός σημείου $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ με $c_2 \neq 0$ είναι η ευθεία $y = c_2$

η τροχιά ενός σημείου $P = \begin{pmatrix} c_1 \\ 0 \end{pmatrix}$ είναι το μονοσύνολο $\{P\}$.



Ας δούμε τώρα τις τροχιές και τις σταθεροποιούσες υποομάδες για τα Παραδείγματα 11.2 (2), (3).

Παραδείγματα 11.6. Έστω G ομάδα.

(1) Δράση της G στη G μέσω συζυγίας. Εδώ η τροχιά του $x \in G$ είναι

$$\mathcal{O}_x = \{gxg^{-1} \in G : g \in G\}$$

και ονομάζεται **κλάση συζυγίας** του x. Συμβολίζεται συχνά με $cl(x)$. Η σταθεροποιούσα υποομάδα του $x \in G$ είναι

$$G_x = \{g \in G : gx = xg\}$$

και ονομάζεται **κεντροποιούσα υποομάδα** του x. Συνήθως συμβολίζεται με $C_G(x)$.

Για παράδειγμα, αν $G = S_3$ και $x = (12), y = (123)$, τότε

$$cl(x) = \{(12), (13), (23)\} \text{ και } G_x = \{e, (12)\},$$
$$cl(y) = \{(123), (132)\} \text{ και } G_y = \{e, (123), (132)\},$$

(2) Δράση της G στη στο σύνολο των υποομάδων της μέσω συζυγίας. Δύο υποομάδες K_1, K_2 της G λέγονται **συζυγείς** αν $K_1 = gK_2g^{-1}$ για κάποιο $g \in G$.

Για παράδειγμα, οι υποομάδες $< (12) >, < (13) >, < (23) >$ της S_3 είναι συζυγείς ανά δύο.

Θεωρώντας τη δράση της G στο σύνολο των υποομάδων της, βλ. Παράδειγμα 11.2 (5), βλέπουμε ότι η τροχιά μια υποομάδας K είναι το σύνολο των υποομάδων της G που είναι συζυγείς με την K. Επίσης η σταθεροποιούσα υποομάδα που αντιστοιχεί στην K είναι

$$\{g \in G : gKg^{-1} = K\}.$$

Αυτή λέγεται η **κανονικοποιούσα υποομάδα** της K και συμβολίζεται συνήθως με $N_G(K)$. Σημειώνουμε ότι η K είναι κανονική υποομάδα της $N_G(K)$. Μάλιστα η $N_G(K)$ είναι η μέγιστη υποομάδα της G στην οποία η K είναι κανονική. Ιδιαίτερα, η υποομάδα K είναι κανονική στη G αν και μόνο αν $N_G(K) = G$.

Το ακόλουθο θεώρημα λέει ότι το πλήθος των στοιχείων μιας τροχιάς ισούται με το δείκτη της αντίστοιχης σταθεροποιούσας υποομάδας. Ποτέ δεν υποτιμούμε αποτέλεσμα που απαριθμεί κάτι.

Θεώρημα 11.7 (θεώρημα τροχιάς-σταθεροποιούσας υποομάδας)**.** *Έστω G μια ομάδα, X ένα G σύνολο και $x \in X$. Τότε*

$$|\mathcal{O}_x| = [G : G_x].$$

Απόδειξη. Έστω $g, h \in G$. Επειδή έχουμε

$$g \cdot x = h \cdot x \Leftrightarrow x = g^{-1}hx \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow gG_x = hG_x,$$

έπεται ότι η απεικόνιση

$$G/G_x \to \mathcal{O}_x, gG_x \mapsto g \cdot x$$

είναι καλά ορισμένη και 1-1. Είναι σαφές ότι είναι και επί, οπότε $[G : G_x] = |\mathcal{O}_x|$. □

Από το προηγούμενο θεώρημα και τα παραδείγματα 11.2(4) και 11.2(5) έπεται άμεσα το εξής.

Πόρισμα 11.8. *Έστω G πεπερασμένη ομάδα, $x \in G$ και $K \leq G$ και . Τότε ισχύουν τα εξής.*

(1) *Το πλήθος των στοιχείων της κλάσης συζυγίας του x ισούται με το δείκτη $[G : C_G x]$ της κεντροποιούσας υποομάδας.*
(2) *Το πλήθος των υποομάδων της G που είναι συζυγείς με την K ισούται με το δείκτη $[G : N_G(K)]$ της κανονικοποιούσας υποομάδας.*

Ξένη ένωση τροχιών. Έστω ότι έχουμε πεπερασμένη ομάδα G που δρα σε πεπερασμένο σύνολο X. Επειδή οι τροχιές της δράσης είναι οι κλάσεις ισοδυναμίας της σχέσης ισοδυναμίας που ορίσαμε στην αρχή αυτής της παραγράφου, έχουμε την ξένη ένωση

$$X = \mathcal{O}_{x_1} \cup ... \cup \mathcal{O}_{x_t},$$

όπου $\mathcal{O}_{x_1}, ..., \mathcal{O}_{x_t}$ είναι οι διακεκριμένες τροχιές. Άρα από το προηγούμενο θεώρημα έχουμε

$$|X| = |\mathcal{O}_{x_1}| \cup ... \cup |\mathcal{O}_{x_t}| = [G : G_{x_1}] \cup ... \cup [G : G_{x_t}]. \tag{11.1}$$

Σύμφωνα με το θεώρημα του Lagrange, η παραπάνω αριθμητική σχέση λέει ότι ο θετικός ακέραιος $|X|$ είναι άθροισμα θετικών διαιρετών της τάξης της G. Αυτή η παρατήρηση είναι

συχνά χρήσιμη. Ακολουθεί μια ειδική περίπτωση της (11.1) που παρακάτω θα χρησιμοποιηθεί πολλές φορές.

Εξίσωση κλάσεων. Έστω G μια πεπερασμένη ομάδα και $cl(y_1), ..., c; (y_t)$ οι κλάσεις συζυγίας της G.

Θεωρώντας τη δράση της G στη G μέσω συζυγίας, έχουμε την ξένη ένωση

$$G = cl(y_1) \cup ... \cup cl(y_t).$$

Θυμίζουμε ότι το κέντρο της G είναι

$$Z(G) = \{a \in G : ag = ga, \text{ για κάθε } a \in G\}.$$

Πρόκειται για κανονική υποομάδα της G, όπως είδαμε στο Παράδειγμα 10.4(9).

Παρατηρούμε ότι μια κλάση συζυγίας $cl(x)$ αποτελείται από ένα μόνο στοιχείο, $cl(x) = \{x\}$, αν και μόνο αν

$$gx = xg \text{ για κάθε } g, \text{ δηλαδή αν και μόνο αν } x \in Z(G).$$

Με άλλα λόγια, το σύνολο $Z(G)$ είναι ή ένωση όλων των κλάσεων συζυγίας που έχουν μοναδικό στοιχείο. Συνεπώς η παραπάνω ξένη ένωση μπορεί να γραφεί στη μορφή

$$G = Z(G) \cup cl(x_1)... \cup cl(x_t),$$

όπου $cl(x_1), ..., cl(x_t)$ είναι όλες οι κλάσεις συζυγίας της G που η καθεμιά έχει τουλάχιστον 2 στοιχεία. Από αυτό και το Πόρισμα 11.8(1) παίρνουμε το εξής.

Πόρισμα 11.9 (Εξίσωση κλάσεων)**.** *Έστω G πεπερασμένη ομάδα. Τότε*

$$|G| = |Z(G)| + [G : C_G(x_1)] + ... + [G : C_G(x_t)],$$

όπου τα $x_1, ..., x_t$ είναι αντιπρόσωποι των κλάσεων συζυγίας της G που έχουν τουλάχιστον 2 στοιχεία.

Η ισότητα στο παραπάνω πόρισμα είναι γνωστή ως η εξίσωση κλάσεων και είναι ιδιαίτερα χρήσιμη.

Εφαρμογή 11.10. *Έστω G ομάδα τάξης p^n, όπου p πρώτος και $n > 0$. Τότε το κέντρο της G είναι μη τετριμμένο. Ιδιαίτερα, αν $n = 2$, τότε η G είναι αβελιανή.*

Απόδειξη. Για τον πρώτο ισχυρισμό, το ζητούμενο είναι σαφές αν η G είναι αβελιανή. Υποθέτουμε ότι η G δεν είναι αβελιανή, ισοδύναμα υπάρχει κλάση ισοδυναμίας με τουλάχιστον 2 στοιχεία. Στο δεξί μέλος της εξίσωσης κλάσεων, κάθε ακέραιος $[G : C_G(x_i)]$ είναι πολλαπλάσιος του p. Από την υπόθεση, το αριστερό σκέλος είναι πολλαπλάσιο του p και επομένως το ίδιο συμβαίνει με το $|Z(G)|$. Ειδικά, $Z(G) \neq e$.

Έστω ότι $|G| = p^2$. Από τον πρώτο ισχυρισμό έχουμε $|Z(G)| > 1$, οπότε από το θεώρημα του Lagrange έχουμε $|Z(G)| = p, p^2$. Στην πρώτη περίπτωση η ομάδα πηλίκο $G/Z(G)$ είναι κυκλική (γιατί έχει τάξη πρώτο αριθμό) και επομένως η G είναι αβελιανή σύμφωνα με την άσκηση 10.5. Στη δεύτερη περίπτωση έχουμε $G = Z(G)$, οπότε η G είναι πάλι αβελιανή. □

Σημειώνουμε ότι την προηγούμενη Εφαρμογή την είδαμε στην παράγραφο ΞΞΞ.

Σταθερά σημεία δράσης. Έστω X ένα G-σύνολο. Είναι δυνατό να υπάρχει $x \in X$ τέτοιο ώστε για κάθε $g \in G$ να ισχύει

$$g \cdot x = x.$$

Κάθε τέτοιο στοιχείο του X λέγεται **σταθερό σημείο** της δράσης της G. Το σύνολο αυτών συμβολίζεται X^G, δηλαδή

$$X^G = \{x \in X : g \cdot x = x \ \forall g \in G\}$$

και λέγεται το **σύνολο των σταθερών σημείων** της δράσης της G.

Από τους ορισμούς έπεται άμεσα ότι ένα $x \in X$ είναι σταθερό σημείο αν και μόνο αν η τροχιά του είναι μονοσύνολο, δηλαδή

$$x \in X^G \Leftrightarrow \mathcal{O}_x = \{x\}. \tag{11.2}$$

Παράδειγμα 11.11. Το σύνολο των σταθερών σημείων της δράσης της G στη G μέσω συζυγίας (Παράδειγμα 11.2(4» είναι το κέντρο $Z(G)$ της G.

Ορισμός 11.12. *Έστω p πρώτος. Μια ομάδα τάξης p^n λέγεται p-ομάδα.*

Το επόμενο λήμμα παρέχει την ύπαρξη σταθερού σημείου όταν δρα p-ομάδα σε πεπερασμένο σύνολο που το πλήθος των στοιχείων του δεν είναι πολλαπλάσιο του p.

Λήμμα 11.13. *Έστω G μια p-ομάδα και X ένα πεπερασμένο G-σύνολο. Τότε*

$$|X| \equiv |X^G| \mod p.$$

Ειδικά, αν το $|X|$ δεν διαιρείται με το p, τότε υπάρχει τουλάχιστον ένα σταθερό σημείο της δράσης της G. Το πρώτο θεώρημα Sylow δίνει δίνει ένα θετικό αποτέλεσμα για το αντίστροφο.

Απόδειξη. Από τις σχέσεις (11.1) και (11.2) έχουμε

$$|X| = |X^G| + |\mathcal{O}_{y_1}| \cup ... \cup |\mathcal{O}_{y_s}|,$$

όπου $\mathcal{O}_{y_i}, i = 1, ..., s$, είναι οι τροχιές (αν υπάρχουν) με $|\mathcal{O}_{y_i}| > 1$. Από το Θεώρημα 11.7 έχουμε

$$|\mathcal{O}_{y_i}| = [G : G_{y_i}]$$

οπότε ασύμφωνα με το θεώρημα του Lagrange, κάθε $|\mathcal{O}_{y_i}|$ είναι διαιρέτης του p^n. Επειδή $|\mathcal{O}_{y_i}| > 1$, κάθε $|\mathcal{O}_{y_i}|$ είναι πολλαπλάσιο του p. Από την πρώτη σχέση έπεται το ζητούμενο. □

Το προηγούμενο λήμμα θα βρει αρκετές εφαρμογές παρακάτω, ειδικά στις αποδείξεις των θεωρημάτων Sylow. Τώρα ας δούμε πως προκύπτει από αυτό το φημισμένο θεώρημα του Cauchy. Στην παράγραφο 10.2 το αποδείξαμε για αβελιανές ομάδας. Εδώ το αποδεικνύουμε γενικά (χωρίς τη χρήση της προηγούμενης ειδικής περίπτωσης).

Θεώρημα 11.14 (θεώρημα του Cauchy)**.** *Αν ο πρώτος p διαιρεί την τάξη πεπερασμένης ομάδας G, τότε η G έχει στοιχείο τάξης p.*

Απόδειξη. Θεωρούμε το καρτεσιανό γινόμενο $G^p = G \times ... \times G$ (p φορές) και το υποσύνολο αυτού

$$X = \{(g_1, ..., g_p) \in G^p - (1, ..., 1) : g_1...g_p = 1\}.$$

Σημειώνουμε ότι αν $g_1g_2...g_p = 1$, τότε $1 = g_p(g_1g_2...g_p)g_p^{-1} = g_pg_1...g_{p-1}$. Επαναλαμβάνοντας έχουμε

$$g_1g_2...g_p = 1 \Rightarrow g_pg_1g_2...g_{p-1} = 1 \Rightarrow$$
$$g_{p-1}g_pg_1...g_{p-2} = 1 \Rightarrow ... \Rightarrow g_2g_3...g_pg_1 = 1.$$

Έστω $H =< a >$ ομάδα τάξης p. Από τις παραπάνω σχέσεις έχουμε ότι η H δρα στο X με

$$a \cdot (g_1, g_2, ..., g_p) = (g_p, g_1, g_2, ..., g_{p-1}),$$
$$a^2 \cdot (g_1, g_2, ..., g_p) = (g_{p-1}, g_p, g_1, ..., g_{p-2}),$$
$$...$$
$$a^{p-1} \cdot (g_1, g_2, ..., g_p) = (g_2, g_3, ..., g_p, g_1).$$

Επειδή το $|X| = p^n - 1$ δεν διαιρείται με το $p = |H|$, από το Λήμμα 11.13 συμπεραίνουμε ότι η δράση της H έχει σταθερό σημείο. Αυτό είναι αναγκαστικά της μορφής $(g, g, ..., g)$. Έχουμε $g^p = 1$. Επειδή ο p είναι πρώτος και $g \neq 1$, έπεται ότι η τάξη του g ισούται με p. □

Η απόδειξη του προηγούμενου θεωρήματος είναι υποψήφια για μετάλλιο κομψότητας στις σημειώσεις αυτές και οφείλεται στον McKay (1959).

11.3. Θεωρήματα Sylow

Ξέρουμε γενικά ότι στις πεπερασμένες ομάδες δεν αληθεύει το αντίστροφο του θεωρήματος του Lagrange. Για παράδειγμα, η ομάδα A_4 που έχει τάξη 12 δεν έχει υποομάδα τάξης 6. Ένα σημαντικό αποτέλεσμα στην αντίστροφη κατεύθυνση παρέχει το πρώτο θεώρημα του Sylow

Πρώτο θεώρημα Sylow. Έστω G μια πεπερασμένη ομάδα και p ένας πρώτος αριθμός που διαιρεί την τάξη της G. Γράφουμε $|G| = p^n m$, όπου το p δεν διαιρεί το m. Κάθε υποομάδα της G με τάξη p^n λέγεται **Sylow** p**-** υποομάδα της G .

Σημειώνουμε ότι μια υποομάδα της G είναι Sylow p-υποομάδα της G αν και μόνο αν ο δείκτης $[G : H]$ είναι σχετικά πρώτος με το p.

Για παράδειγμα, η υποομάδα A_3 της S_3 είναι 3-Sylow υποομάδα της S_3. Καθεμιά από τις $\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle$ είναι 2-Sylow υποομάδα της S_3. Αν p είναι πρώτος, τότε η μέγιστη δύναμη του p που διαιρεί το $p!$ είναι p^1 και επομένως μια Sylow p-υποομάδα της S_p είναι η $\langle\tau\rangle$ για οποιοδήποτε κύκλο της S_p μήκους p.

Θεώρημα 11.15 (Πρώτο θεώρημα Sylow)**.** *Έστω G μια πεπερασμένη ομάδα και p ένας πρώτος που διαιρεί την τάξη της G. Τότε η G έχει Sylow p-υποομάδα.*

Απόδειξη. Χρησιμοποιούμε επαγωγή στην τάξη της G. Αν $|G|$=1 δεν υπάρχει κάτι να δείξουμε. Υποθέτουμε ότι $|G| > 1$ και το αποτέλεσμα ισχύει για κάθε ομάδα με τάξη μικρότερη της $|G|$.

Αν η G έχει υποομάδα H με δείκτη σχετικό πρώτο με την τάξη $|G|$, τότε από επαγωγή η H έχει Sylow p-υποομάδα και αυτή είναι Sylow p-υποομάδα της G. Μπορούμε έτσι να υποθέσουμε ότι κάθε γνήσια μη τετριμμένη υποομάδα της G έχει τάξη πολλαπλάσιο του p. Από την εξίσωση κλάσεων της G έχουμε

$$|G| = |Z(G)| + [G : C_G(x_1)] + ... + [G : C_G(x_t)],$$

όπου τα $x_1, ..., x_t$ είναι αντιπρόσωποι των κλάσεων συζυγίας της G που έχουν τουλάχιστον 2 στοιχεία. Οι ακέραιοι $|G|, [G : C_G(x_1)], ..., [G : C_G(x_t)]$ διαιρούνται με το p και επομένως ο ακέραιος $|Z(G)|$ διαιρείται με το p. Από το θεώρημα του Cauchy για αβελιανές ομάδας (Θεώρημα 10.9) έπεται ότι η ομάδα $Z(G)$ περιέχει στοιχείο a τάξης p.

Επειδή $a \in Z(G)$, η υποομάδα $\langle a\rangle$ είναι κανονική στη G. Θεωρούμε το φυσικό επιμορφισμό ομάδων

$$f : G \to G/\langle a\rangle.$$

Έστω p^n η μέγιστη δύναμη του p που διαιρεί την τάξη της G. Τότε το p^{n-1} είναι η μέγιστη δύναμη του p που διαιρεί την τάξη της $G/\langle a\rangle$. Από επαγωγή υπάρχει Sylow p-υποομάδα, έστω K, της $G/\langle a\rangle$. Τότε $|K| = p^{n-1}$ και η υποομάδα $f^{-1}(K)$ της G είναι τέτοια ώστε

$$f^{-1}(K)/\langle a\rangle \simeq K.$$

Άρα $|f^{-1}(K)| = |K||\langle a\rangle| = p^{n-1}p = p^n$. Δηλαδή η $f^{-1}(K)$ είναι μια Sylow p-υποομάδα της G.

□

Παρατήρηση. Σημειώνουμε ότι ως πόρισμα του πρώτου θεωρήματος Sylow προκύπτει το θεώρημα του Cauchy, που είδαμε με διαφορετική απόδειξη στην παράγραφο 11.2. Πράγματι, αν G είναι πεπερασμένη ομάδα και p πρώτος που διαιρεί την τάξη της, τότε η G έχει υποομάδα H τάξης p^n για κάποιο $n > 0$, σύμφωνα με το πρώτο θεώρημα Sylow. Έστω $a \in H$, $a \neq 1$. Από το θεώρημα του Lagrange, η τάξη του a είναι της μορφής p^k, $k > 1$. Το στοιχείο $a^{p^{k-1}}$ έχει τάξη p.

Δεύτερο θεώρημα Sylow. Υπενθυμίζουμε ότι δύο υποομάδες H, K ομάδας G λέγονται **συζυγείς** αν υπάρχει $g \in G$ με $K = gHg^{-1}$.Είναι σαφές ότι συζυγείς υποομάδες έχουν την ίδια τάξη. Άρα συζυγής υποομάδα μιας Sylow p-υποομάδας της G είναι επίσης Sylow p-υποομάδας της G. Το δεύτερο θεώρημα Sylow δίνει αποτέλεσμα στην αντίστροφη κατεύθυνση.

Θεώρημα 11.16 (δεύτερο θεώρημα Sylow)**.** *Κάθε δύο Sylow p- υποομάδες πεπερασμένης ομάδας G είναι συζυγείς.*

Απόδειξη. Έστω P μια Sylow p-υποομάδα της G και Q μια p-υποομάδα της G (όχι αναγκαστικά Sylow p-υποομάδα). Θεωρούμε τη δράση της Q σύνολο $X = G/P$ με αριστερό πολλαπλασιασμό, $q \cdot (gP) = qgP$. Επειδή το X δεν διαιρείται με το p, από το Λήμμα 11.13 έπεται ότι η δράση έχει σταθερό σημείο. Αυτό σημαίνει ότι υπάρχει $g \in G$ με

$$qgP = gP, \forall q \in Q.$$

Άρα $Q \subseteq gPg^{-1}$.

Τώρα, αν επιπλέον υποθέσουμε ότι και η Q είναι Sylow p-υποομάδα της G, τότε η τελευταία σχέση δίνει ισότητα $Q = gPg^{-1}$, αφού τα σύνολα Q, gPg^{-1} έχουν το ίδιο πεπερασμένο πλήθος στοιχείων. □

Η πρώτη παράγραφος της προηγούμενης απόδειξης δίνει άμεσα το εξής αποτέλεσμα.

Πόρισμα 11.17. *Έστω G πεπερασμένη ομάδα και $H \leq G$ με $|H| = p^k$, όπου p πρώτος. Τότε υπάρχει Sylow p-υποομάδα της G που περιέχει την H.*

Τρίτο θεώρημα Sylow. Αν G είναι πεπερασμένη ομάδα και p πρώτος διαιρέτης της τάξης της G, με n_p συμβολίζουμε το πλήθος των Sylow p- υποομάδων της G.

Θεώρημα 11.18 (τρίτο θεώρημα Sylow)**.** *Έστω G ομάδα τάξης $p^n m$ όπου p είναι πρώτος και το m δεν είναι πολλαπλάσιο του p. Τότε*

$$n_p \equiv 1 \mod p \quad \text{και} \quad n_p | m.$$

Απόδειξη. Ας δείξουμε πρώτα τη σχέση $n_p|m$. Έστω P μια Sylow p-υποομάδα της G. Από το δεύτερο θεώρημα Sylow έπεται ότι το n_p ισούται με το πλήθος των συζυγών υποομάδων της P στη G, δηλαδή με το δείκτη $[G : N_G(P)]$ σύμφωνα με το Πόρισμα 11.8. Όμως $[G : N_G(P)]|[G : P]$ αφού $P \leq N_G(P)$. Δηλαδή, $[G : N_G(P)]|m$.

Για την άλλη σχέση, ας θεωρήσουμε το σύνολο

$$X = \{P_1, ..., P_t\}$$

όλων των Sylow p- υποομάδων της G και τη δράση της ομάδας $P = P_1$ σε αυτό που δίνεται μέσω συζυγίας.

Ισχυριζόμαστε ότι η δράση έχει μοναδική τροχιά με 1 στοιχείο, την $\mathcal{O}_P$.

Πράγματι, αν $\mathcal{O}_{P_i} = \{P_i\}$, τότε

$$P \subseteq N_G(P_i).$$

Οι ομάδες P, P_i της $N_G(P_i)$ είναι Sylow p- υποομάδες της $N_G(P_i)$ (αφού είναι Sylow p- υποομάδες της G). Από το δεύτερο θεώρημα Sylow, είναι συζυγείς υποομάδες της $N_G(P_i)$ και άρα ίσες.

Από τον ισχυρισμό και το Λήμμα 11.13 έχουμε $n_p \equiv 1 \mod p$. □

Εφαρμογές θεωρημάτων Sylow. Μια ομάδα G λέγεται **απλή** αν οι μόνες κανονικές υποομάδες της G είναι οι $\{1\}$ και G. Για παράδειγμα, κάθε ομάδα με τάξη πρώτο αριθμό είναι απλή. Στη συνέχεια θα δούμε πως χρησιμοποιούνται τα θεωρήματα Sylow για να δείξουμε ότι μια ομάδα δεν είναι απλή ή ότι είναι κυκλική. Επίσης στα δύο τελευταία παραδείγματα θα δούμε περιπτώσεις που τα θεωρήματα Sylow επιτρέπουν την ταξινόμηση ομάδων συγκεκριμένης τάξης.

Παραδείγματα 11.19.

(1) Δεν υπάρχει απλή ομάδα τάξης 102.

Πράγματι, έστω G ομάδα τάξης 102. Έχουμε $102 = 2 \cdot 3 \cdot 17$. Από το τρίτο θεώρημα Sylow, το πλήθος n_{17} των 17-Sylow υποομάδων της G ικανοποιεί $n_{17} \equiv 1 \mod 17$ και $n_{17}|6$. Άρα $n_{17} = 1$, δηλαδή υπάρχει μοναδική 17-Sylow υποομάδα H της G. Από το δεύτερο θεώρημα Sylow η H ισούται με κάθε συζυγή της στη G και επομένως είναι κανονική υποομάδα της G.

(2) Δεν υπάρχει απλή ομάδα τάξης 12.

Πράγματι, θα δείξουμε ότι κάθε ομάδα G τάξης $12 = 2^2 \cdot 3$ έχει κανονική υποομάδα τάξης 3 ή κανονική υποομάδα τάξης 4.

Από το τρίτο θεώρημα Sylow, το πλήθος n_3 των 3-Sylow υποομάδων της G τάξης 3 ικανοποιεί $n_3 \equiv 1 \mod 3$ και $n_3|4$. Άρα $n_3 = 1$ ή $n_3 = 4$.

Στην πρώτη περίπτωση υπάρχει μοναδική 3-Sylow υποομάδα της G που οφείλει να είναι κανονική στη G από το δεύτερο θεώρημα Sylow.

Στη δεύτερη περίπτωση έχουμε 4 υποομάδες που η καθεμιά έχει τάξη 3. Ας υπολογίσουμε το πλήθος των στοιχείων της ένωσης τους. Επειδή το 3 είναι πρώτος, κάθε δύο από αυτές τις Sylow 3-υποομάδες έχουν τομή το σύνολο $\{1\}$ σύμφωνα με το θεώρημα του Lagrange και επομένως η ένωση όλων των Sylow 3-υποομάδων της G περιέχει

$$4 \cdot (3 - 1) = 8$$

στοιχεία διάφορα του 1. Από το πρώτο θεώρημα Sylow υπάρχει Sylow 2-υποομάδα της G τάξης 4. Αυτή είναι μοναδική καθώς $|G| - 8 = 4$. Άρα είναι κανονική στη G από το δεύτερο θεώρημα Sylow.

(3) Έστω $p < q$ πρώτοι και G ομάδα τάξης pq. Θα δείξουμε ότι η G δεν είναι απλή και στη συνέχεια θα δείξουμε ότι αν το p δεν διαιρεί το $q - 1$, τότε η G είναι κυκλική.

Από το τρίτο θεώρημα Sylow έχουμε $n_q \equiv 1 \mod q$ και $n_q|p$. Επειδή $p < q$ έπεται ότι $n_q = 1$. Η μοναδική q-Sylow υποομάδα της G, έστω Q, είναι κανονική από το δεύτερο θεώρημα Sylow.

Υποθέτουμε τώρα ότι το p δεν διαιρεί το $q-1$. Όπως ακριβώς πριν παίρνουμε $n_p \equiv 1 \mod p$ και $n_p|p$. Από τη νέα υπόθεση έπεται ότι $n_p = 1$ και άρα η Sylow p-υποομάδα της G, έστω P, είναι κανονική στη G.

Επομένως έχουμε κανονικές υποομάδες P, Q της G με αντίστοιχες τάξεις p, q. Επειδή οι p, q είναι διακεκριμένοι πρώτοι, από το θεώρημα του Lagrange έχουμε

$$P \cap Q = \{1\}.$$

Από την Πρόταση 10.12 έχουμε $PQ = G$, οπότε από την Πρόταση 10.13 έχουμε

$$G \simeq P \times Q.$$

Επειδή οι p, q είναι διακεκριμένοι πρώτοι, έχουμε

$$P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_p \simeq \mathbb{Z}_{pq},$$

δηλαδή $G \simeq \mathbb{Z}_{pq}$ που είναι κυκλική ομάδα.

(4) Θα δείξουμε ότι κάθε ομάδα G τάξης $345 = 3 \times 5 \times 23$ είναι κυκλική.

Όπως στα προηγούμενα παραδείγματα διαπιστώνουμε ότι $n_{23} = n_5 = 1$. Άρα οι αντίστοιχες p-Sylow υποομάδες, έστω H_{23}, H_5, είναι κανονικές στη G. Οι αντίστοιχες ομάδες πηλίκα έχουν τάξεις 3×5 και 3×23, οπότε από το προηγούμενο παράδειγμα είναι κυκλικές. Από το Παράδειγμα 10.6(4) έπεται ότι η ομάδα μεταθετών $[G, G]$ περιέχεται

και στην H_{23} και στην H_5. Άρα $[G,G]=1$ από το θεώρημα Lagrange. Συνεπώς η G είναι αβελιανή. Από την άσκηση 8.2 έπεται ότι είναι κυκλική.

(5) **Ταξινόμηση ομάδων τάξης** $2p$**.** Έστω $p>2$ πρώτος και G ομάδα τάξης $2p$. Θα δείξουμε ότι η G είναι κυκλική ή ισόμορφη με τη διεδρική D_p.

Από το θεώρημα του Cauchy η G έχει υποομάδες $\langle a\rangle, \langle b\rangle$ με τάξεις $2, p$ αντίστοιχα. Η $\langle b\rangle$ είναι κανονική στη G αφού έχει δείκτη 2 (άσκηση 10.1). Άρα για κάποιο $k<p$ έχουμε $aba^{-1}=b^k$. Επομένως

$$b^{k^2}=(b^k)^k=(aba^{-1})^k=ab^ka^{-1}=a^2ba^{-2}=b.$$

Δηλαδή $b^{k^2-1}=1$. Συνεπώς $p|k^2-1$ και παίρνουμε $p|k-1$ ή $p|k+1$.

Στην πρώτη περίπτωση έχουμε $k=1$, οπότε $ab=ba$ και το στοιχείο ab έχει τάξη $2p=|G|$, δηλαδή η G είναι κυκλική.

Στη δεύτερη περίπτωση έχουμε $k+1=p$, οπότε $aba^{-1}=b^{-1}$. Εύκολα επαληθεύεται ότι τα ακόλουθα στοιχεία της G

$$1, b, b^2, ..., b^{p-1}, a, ba, b^2a, ..., b^{p-1}a$$

είναι ανά δύο διακεκριμένα και επειδή το πλήθος τους είναι $2p$ έχουμε

$$G=\{1, b, b^2, ..., b^{p-1}, a, ba, b^2a, ..., b^{p-1}a\}.$$

Με το συμβολισμό του παραδείγματος 7.4(10), είναι υπόθεση ρουτίνας η επαλήθευση ότι η απεικόνιση $D_p\to G, r^is^j\mapsto b^ia^j$, $(i=0,1,...,p-1,\ j=0,1)$ είναι ομομορφισμός ομάδων. Επειδή είναι επί και $|D_p|=|G|<\infty$, είναι ισομορφισμός.

(6) **Ταξινόμηση ομάδων τάξης** 66**.** Θα δείξουμε ότι κάθε ομάδα τάξης 66 είναι ισόμορφη με ακριβώς μία από τις ακόλουθες ομάδες

$$\mathbb{Z}_{66},\ \ D_{33},\ \ D_{11}\times\mathbb{Z}_3,\ \ D_3\times\mathbb{Z}_{11}.$$

Πρώτο βήμα. Οι παραπάνω 4 ομάδες είναι ανά δύο μη ισόμορφες. Πράγματι, η πρώτη είναι αβελιανή ενώ οι υπόλοιπες δεν είναι. Η δεύτερη έχει 33 στοιχεία τάξης 2 (τις ανακλάσεις), η τρίτη 11 και η τέταρτη 3.

Δεύτερο βήμα. Έστω G ομάδα τάξης $66=2\times3\times11$. Για $p=2,3,11$ έστω H_p Sylow-p υποομάδα της G. Από το τρίτο θεώρημα Sylow έπεται ότι $n_{11}\equiv1 \mod 11$ και $n_{11}|6$. Άρα $n_{11}=1$ και από το δεύτερο θεώρημα Sylow έχουμε $H_{11}\trianglelefteq G$. Από την πρόταση 10.11 έχουμε $H\leq G$, όπου $H=H_3H_{11}$. Από το παράδειγμα (3) που προηγήθηκε έχουμε ότι η H είναι κυκλική, έστω $H=\langle x\rangle$. Επειδή η H έχει δείκτη 2 στη G, είναι κανονική στη G. Επομένως γράφοντας $H_2=\langle y\rangle$, υπάρχει $0\leq i\leq31$ με $yxy^{-1}=x^i$. Δηλαδή

$$yx=x^iy.$$

Έχουμε $G=HH_2$, δηλαδή κάθε στοιχείο της G είναι της μορφής $x^ay^b, x=0,...,31,\ j=0,1$. Το γινόμενο δύο στοιχείων της μορφής x^ay^b μπορεί να υπολογιστεί με την πιο πάνω σχέση. Με άλλα λόγια, το i καθορίζει τη δομή της ομάδας G.

Τρίτο βήμα. Θα δούμε τώρα ότι το i μπορεί να λάβει το πολύ 4 τιμές. Ξέρουμε ότι συζυγή στοιχεία έχουν την ίδια τάξη (άσκηση 7.5), οπότε

$$|x|=|x^i|\Rightarrow \mu\kappa\delta(33,i)=1.$$

Μία άλλη σχέση για το i προκύπτει ως εξής

$$x=y(yxy^{-1})y^{-1}=yx^iy^{-1}=(yxy^{-1})^i=x^{i^2}.$$

Άρα $33|i^2-1\Rightarrow 11|i+1$ ή $11|i-1$. Από αυτή και την πιο πάνω σχέση του i εύκολα έπεται ότι $i\in\{1,10,23,32\}$.

Από το προηγούμενα βήματα έπεται το ζητούμενο.

Σχόλια

(1) Για κάθε θετικό ακέραιο n, έστω $g(n)$ το πλήθος των ανά δύο μη ισόμορφων ομάδων τάξης n. Στον ακόλουθο πίνακα δίνονται οι τιμές $g(n)$ για $n\leq12$.

n	$g(n)$	αντιπρόσωποι ομάδων
1	1	1
2	1	$\mathbb{Z}_2$
3	1	$\mathbb{Z}_3$
4	2	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	1	$\mathbb{Z}_5$
6	2	$\mathbb{Z}_6, S_3$
7	1	$\mathbb{Z}_7$
8	5	$\mathbb{Z}_8,\ \mathbb{Z}_4 \times \mathbb{Z}_2\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_4,\ Q_8$
9	2	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$
10	2	$\mathbb{Z}_{10},\ D_5$
11	1	$\mathbb{Z}_{11}$
12	5	$\mathbb{Z}_{12},\ \mathbb{Z}_6 \times \mathbb{Z}_2,\ A_4, D_6, Dic_3$

Για παράδειγμα έχουμε $g(p) = 1$ αν p είναι πρώτος, αφού κάθε δύο ομάδες τάξης p είναι ισόμορφες (ως κυκλικές ίδιας τάξης). Επίσης για κάθε περιττό πρώτο p έχουμε $g(2p) = 2$ από το Παράδειγμα 11.19(5).

Δεν έχουμε συναντήσει στις σημειώσεις αυτές τις ομάδες Q_8 (ομάδα των quaternions) και Dic_3 (δικυκλική ομάδα τάξης 12). Η πρώτη μπορεί να ορισθεί ως η υποομάδα της $GL(2, \mathbb{R})$ που παράγεται από τους πίνακες

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

και η δεύτερη ως η υποομάδα της $GL(2, \mathbb{C})$ που παράγεται από τους πίνακες

$$\begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

όπου $\omega = \cos(2\pi/6) + i \sin(2\pi/6)$.

(2) Η έννοια της απλής ομάδας εισήχθη από τον Galois περίπου 190 χρόνια πριν. Το ότι η ομάδα A_5 των άρτιων μεταθέσεων της S_5 είναι απλή έπαιξε σημαντικό ρόλο στην απόδειξή του ότι το γενικό πολυώνυμο βαθμού 5 δεν είναι επιλύσιμο με ριζικά. Δύο θεμελιώδη θεωρήματα για απλές ομάδες είναι τα ακόλουθα.

(Burnside, 1904) Η τάξη κάθε πεπερασμένης μη αβελιανής απλής ομάδας διαιρείται με τουλάχιστον 3 διαφορετικούς πρώτους.

(Feit-Thompson, 1962) Κάθε πεπερασμένη μη αβελιανή απλή ομάδα έχει άρτια τάξη.

Ένα από τα σημαντικά επιτεύγματα των σύγχρονων μαθηματικών είναι η ταξινόμηση των απλών πεπερασμένων ομάδων που ολοκληρώθηκε τη δεκαετία του 2000. Η απόδειξη περιέχεται σε εκατοντάδες ερευνητικά άρθρα και ο συνολικός αριθμός σελίδων είναι δεκάδες χιλιάδες, https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups.

Ασκήσεις Κεφαλαίου 11

Ομάδα1: 1-5, 17.
Ομάδα2: 6-10.
Ομάδα3: 11.

1. Στα Παραδείγματα 11.2(3) και (4) δείξτε ότι οι απεικονίσεις είναι καλά ορισμένες (όπου χρειάζεται) και είναι δράσεις.
2. Δείξτε ότι το σύνολο G_x του ορισμού 11.4 είναι πράγματι υποομάδα της G.
3. Είναι δυνατό η εξίσωση κλάσεων μιας ομάδας τάξης 20 να έχει τη μορφή $20 = 1+3+6+10$;
4. Δείξε ότι κάθε ομάδα τάξης 39 που δρα σε σύνολο με 20 στοιχεία έχει σταθερό σημείο.
5. Η S_3 δρα σε ένα σύνολο X τεσσάρων στοιχείων έτσι ώστε για κάθε $x \in X$ υπάρχει $g \in G$ με $g \cdot x \neq x$. Ποιο είναι το πλήθος των τροχιών και πόσα στοιχεία έχει η καθεμιά;
6. Η ομάδα $GL(2, \mathbb{R})$ δρα στο $\mathbb{R}^2$ μέσω γινομένου πινάκων
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$
Πόσες τροχιές έχει η δράση και ποιες είναι; Ποια είναι η τροχιά του $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$;
7. Θεωρούμε την προσθετική ομάδα G των πραγματικών αριθμών να δρα στο επίπεδο $\mathbb{R}^2$ μέσω
$$G \times \mathbb{R}^2 \to \mathbb{R}^2, (\theta, P) \mapsto r_\theta(P),$$
όπου r_θ είναι η περιστροφή του επιπέδου γύρω από το σημείο $(0, 0)$ κατά γωνία θ. Βρείτε τις τροχιές και τις σταθεροποιούσες υποομάδες της δράσης.
8. Θεωρούμε τη δράση της D_4 στις κορυφές τετραγώνου όπως στο Παράδειγμα 11.3(1). Ποια είναι η σταθεροποιούσα υποομάδα της κορυφής 1; Επεκτείνουμε κατά τον προφανή τρόπο σε δράση επί του συνόλου των πλευρών. Ποια είναι η σταθεροποιούσα της πλευράς 12;
9. Έστω G ομάδα και $H, K \leq G$ με $H \trianglelefteq K$. Δείξτε ότι $K \leq N_G(H)$.
10. Έστω G μια ομάδα και X ένα G - σύνολο. Δείξτε ότι για κάθε $g \in G$ και $x \in X$, οι σταθεροποιούσες υποομάδες G_x, G_{gx} είναι συζυγείς.
11. Έστω G ομάδα που έχει τουλάχιστον μία κλάση συζυγίας με ακριβώς δύο στοιχεία. Δείξτε ότι η G περιέχει γνήσια μη τετριμμένη κανονική υποομάδα.
12. Έστω G πεπερασμένη ομάδα και N κανονική υποομάδα της G. Δείξτε ότι αν $cl(x)$ είναι μια κλάση συζυγίας της G, τότε $cl(x) \subseteq N$ ή $cl(x) \cap N = \emptyset$. Στη συνέχεια δείξτε ότι υπάρχουν $x_1, ..., x_s \in G$ με
$$N = |cl(x_1)| + ... + |cl(x_s)|.$$
13. Έστω G μια p-ομάδα και N μη τετριμμένη κανονική υποομάδα της G. Δείξτε ότι $N \cap Z(G) \neq \{1\}$.
14. Έστω G μια p-ομάδα. Δείξτε ότι η G έχει κανονική υποομάδα τάξης p^{n-1}.
15. Χρησιμοποιήστε δράσεις για να δώσετε μια άλλη απόδειξη της Εφαρμογής 10.15 που λέει ότι αν p είναι ο ελάχιστος πρώτος που διαιρεί την τάξη μιας πεπερασμένης ομάδας G κι H είναι υποομάδα της G με δείκτη p, τότε H είναι κανονική στη G.
16. Έστω p πρώτος. Δίνετε η εξής μη αβελιανή υποομάδα της $GL(3, \mathbb{Z}_p)$
$$H = \{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \}.$$
Βρείτε την τάξη του κέντρου της H χωρίς να κάνετε υπολογισμούς.

17. Έστω G πεπερασμένη ομάδα τάξης n. Επιλέγουμε τυχαία δύο στοιχεία της G με επανατοποθέτηση. Δείξτε ότι η πιθανότητα αυτά να αντιμετατίθενται ισούται με t/n, όπου t είναι το πλήθος των κλάσεων συζυγίας της G.
18. Έστω P μια Sylow p-υποομάδα της G. Δείξτε ότι η P είναι η μοναδική Sylow p-υποομάδα της $N_G(P)$.
19. Δείξτε ότι δεν υπάρχει απλή ομάδα τάξης 56.
20. Δείξτε ότι κάθε ομάδα τάξης 105 έχει υποομάδα τάξης 35.
21. Είναι δυνατό το κέντρο μιας ομάδας τάξης 308 να έχει τάξη 4;
22. Δείξτε ότι κάθε ομάδα τάξης 175 είναι αβελιανή.
23. Έστω $f : G \to G$ ένας αυτομορφισμός πεπερασμένης ομάδας G και H μια Sylow p-υποομάδα της G.
    i) Είναι σωστό ότι η υποομάδα $f(H)$ της G είναι Sylow p-υποομάδα ;
    ii) Είναι σωστό ότι $f(H) = H$; Αν όχι βρείτε μια επιπλέον συνθήκη στην H που εξασφαλίζει θετική απάντηση.
24. Έστω p πρώτος. Δείξτε ότι το πλήθος των Sylow p- υποομάδων της S_p ισούται με $(p-2)!$. Με βάση αυτό δώστε μια νέα απόδειξη του θεωρήματος Wilson, ότι δηλαδή $(p-1)! \equiv -1 \mod p$.
25. Δείξτε ότι αν G είναι ομάδα τάξης 231, τότε το κέντρο της G περιέχει στοιχείο τάξης 11.
26. Έστω p πρώτος και $H, K \leq GL(3, \mathbb{Z}_p)$ με $|H| = |K| = p^3$. Δείξτε ότι υπάρχει $g \in G$ με $K = gHg^{-1}$.

Υποδείξεις Κεφαλαίου 11

1.
2.
3. *Λύση.* Όχι καθώς κάθε όρος πρέπει να διαιρεί το 20 σύμφωνα με το θεώρημα τροχιάς-σταθεροποιούσας υποομάδας.
4. *Υπόδειξη.* Από τη σχέση (11.1) έπεται ότι το 20 είναι άθροισμα θετικών διαιρετών του 39. Δείξτε ότι σε κάθε τέτοιο άθροισμα, το 1 εμφανίζεται τουλάχιστον μία φορά.
5. *Απάντηση.* Τροχιές είναι ομόκεντροι κύκλοι με κέντρο το σημείο $(0,0)$ και για κάθε σημείο διάφορο του $(0,0)$ η σταθεροποιούσα υποομάδα είναι η κυκλική υποομάδα της προσθετικής ομάδας των πραγματικών που παράγεται από το 2π.
6.
7. *Υπόδειξη.* Δείξτε την ισότητα $G_{gx} = gG_xg^{-1}$.
8. *Υπόδειξη.* Θεωρήστε τη δράση της G μέσω συζυγίας στο σύνολο X που είναι κλάση συζυγίας με 2 στοιχεία και εφαρμόστε το θεώρημα τροχιάς-σταθεροποιούσας υποομάδας.
9.
10. *Υπόδειξη.* Χρησιμοποιήστε την ισότητα της προηγούμενης άσκησης.
11. *Υπόδειξη.* Από το θεώρημα του Cauchy και την Εφαρμογή 11.10 έπεται ότι υπάρχει στοιχείο a του κέντρου της G τάξης p. Θεωρήστε το πηλίκο $G/\langle a\rangle$ και εφαρμόστε επαγωγή στο n.
12. *Υπόδειξη.* Θεωρήστε τη δράση τις G μέσω αριστερού πολλαπλασιασμού στο $Q = G/H$. Δείξτε ότι ο πυρήνας του αντίστοιχου ομομορφισμού ομάδων $a : G \to S_X$ ισούται με το N.
13.
14.
15.
16.
17.
18. *Υπόδειξη.* Αυτό το είδαμε στην απόδειξη του τρίτου θεωρήματος Sylow.
19. *Υπόδειξη.* Μετρώντας στοιχεία τάξης 7, δείξτε ότι αν $n_7 = 8$, τότε $n_2 = 1$.
20. *Υπόδειξη.* Δείξτε ότι από τους n_5, n_7 τουλάχιστον ένας ισούται με 1. Θεωρήστε το γινόμενο των αντίστοιχων Sylow υποομάδων και εφαρμόστε την Πρόταση 10.11.
21. *Απάντηση.* Όχι. Χρησιμοποιήστε την Εφαρμογή 10.16 και την άσκηση 10.5
22. *Υπόδειξη.* Χρησιμοποιήστε την άσκηση 10.8(2).
23.
24. *Απάντηση.* Ναι.
25. *Υπόδειξη.* Δείξτε ότι υπάρχει μοναδική Sylow 11-υποομάδα H και θεωρήστε τη δράση της G σε αυτή μέσω συζυγίας. Ίσως η άσκηση 10.33 είναι χρήσιμη.
26. *Υπόδειξη.* Δεύτερο θεώρημα Sylow.

Ευρετήριο