

Δημητρίου Στρατηγοπούλου

ΣΥΓΧΡΟΝΗ ΑΛΓΕΒΡΑ



ΕΚΔΟΣΕΙΣ ΣΥΜΜΕΤΡΙΑ

Δημητρίου Στρατηγοπούλου

ΣΥΓΧΡΟΝΗ
ΑΛΓΕΒΡΑ

ΕΙΣΑΓΩΓΗ

ΕΚΔΟΣΕΙΣ : ΣΥΜΜΕΤΡΙΑ

ISBN 960-266-051-1

**Copyright 1997, by Dimitris Stratigopoulos
All Rights Reserved.**

**This book, or parts therefore,
may not reproduced in any form
without permission of the author**

Στη μνήμη του πατέρα μου

Περιεχόμενα

	Εισαγωγή	11
Κεφάλαιο 0	Σύνολα, συναρτήσεις, σχέσεις	17
1	Σύνολα, Αλγεβρα Boole	19
2	Συναρτήσεις	25
3	Σχέσεις	30
4	Σχέση Ισοδυναμίας	31
5	Σχέση Διάταξης	35
6	Εσωτερικοί και Εξωτερικοί Νόμοι	42
7	Σχέση Ισοδυναμίας Συμβιβαστή με Εσωτερικό Νόμο	49
8	Φυσικοί Αριθμοί	51
9	Ακέραιοι, Ρητοί Αριθμοί	53
10	Πληθάριθμοι	56
11	Πράξεις και Διάταξη Πληθαρίθμων	61
12	Βασικές Αλγεβρικές Δομές	66
13	Αντινομίες, Αξιώματα στη Θεωρία Συνόλων	70
14	Αλγεβρα Boole	71
15	Κυκλώματα Διακοπών	75
16	Διατάξεις, Μεταθέσεις, Συνδυασμοί	79
	Ασκήσεις	83
Κεφάλαιο 1	Διαιρετότητα στους ακεραίους	89
1	Διαίρεση Ακεραίων	90
2	Ακέραιοι ως προς Μέτρο m	97
3	Αριθμητικές Συναρτήσεις	103
4	Ισοδυναμίες Ανωτέρου Βαθμού	106
	Ασκήσεις	109

Κεφάλαιο 2	Αλγεβρικές δομές εσωτερικών νόμων	113
1	Ημιομάδα, Μονοειδές, Ομάδα.....	113
2	Δακτύλιοι, Σώματα.....	116
3	Ο Δακτύλιος των Ακεραίων mod m	119
4	Ισοδύναμοι Ορισμοί Ομάδας.....	122
5	Ομάδα Αντιστρέψιμων Στοιχείων Δακτυλίου.....	124
	Ασκήσεις.....	126
Κεφάλαιο 3	Δομές περιεχόμενες σε άλλες	129
1	Υποομάδα, Υποδακτύλιος, Υπόσωμα.....	129
2	Ιδιότητες Υποομάδων.....	131
3	Δείκτης Υποομάδας.....	132
4	Υποομάδα Παραγόμενη από Υποσύνολο Ομάδας.....	133
5	Υποομάδα Παραγόμενη από Μονοσύνολο.....	134
6	Τάξη Στοιχείου.....	136
7	Υποομάδες Κυκλικής Ομάδας.....	138
	Ασκήσεις.....	140
Κεφάλαιο 4	Ομάδα πηλίκου, δακτύλιος πηλίκου	143
1	Κανονική Υποομάδα, Ομάδα Πηλίκου.....	144
2	Δακτύλιος Πηλίκου.....	148
	Ασκήσεις.....	151
Κεφάλαιο 5	Ομομορφισμοί ομάδων	152
1	Ομομορφισμοί, Βασικές Ιδιότητες.....	153
2	Θεωρήματα Ισομορφισμού Ομάδων.....	157
3	Ταξινόμηση Κυκλικών Ομάδων.....	159
4	Αυτομορφισμοί, Αναλλοίωτες υποομάδες.....	161
	Ασκήσεις.....	164
Κεφάλαιο 6	Ευθέα γινόμενα	165
1	Ευθύ Γινόμενο Ομάδων, Δακτυλίων.....	165
2	Εσωτερικό Ευθύ Γινόμενο.....	168
3	Εφαρμογή : Ταξινόμηση των ομάδων τάξης ≤ 7	172
	Ασκήσεις.....	174

Κεφάλαιο 7	Ομομορφισμοί δακτυλίων	175
1	Ομομορφισμοί, Βασικές Ιδιότητες.....	175
2	Χαρακτηριστική, Πρώτα Υποσώματα.....	178
3	Δύο Επεκτάσεις Δακτυλίου.....	181
	Ασκήσεις.....	187
Κεφάλαιο 8	Ιδεώδη δακτυλίου, πράξεις ιδεωδών	188
1	Ιδεώδη Παραγόμενα από Υποσύνολο.....	188
2	Πράξεις με Ιδεώδη.....	191
3	Μέγιστα Ιδεώδη.....	193
4	Πρώτα Ιδεώδη.....	194
	Ασκήσεις.....	196
Κεφάλαιο 9	Δακτύλιοι πολυωνύμων	198
1	Δακτύλιοι Πολυωνύμων.....	198
2	Αλγόριθμος της Διαίρεσης Πολυωνύμων.....	204
	Ασκήσεις.....	207
Κεφάλαιο 10	Κύριοι δακτύλιοι διαιρετότητα	209
1	Κύριοι Δακτύλιοι.....	209
2	Διαιρετότητα.....	211
3	Μέγιστος Κοινός Διαιρέτης.....	215
1	Ελάχιστο Κοινό Πολλαπλάσιο.....	218
	Ασκήσεις.....	219
Κεφάλαιο 11	Πεδία μονοσήμαντης παραγοντοποίησης	222
1	Δακτύλιοι Μονοσήμαντης Παραγοντοποίησης.....	222
2	Παραγοντοποίηση στους Δακτυλίους $\mathbb{Q}[x]$, $\mathbb{Z}[x]$	225
3	Μονοσήμαντη Παραγοντοποίηση στον $A[x]$	227
	Ασκήσεις.....	229

Κεφάλαιο 12	Ρίζες πολυωνύμου	230
1	Ρίζες Πολυωνύμων	231
2	Παράγωγος Πολυωνύμου	233
3	Ακέραιες και Ρητές Ρίζες	238
	Ασκήσεις	239
Κεφάλαιο 13	Εισαγωγή στις επεκτάσεις σωμάτων	242
1	Επέκταση Σώματος, Αλγεβρικά Στοιχεία	242
2	Αλγεβρική Επέκταση	247
3	Κατασκευές με Κανόνα και Διαβήτη	250
4	Σώμα Ριζών Πολυωνύμου	256
	Ασκήσεις	261
Κεφάλαιο 14	Συμμετρικές ομάδες	264
2	Αρτιες, Περιττές Μεταθέσεις	269
3	Εναλλάσσουσα Υποομάδα της S_n	271
4	Ομάδες Ισόμορφες με Ομάδες Μεταθέσεων	272
	Ασκήσεις	278
	Βιβλιογραφία	280
	Ευρετήριο	282

Εισαγωγή

Η ιστορική εξέλιξη της Άλγεβρας χωρίζεται σε δύο περιόδους.

Η πρώτη περίοδος χρονολογείται μέχρι το τέλος του 17^{ου} αιώνα. Η Άλγεβρα της περιόδου αυτής λέγεται *Κλασσική Άλγεβρα* και χαρακτηρίζεται από το γεγονός ότι τα σύμβολα που χρησιμοποιεί παριστάνουν πάντοτε αριθμούς. Τα προβλήματα της, με τα οποία ασχολήθηκαν οι μαθηματικοί της εποχής αυτής, είναι κυρίως η λύση πολυωνυμικών εξισώσεων και γραμμικών συστημάτων.

Η Άλγεβρα της δεύτερης περιόδου λέγεται *αφηρημένη ή Σύγχρονη Άλγεβρα*. Η εποχή της αρχίζει με την αποδοχή ότι ένα σύμβολο μπορεί να παριστά *οτιδήποτε*: Μια συμμετρία ή στροφή ενός σχήματος του επιπέδου ή του χώρου, ένα διακόπτη, μια πράξη μεταξύ αντικειμένων της νοήσεως ακόμη και υλικό εισαγόμενο σε μια μηχανή.

Η σύγχρονη άλγεβρα βρίσκει εφαρμογές σε άλλους κλάδους των μαθηματικών, π.χ στη Γεωμετρία και τη Συνδυαστική και χρησιμοποιείται σε διάφορα πεδία επιστημών και της τεχνολογίας, όπως στην ατομική φυσική και την επιστήμη των υπολογιστών. Γενικεύει γνωστά συστήματα αριθμών κατασκευάζοντας νέα χρήσιμα συστήματα. Ενοποιεί φαινομενικά ξένες μεταξύ τους ενότητες και αποδεικνύει ότι πρόκειται περί των αυτών πραγμάτων υπό διάφορον μορφήν. Π.χ. οι στροφές του επιπέδου που απεικονίζουν ένα τετράγωνο στον εαυτό του ταυτίζονται με τους αριθμούς του συνόλου $\{1, i, -1, -i\}$.

Επί αιώνες προσπαθούσαν οι μαθηματικοί να λύσουν τις πολυωνυμικές εξισώσεις τρίτου βαθμού κάνοντας ρητές πράξεις με τους συντελεστές και βγάζοντας ριζικά, (μέθοδος των ριζικών) να βρουν δηλαδή τύπους ανάλογους του τύπου $x = \frac{(-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma})}{2\alpha}$, που μάς δίνει τις ρίζες εξίσωσης δευτέρου βαθμού $ax^2 + bx + \gamma = 0$.

Τελικά βρέθηκαν ανάλογοι τύποι από τον Ιταλό Tartaglia (1506(;)-1557). Ο Tartaglia παρατήρησε ότι η εξίσωση τρίτου βαθμού $x^3 + ax^2 + bx + \gamma = 0$ με

την αντικατάσταση $y = x + \frac{a}{3}$ μετασχηματίζεται στην εξίσωση $y^3 + py + q = 0$

(1). Παίρνοντας $\omega = \frac{-1 + \sqrt{-3}}{2}$, οπότε $\omega^3 = 1$ και $x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2)$, ο Tartaglia βρήκε ότι οι ρίζες της εξίσωσης (1) είναι

$$y_1 = a + \beta$$

$$y_2 = \omega a + \omega^2 \beta$$

$$y_3 = \omega^2 a + \omega \beta$$

όπου $a = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}$, $\beta = \sqrt[3]{-\frac{q}{2} - \sqrt{D}}$ και $D = \frac{q^2}{4} + \frac{q^3}{27}$ είναι η διακρίνουσα της εξίσωσης (1). Η λύση του Tartaglia δημοσιεύτηκε χωρίς την έγκρισή του από τον Cardano* και δημιουργήθηκε σύγχυση ως προς την κυριότητα της λύσης της τριτοβάθμιας εξίσωσης.

Το 1545 ο Ferrari, μαθητής του Cardano, έδωσε τη λύση της γενικής εξίσωσης τετάρτου βαθμού.

Μετά τη λύση των Tartaglia και Ferrari της εξίσωσης τρίτου και τετάρτου βαθμού, πολλοί πίστεψαν ότι γρήγορα θα βρεθούν και τύποι για τις λύσεις της εξίσωσης πέμπτου και ανωτέρου βαθμού.

Η πρώτη στη συνέχεια εντυπωσιακή ανακάλυψη οφείλεται στον Lagrange. Στο τέλος του 18^{ου} αιώνα ο Lagrange παρουσιάζει μέθοδο αναγωγής της λύσης μιας εξίσωσης σε λύση άλλων εξισώσεων, οι οποίες ονομάστηκαν επιλύουσες. Αν η εξίσωση είναι βαθμού ≤ 4 , οι επιλύουσες εξισώσεις είναι μικρότερου βαθμού, οπότε η λύση εξίσωσης τετάρτου βαθμού ανάγεται σε λύση εξίσωσης τρίτου βαθμού και αυτή σε λύση δευτεροβάθμιας εξίσωσης. Όμως οι επιλύουσες εξισώσεις των εξισώσεων πέμπτου βαθμού είναι έκτου βαθμού. Και τότε για πρώτη φορά διατυπώνεται η άποψη ότι δυνατόν η εξίσωση 5^{ου} βαθμού να μην επιλύεται με τη μέθοδο των ριζικών.

Και πραγματικά, ο Abel αποδεικνύει το 1828 ότι δεν υπάρχουν τύποι που να δίνουν τις ρίζες εξίσωσης πέμπτου βαθμού, όπως σε εξισώσεις μικρότερου βαθμού.

Πρέπει να σημειωθεί ότι και ο Ruffini έδωσε το 1813 μια απόδειξη αυτού, η οποία όμως αποδείχτηκε το 1876 ότι είχε κενά.

Ικανή και αναγκαία συνθήκη για να είναι επιλύσιμη μια εξίσωση με τη μέθοδο των ριζικών έδωσε ο Evariste Galois (1811 + 20 χρόνια και 7 μήνες) θέτοντας τα θεμέλια για τη σύγχρονη θεωρία εξισώσεων.

* Είναι ενδιαφέρον ν' αναφέρουμε δείγμα γραφής της εποχής Cardano. Αντί $\sqrt{7 + \sqrt{14}}$ γράφει ο Cardano R.V.7p:R14. Το γράμμα V σήμαινε ότι όλα τα επόμενα είναι κάτω από το ριζικό.

Δύο άρθρα του, που έστειλε το 1829 και 1830 στην Ακαδημία Παρισίων, χάθηκαν. Το τρίτο άρθρο του με τίτλο "*Memoire sur les conditions de résolvibilité des équations par radicaux*" επιστράφηκε ως ακατανόητο από τον Poisson το 1831. Την τελευταία νύχτα της ζωής του, πριν τη μοιραία μονομαχία που θα έδινε, έστειλε στο φίλο του Auguste Chevalier τ' αποτελέσματά του. Μετά από πολλές προσπάθειες του αδελφού του και του φίλου του ανακοινώθηκαν στη Ακαδημία των Παρισίων από τον Liouville το 1843. Η ευφυής μαθηματική ιδέα του Galois ήταν ν' αντιστοιχίσει σε μια εξίσωση $x^n + a_n x^{n-1} + \dots + a_1 x + a_0 = 0$ με συντελεστές από ένα σώμα, μια ομάδα μεταθέσεων των ριζών $x_1, x_2, \dots, x_n$, οι οποίες αφήνουν αμετάβλητες όλες τις σχέσεις των ριζών με τιμές τιμές στο σώμα των συντελεστών. Π.χ. έστω η εξίσωση $x^4 - x^2 - 2 = 0$. Οι ρίζες της x_1, x_2, x_3, x_4 πληρούν τις σχέσεις $x_1 x_2 = -2$, $x_1 + x_2 = 0$, $x_3 x_4 = 1$, $x_3 + x_4 = 0$. Οι μεταθέσεις των ριζών που αφήνουν αναλλοίωτες τις σχέσεις αυτές είναι τέσσερις, η ταυτοτική, η μετάθεση που αλλάζει τις x_1, x_2 (ή x_3, x_4) και αφήνει σταθερές τις x_3, x_4 , (αντίστοιχα x_1, x_2) και εκείνη που αλλάζει ταυτόχρονα τις x_1, x_2 και x_3, x_4 . Αυτές οι μεταθέσεις αποτελούν μια ομάδα και η επιλυσιμότητα της εξίσωσης μεταφράζεται από τον Galois με απλή ιδιότητα της ομάδας αυτής.

Η θεωρία των ομάδων μετά την εφαρμογή της στη θεωρία εξισώσεων, καθιερώνεται θριαμβευτικά σε περίοπτη θέση στα μαθηματικά.

Ένα άλλο πεδίο εφαρμογών της θεωρίας των ομάδων και της Άλγεβρας γενικότερα είναι η Γεωμετρία.

Τα περίφημα άλυτα προβλήματα της αρχαιότητας, ο διπλασιασμός του κύβου, η τριχοτόμηση γωνίας και ο τετραγωνισμός του κύκλου με κανόνα και διαβήτη βρίσκουν τη λύση τους με τη σύγχρονη θεωρία των επεκτάσεων των σωμάτων.

Το 19^ο αιώνα έγινε μεγάλη αναστάτωση στο χώρο της Γεωμετρίας. Ανακαλύπτονται Γεωμετρίες διάφορες της Ευκλείδειας Γεωμετρίας. Η διαφορά τους είναι το αξίωμα του Ευκλείδη κατά το οποίο από κάθε σημείο P εκτός δοσμένης ευθείας (ε) περνά μια μόνο ευθεία παράλληλη προς αυτήν. Οι μη Ευκλείδειες γεωμετρίες δέχονται ότι περνούν από το σημείο P άπειρες παράλληλες ευθείες στην (ε) (Γεωμετρία του Lobatchevski) ή καμμία (Γεωμετρία Riemann).

Ο Lobatchevski δέχεται ότι υπάρχει μια γωνία $\pi(a)$, που εξαρτάται από την απόσταση α του σημείου P από την ευθεία (ε), ονομαζόμενη γωνία της *παράλληλης*, με την εξής ιδιότητα: Όλες οι ευθείες που περνούν από το P και σχηματίζουν με την κάθετο PP' στην (ε) γωνία μικρότερη της $\pi(a)$ τέμνουν την ευθεία, ενώ όλες οι άλλες δεν την τέμνουν. Αν $\pi(a) = \frac{\pi}{2}$, έχουμε

την Ευκλείδεια Γεωμετρία. Η γωνία $\pi(a) \rightarrow \frac{\pi}{2}$, όταν $a \rightarrow 0$ και $\pi(a) \rightarrow 0$, όταν $a \rightarrow \infty$. Ο Lobatchevski απέδειξε ότι το άθροισμα των γωνιών ενός τριγώνου είναι $< \pi$ και ο Riemann ότι είναι $> \pi$.

Προς τα τέλη του 19^{ου} αιώνα ο Felix Klein προτείνει να διακρίνουν τις Γεωμετρίες μεταξύ τους μέσω μιας ομάδας μετασχηματισμών: Γεωμετρία είναι η μελέτη των ιδιοτήτων εκείνων που μένουν αναλλοίωτες με μια ομάδα μετασχηματισμών.

Η ανάπτυξη της αντιμεταθετικής άλγεβρας όχι μόνο μας έδωσε ένα σύγχρονο κλάδο της άλγεβρας, αλλά συνετέλεσε στη δημιουργία ενός νέου κλάδου των Μαθηματικών, της *Αλγεβρικής Γεωμετρίας*. Γεωμετρικά προβλήματα επιλύονται με μεθόδους της σύγχρονης άλγεβρας. Και αντίστροφα.

Ένα άλλο πεδίο της άλγεβρας είναι η *Θεωρία Αριθμών*, η μελέτη δηλαδή των ιδιοτήτων των ακεραίων αριθμών. Υπάρχουν πολλά και πολύπλοκα προβλήματα στην περιοχή αυτή.

Ένα πρόβλημα για τη λύση του οποίου εισήχθησαν νέες ιδέες και τεχνικές είναι το περίφημο πρόβλημα του Fermat ότι η εξίσωση $x^n + y^n = z^n$ για $n \geq 3$ δεν έχει ακέραιες λύσεις x, y, z . Το πρόβλημα αυτό λύθηκε ύστερα από προσπάθειες 350 χρόνων των μεγαλύτερων μαθηματικών πριν 3 περίπου χρόνια, με μεθόδους της Αλγεβρικής Γεωμετρίας.

Ένα από τα σπουδαιότερα προβλήματα της θεωρίας των ομάδων είναι η ταξινόμηση όλων των ομάδων, πεπερασμένης τάξης, οι οποίες δεν είναι ισόμορφες μεταξύ τους (βλ.Κεφ.5). Το πρόβλημα αυτό αναλύεται σε δύο υποπροβλήματα:

- α) Τον προσδιορισμό όλων των πεπερασμένων απλών ομάδων (ομάδων με δύο μόνο υποομάδες).
- β) Τον προσδιορισμό των πεπερασμένων ομάδων G , οι οποίες περιέχουν δοσμένη ομάδα K σαν κανονική υποομάδα και το πηλίκο G/K είναι ισόμορφη ομάδα με μια άλλη ομάδα H .

Το πρόβλημα (α) λύθηκε την περασμένη δεκαετία. Οι σχετικές εργασίες καταλαμβάνουν 15000 σελίδες περίπου σε διάφορα περιοδικά. Η κλάση των απλών πεπερασμένων ομάδων περιλαμβάνει 18 υποκλάσεις ομάδων και 26 μεμονομένες ομάδες.

Το δεύτερο πρόβλημα αποτελεί θέμα ενός πεδίου, που ονομάζεται *συνομολογίες ομάδων* (cohomology of groups).

Στο τέλος του 19^{ου} αιώνα ο Sophus Lie άρχισε τη μελέτη μιας κλάσης άπειρων ομάδων, οι οποίες ονομάζονται *συνεχείς ομάδες* και είναι χρήσιμες στη θεωρία των διαφορικών εξισώσεων και των εφαρμογών τους στη

Μηχανική.

Μια άλλη κλάση άπειρων ομάδων είναι η κλάση των *ασυνεχών ομάδων*, που μελετήθηκαν από τους Poincaré, Klein, Frilke (κ.α.) σε σχέση με μια κλάση μιγαδικών συναρτήσεων (automorphic functions).

Στην εισαγωγή αυτή επιχειρήσαμε να επισημάνουμε την προέλευση θεμάτων της σύγχρονης άλγεβρας.

Στο κείμενο που ακολουθεί γίνονται επί πλέον ιστορικές αναφορές.

Στο κεφάλαιο 0 παρουσιάζονται βασικές έννοιες και εφαρμογές αυτών, απαραίτητες για τη μελέτη σύγχρονων μαθηματικών, κυρίως αλγεβρικών θεωριών.

Τα υπόλοιπα κεφάλαια 1-14 αποτελούν διδακτικές ενότητες με τη μικρότερη δυνατή έκταση, αρκετή για μια ικανοποιητική ενημέρωση του αναγνώστη στα διαπραγματευόμενα θέματά τους. Κάθε κεφάλαιο συνοδεύεται από πολλά παραδείγματα, από εφαρμογές και μια επιμελημένη συλλογή ασκήσεων.

Ο τίτλος του κεφαλαίου, λόγω της μικρής έκτασής του, προσδιορίζει το περιεχόμενό του. Οι παρατηρούμενες επαναλήψεις σκοπό έχουν τη διευκόλυνση του αναγνώστη.

Αφορμή για τη συγγραφή του παρόντος στάθηκε η επιθυμία των φοιτητών μας, που εκφράστηκε προ εξαμήνου σε γενική συνέλευση του Τομέα Θεωρητικών Μαθηματικών.

Η επιθυμία τους αυτή πραγματοποιήθηκε με την πολύτιμη συνεργασία και βοήθεια του μεταπτυχιακού μας φοιτητή κ. Παναγιώτη Σκοινιώτη. Τον ευχαριστώ θερμά.

Δ. Στρατηγόπουλος
Καθηγητής Πανεπιστημίου Πατρών

Ο | Σύνολα συναρτήσεις, σχέσεις

Στα μαθηματικά ασχολούμεθα με οικογένειες αντικειμένων. Μια οικογένεια αντικειμένων είναι καθορισμένη, όταν δίνεται μια ιδιότητα με την οποία μπορούμε να διακρίνουμε αν κάποιο αντικείμενο ανήκει στην οικογένεια ή δεν ανήκει.

Μια μαθηματική θεωρία συνίσταται από μια οικογένεια αντικειμένων και από προτάσεις που θεωρούνται αληθείς και λέγονται αξιώματα της θεωρίας.

Ανάπτυξη της θεωρίας σημαίνει αποδείξεις θεωρημάτων, απαντήσεις δηλαδή, σε ερωτήματα αν άλλες προτάσεις είναι αληθείς. Με τον όρο πρόταση εννοούμε ένα πλήθος λέξεων στο οποίο μπορούμε ν' αντιστοιχίσουμε τη λογική τιμή "αληθής ή ψευδής".

Τα αξιώματα μιας θεωρίας δεν πρέπει να οδηγούν σε αντίφαση, σε θεωρήματα δηλαδή του τύπου "η πρόταση P είναι αληθής και ψευδής".

Μια οικογένεια E αντικειμένων με μια κοινή ιδιότητα I λέγεται **σύνολο**. Κάθε αντικείμενο της οικογένειας E λέγεται **στοιχείο** ή **μέλος** του συνόλου E .

Αν E είναι ένα σύνολο και το αντικείμενο x είναι στοιχείο του συνόλου E , γράφουμε $x \in E$. Διαφορετικά γράφουμε $x \notin E$. Αν I είναι η

ιδιότητα με την οποία διακρίνουμε τα στοιχεία ενός συνόλου E , γράφουμε $E = \{x; x \text{ έχει την ιδιότητα } I\}$, π.χ. $\mathbb{R}^+ = \{x; x \in \mathbb{R} \text{ και } x > 0\}$.

Αν P, Q δύο προτάσεις, γράφουμε $P \Rightarrow Q$, στις εξής περιπτώσεις:

- 1) P αληθής, Q αληθής
- 2) P ψευδής, Q ψευδής
- 3) P ψευδής, Q αληθής

Γράφουμε $P \not\Rightarrow Q$, αν η P είναι αληθής και η Q ψευδής. Δύο προτάσεις P, Q λέγονται λογικά ισοδύναμες και γράφουμε $P \Leftrightarrow Q$, όταν $P \Rightarrow Q$ και $Q \Rightarrow P$.

Για κάθε πρόταση P υπάρχει μια πρόταση Q , που είναι η άρνηση της P . Όταν η P είναι αληθής, η Q είναι ψευδής και όταν η P είναι ψευδής, η Q είναι αληθής. Η πρόταση Q συμβολίζεται με P' .

Συνδυάζοντας δύο προτάσεις A, B , που καθεμιά από αυτές μπορεί να είναι αληθής ή ψευδής, μπορούμε να σχηματίσουμε την πρόταση " A και B " και την πρόταση " A ή B ". Η τιμή αληθείας των νέων προτάσεων εξαρτάται βεβαίως από την τιμή αληθείας των A, B και δίνεται από τον παρακάτω πίνακα, όπου a σημαίνει αληθής και ψ ψευδής. Στον ίδιο πίνακα δίνεται και η τιμή αληθείας της πρότασης " $A \Rightarrow B$ "

A	B	$A \text{ και } B$	$A \text{ ή } B$	$A \Rightarrow B$
a	a	a	a	a
a	ψ	ψ	a	ψ
ψ	a	ψ	a	a
ψ	ψ	ψ	ψ	a

Ο πίνακας αληθείας της άρνησης P' της πρότασης P είναι

P	P'
a	ψ
ψ	a

Έστω I μια ιδιότητα. Αν υπάρχει στοιχείο του συνόλου A με την ιδιότητα I , γράφουμε $(\exists x \in A) I$. Αν κάθε στοιχείο του συνόλου A έχει την ιδιότητα I , γράφουμε $(\forall x \in A) I$. Η άρνηση της πρότασης $(\forall x \in A) P$ είναι η πρόταση $(\exists x \in A) P'$. Η άρνηση της πρότασης $(\exists x \in A) P$ είναι η πρόταση $(\forall x \in A) P'$.

Ο κανόνας απόδειξης στον οποίο ανάγονται όλες οι αποδείξεις είναι ο εξής:

Αν $P \Rightarrow Q$ και το P είναι θεώρημα, τότε Q είναι θεώρημα.

Μια αξιωματική θεμελίωση της θεωρίας των συνόλων παρουσιάζει μεγάλες δυσκολίες και δεν είναι απαραίτητη για το σκοπό του βιβλίου. Περιοριζόμαστε στην περιγραφική θεωρία των συνόλων.

1. ΣΥΝΟΛΑ, ΑΛΓΕΒΡΑ BOOLE

Ορίζοντας πράξεις με σύνολα, που έχουν στοιχεία σ' ένα σύνολο E , δημιουργούμε μια άλγεβρα.

Η άλγεβρα αυτή έχει ενδιαφέρουσες εφαρμογές στη θεωρία π.χ. των κυκλωμάτων των διακοπών και στην προτασιακή λογική. Χρονολογείται από το 1947, όταν ο George Boole δημοσίευσε το βιβλίο του "*The Mathematical Analysis of Logic*", όπου υπεδείκνυε πώς αλγεβρικά σύμβολα μπορούν να χρησιμοποιηθούν στη λογική. Γι' αυτό η άλγεβρα αυτή φέρει το όνομα άλγεβρα Boole.

Ορισμός 1. Ένα σύνολο A λέγεται υποσύνολο του B και γράφουμε $A \subseteq B$ (ή $B \supseteq A$), αν όλα τα στοιχεία του A είναι στοιχεία του B . Συμβολικά:

$$A \subseteq B \Leftrightarrow (a \in A \Rightarrow a \in B)$$

Π.χ. $\{1, 2, 3\} \subseteq \{0, 1, 2, 3, 4\}$, $\{X, A\} \subseteq \{A, B, \Gamma, X\}$.

Γράφουμε $A \subset B$, αν $A \subseteq B$ και $A \neq B$. Το A λέγεται τότε **γνήσιο** υποσύνολο του B .

Πρόταση 1. Για οποιαδήποτε σύνολα A, B, Γ , ισχύουν οι ιδιότητες:

1. $A \subseteq A$
2. $A \subseteq B, B \subseteq A \Rightarrow A = B$
3. $A \subseteq B, B \subseteq \Gamma \Rightarrow A \subseteq \Gamma$
4. $A = B \Leftrightarrow (A \subseteq B \text{ και } B \subseteq A)$

Η απόδειξη είναι απλή. □

Δεχόμαστε την ύπαρξη ενός συνόλου χωρίς στοιχεία. Το σύνολο αυτό λέγεται **κενό** σύνολο και συμβολίζεται με $\emptyset$.

Πρόταση 2. Για κάθε σύνολο A , $\emptyset \subseteq A$.

Απόδειξη. Δεν υπάρχει στοιχείο του $\emptyset$, που δεν ανήκει στο A . □

Σε πολλές περιπτώσεις η μελέτη συνόλων προσεγγίζεται με την ανάλυση των συνόλων αυτών σε απλά υποσύνολα. Με τη σύνθεση αυτών μπορούμε να έχουμε σαφέστερη εικόνα τους. Έτσι είναι χρήσιμο να δούμε τρόπους κατασκευής νέων συνόλων από γνωστά σύνολα.

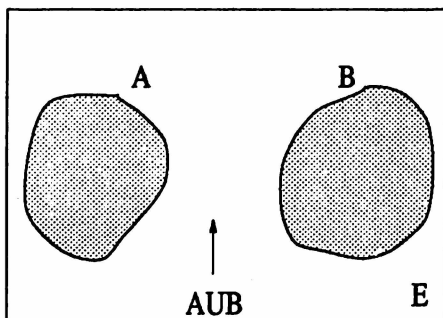
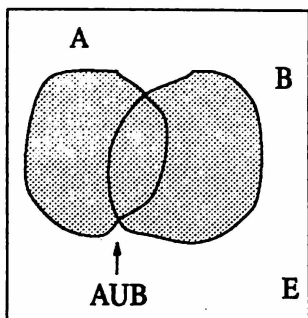
Δυναμοσύνολο ενός συνόλου A λέγεται το σύνολο των υποσυνόλων του και συμβολίζεται με $\mathcal{P}(A)$. Συνεπώς

$$\mathcal{P}(A) = \{X; X \subseteq A\}$$

Π.χ. αν $A = \{a, \beta\}$, τότε $\mathcal{P}(A) = \{\emptyset, \{a\}, \{\beta\}, A\}$.

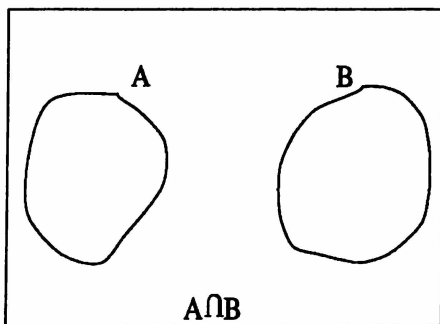
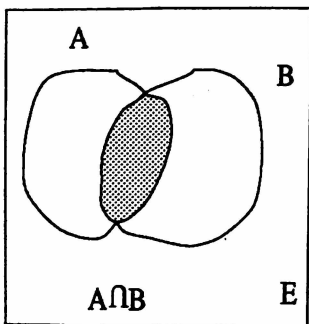
Ένωση δύο συνόλων A, B λέγεται το σύνολο που περιέχει ως στοιχεία τα στοιχεία των A, B και μόνο αυτά. Συμβολίζεται με $A \cup B$. Συνεπώς

$$A \cup B = \{x; x \in A \text{ ή } x \in B\}$$



Τομή δύο συνόλων A, B λέγεται το σύνολο που περιέχει ως στοιχεία τα κοινά στοιχεία των A, B και μόνο αυτά. Συμβολίζεται με $A \cap B$. Συνεπώς

$$A \cap B = \{x; x \in A \text{ και } x \in B\}$$



Αν $A \cap B = \emptyset$, τα σύνολα A, B λέγονται **ξένα** μεταξύ τους.

Παράδειγμα 1. Έστω

$$A = \{(x, y); x, y \in \mathbb{R} \text{ με } x - 2y + a = 0\}$$

$$B = \{(x, y); x, y \in \mathbb{R} \text{ με } x^2 + y^2 = \beta^2\}$$

Τότε

$$A \cup B = \{(x, y); x, y \in \mathbb{R} \text{ με } (x - 2y + a)(x^2 + y^2 - \beta^2) = 0\}$$

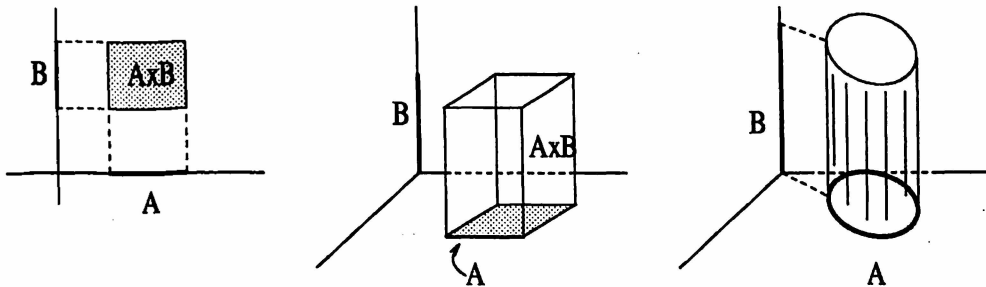
$$A \cap B = \{(x, y); x, y \in \mathbb{R} \text{ με } \lambda(x - 2y + a) + \mu(x^2 + y^2 - \beta^2) = 0, \lambda, \mu \in \mathbb{R}\}$$

Καρτεσιανό γινόμενο δύο συνόλων A, B λέγεται το σύνολο των στοιχείων της μορφής (a, β) , όπου $a \in A$ και $\beta \in B$. Τα στοιχεία (a, β) λέγονται διατεταγμένα ζεύγη και το καρτεσιανό γινόμενο των A, B συμβολίζεται με $A \times B$. Συνεπώς

$$A \times B = \{(a, \beta); a \in A \text{ και } \beta \in B\}.$$

Προφανώς $A \times \emptyset = \emptyset$.

Σε μερικές περιπτώσεις μπορούμε να παραστήσουμε γραφικά το καρτεσιανό γινόμενο:



Πρόταση 3. Για οποιαδήποτε σύνολα A, B, Γ ισχύει

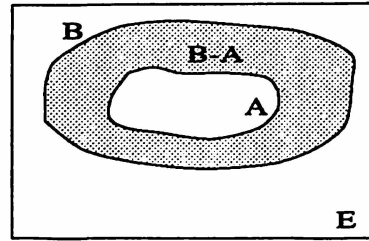
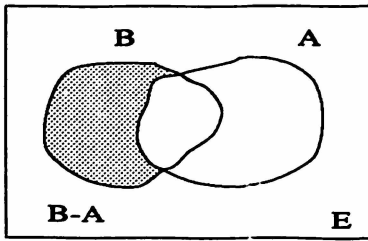
1. $A \times (B \cup \Gamma) = (A \times B) \cup (A \times \Gamma)$
2. $A \times (B \cap \Gamma) = (A \times B) \cap (A \times \Gamma)$

Απόδειξη. 1) Έστω $x \in A \times (B \cup \Gamma)$. Τότε $x = (a, \beta)$ με $a \in A$ και $\beta \in B \cup \Gamma$. Συνεπώς $x = (a, \beta)$ με $a \in A$ και $\beta \in B$ ή $\beta \in \Gamma$, οπότε $x \in A \times B$ ή $x \in A \times \Gamma$, δηλαδή $A \times (B \cup \Gamma) \subseteq (A \times B) \cup (A \times \Gamma)$.

Αντίστροφα, έστω x στοιχείο του δεύτερου μέλους της 1. Τότε $x = (a, \beta)$ με $a \in A$, $\beta \in B$ ή $x = (a, \beta)$ με $a \in A$ και $\beta \in \Gamma$, συνεπώς $x = (a, \beta)$ με $a \in A$ και $\beta \in B \cup \Gamma$, δηλαδή $x \in A \times (B \cup \Gamma)$. Ανάλογα αποδεικνύεται η 2. □

Διαφορά του συνόλου A από το σύνολο B λέγεται το σύνολο

$$B - A = \{x; x \in B \text{ και } x \notin A\}.$$



Πρόταση 4. Για οποιαδήποτε υποσύνολα A, B, Γ του E ισχύει

- 1) $A - B = \emptyset \Leftrightarrow A \subseteq B$
- 2) $A \cap (B - \Gamma) = (A \cap B) - (A \cap \Gamma)$
- 3) $A \cup (B - \Gamma) \supseteq (A \cup B) - (A \cap \Gamma)$

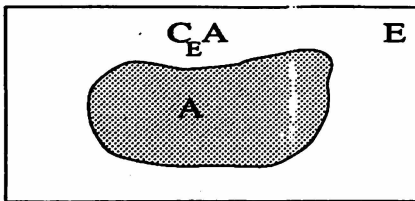
Οι αποδείξεις είναι απλές και παραλείπονται. □

Συμπλήρωμα ενός υποσυνόλου A του E ως προς E λέγεται το σύνολο $E - A$ και συμβολίζεται με $C_E A$ ή A' , όταν το E υπονοείται. Συνεπώς

$$A' = \{x \in E; x \notin A\}$$

Πρόταση 5. Έχουμε $(A')' = A$, $A \cap A' = \emptyset$, $A \cup A' = E$.

Η απόδειξη είναι απλή. □



$$C_E E = \emptyset, C_E \emptyset = E.$$

Θεώρημα 1. Για οποιαδήποτε υποσύνολα X, Y, Z του E ισχύουν οι ιδιότητες:

1. Η προσεταιριστική ιδιότητα της ένωσης και της τομής

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z, \quad X \cap (Y \cap Z) = (X \cap Y) \cap Z$$

2. Η αντιμεταθετική ιδιότητα της ένωσης και της τομής

$$X \cup Y = Y \cup X, \quad X \cap Y = Y \cap X$$

3. Η ιδιότητα του "αδυνάμου" της ένωσης και της τομής

$$X \cup X = X, \quad X \cap X = X$$

Δηλαδή δεν υπάρχουν "δυνάμεις" του X ως προς την ένωση και την τομή διάφορες του X , όπως π.χ. στον πολλαπλασιασμό των πραγματικών αριθμών που $x \cdot x = x$ μόνο για $x = 0$ ή $x = 1$.

4. Οι ιδιότητες των Pierce και De Morgan

$$(A \cup B)' = A' \cap B' \quad , \quad (A \cap B)' = A' \cup B'$$

5. Η επιμεριστική ιδιότητα της τομής ως προς την ένωση

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

και της ένωσης ως προς την τομή

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

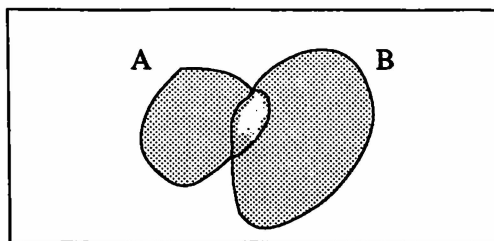
Οι αποδείξεις δεν παρουσιάζουν δυσκολία.

□

Συνεχίζουμε την κατασκευή συνόλων από δύο σύνολα A, B .

Συμμετρική διαφορά δύο συνόλων A, B λέγεται το σύνολο

$$\begin{aligned} A \Delta B &= (A \cap B') \cup (B \cap A') \\ &= (A - B) \cup (B - A) \\ &= (A \cup B) - (A \cap B) \end{aligned}$$



Θεώρημα 2. Η συμμετρική διαφορά έχει τις παρακάτω ιδιότητες

1. $A \Delta B = B \Delta A$
2. $A \Delta \emptyset = A$, $A \Delta A = \emptyset$
3. $A \Delta E = A'$, $A \Delta A' = E$
4. $A \Delta (B \Delta \Gamma) = (A \Delta B) \Delta \Gamma$
5. $A \cap (B \Delta \Gamma) = (A \cap B) \Delta (A \cap \Gamma)$

Αποδεικνύουμε τις ιδιότητες 4,5. Οι υπόλοιπες είναι απλές.

- (4) Έχουμε $A\Delta(B\Delta\Gamma) = (A \cap (B\Delta\Gamma)') \cup (A' \cap (B\Delta\Gamma))$. Βάσει της πρότ.4 και του θεωρ.1(2,4,5) έχουμε

$$\begin{aligned}
 A \cap (B\Delta\Gamma)' &= A \cap ((B \cap \Gamma') \cup (\Gamma \cap B'))' \\
 &= A \cap ((B \cap \Gamma')' \cap (\Gamma \cap B')') \\
 &= A \cap ((B' \cup \Gamma) \cap (B \cup \Gamma')) \\
 &= A \cap (((B' \cup \Gamma) \cap B) \cup ((B' \cup \Gamma) \cap \Gamma')) \\
 &= A \cap (((B' \cap B) \cup (\Gamma \cap B)) \cup ((B' \cap \Gamma') \cup (\Gamma \cap \Gamma'))) \\
 &= A \cap ((\Gamma \cap B) \cup (B' \cap \Gamma')) \\
 &= (A \cap (\Gamma \cap B)) \cup (A \cap (B' \cap \Gamma')) \\
 &= (A \cap B \cap \Gamma) \cup (A \cap B' \cap \Gamma')
 \end{aligned}$$

και

$$\begin{aligned}
 A' \cap (B\Delta\Gamma) &= A' \cap ((B \cap \Gamma') \cup (B' \cap \Gamma)) \\
 &= (A' \cap (B \cap \Gamma')) \cup (A' \cap (B' \cap \Gamma)) \\
 &= (A' \cap B \cap \Gamma') \cup (A' \cap B' \cap \Gamma)
 \end{aligned}$$

Συνεπώς

$$A\Delta(B\Delta\Gamma) = (A \cap B \cap \Gamma) \cup (A \cap B' \cap \Gamma') \cup (A' \cap B \cap \Gamma') \cup (A' \cap B' \cap \Gamma)$$

δηλαδή $A\Delta(B\Delta\Gamma)$ είναι συμμετρική ως προς A, B, Γ . Άρα

$$A\Delta(B\Delta\Gamma) = \Gamma\Delta(A\Delta B) = (A\Delta B)\Delta\Gamma$$

- (5) Είναι

$$\begin{aligned}
 A \cap (B\Delta\Gamma) &= A \cap ((B' \cap \Gamma) \cup (B \cap \Gamma')) \\
 &= (A \cap (B' \cap \Gamma)) \cup (A \cap (B \cap \Gamma')) \\
 &= (A \cap B' \cap \Gamma) \cup (A \cap B \cap \Gamma')
 \end{aligned}$$

και

$$\begin{aligned}
 (A \cap B)\Delta(A \cap \Gamma) &= ((A \cap B) \cap (A \cap \Gamma)') \cup ((A \cap B)' \cap (A \cap \Gamma)) \\
 &= ((A \cap B) \cap (A' \cup \Gamma')) \cup ((A' \cup B') \cap (A \cap \Gamma)) \\
 &= ((A \cap B) \cap A') \cup ((A \cap B) \cap \Gamma') \cup \\
 &\quad ((A' \cap (A \cap \Gamma)) \cup ((A \cap \Gamma) \cap B')) \\
 &= (A \cap B \cap \Gamma') \cup (A \cap B' \cap \Gamma) = A \cap (B\Delta\Gamma)
 \end{aligned}$$

Άρα η ιδιότητα αποδείχτηκε. □

Οικογένειες συνόλων

Έστω ένα σύνολο $I \neq \emptyset$ και για κάθε $i \in I$ ένα υποσύνολο A_i ενός συνόλου E . Το σύνολο I λέγεται σύνολο **δεικτών** και το σύνολο των συνόλων A_i με $i \in I$ **οικογένεια** συνόλων με σύνολο δεικτών I . Την οικογένεια αυτή συμβολίζουμε με $(A_i)_{i \in I}$. Ορίζουμε την ένωση $\bigcup_{i \in I} A_i$ και την τομή $\bigcap_{i \in I} A_i$ της οικογένειας $(A_i)_{i \in I}$ ως εξής:

$$\bigcup_{i \in I} A_i = \{x; \text{υπάρχει } i \in I \text{ τέτοιο, ώστε } x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x; \text{για κάθε } i \in I, x \in A_i\}$$

Το καρτεσιανό γινόμενο της οικογένειας $(A_i)_{i \in I}$ συμβολίζεται με $\prod_{i \in I} A_i$ και ορίζεται από την ισότητα

$$\prod_{i \in I} A_i = \{x; x = (x_i)_{i \in I} \text{ με } x_i \in A_i\}$$

2. ΣΥΝΑΡΤΗΣΕΙΣ

Έστω A, B δύο σύνολα. Μία αντιστοιχία των στοιχείων των A, B έτσι, ώστε σε κάθε στοιχείο x του A ν' αντιστοιχίζεται ένα **μόνο** στοιχείο y του B λέγεται **συνάρτηση** με πεδίο ορισμού A και πεδίο τιμών B . Αν f μια συνάρτηση με πεδίο ορισμού το σύνολο A και πεδίο τιμών το B , γράφουμε

$$f: A \rightarrow B \quad \text{ή} \quad A \xrightarrow{f} B$$

Αν στο $x \in A$ αντιστοιχίζεται με την f το $y \in B$, γράφουμε $x \xrightarrow{f} y$ ή $y = f(x)$. Το x λέγεται **αρχέτυπο** και το y **τιμή** της f στο x .

Το σύνολο $\{f(x); x \in A\}$ συμβολίζεται με $f(A)$ και λέγεται **σύνολο τιμών** της $f: A \rightarrow B$ ή **εικόνα** της f . Αν $f(A) = B$, η συνάρτηση $f: A \rightarrow B$ λέγεται επί του B . Μια συνάρτηση $f: A \rightarrow B$ λέγεται **αμφιμονοσήμαντη** ή 1-1, αν $f(x) = f(y)$ συνεπάγεται $x = y$. Προφανώς η $f: A \rightarrow B$ είναι αμφιμονοσήμαντη, αν

$$x, y \in A, x \neq y \Rightarrow f(x) \neq f(y)$$

Δύο συναρτήσεις $f: A \rightarrow B$ και $g: \Gamma \rightarrow \Delta$ λέγονται **ίσες** και γράφουμε $f = g$, αν

$$A = \Gamma, B = \Delta \text{ και } f(x) = g(x) \text{ για κάθε } x \in A.$$

Γράφημα ή γραφική παράσταση της $f : A \rightarrow B$ λέγεται το σύνολο $\{(x, f(x)); x \in A\}$.

Έστω $S \subseteq A$. Η συνάρτηση $g : S \rightarrow B$ με τιμή $g(x) = f(x)$ για κάθε $x \in S$, λέγεται **περιορισμός** της f στο S , ενώ η f λέγεται **επέκταση** της g στο A .

Η συνάρτηση $f : A \rightarrow A$ με τιμή $f(x) = x$ για κάθε $x \in A$ λέγεται **ταυτοτική** συνάρτηση του A και συμβολίζεται με 1_A . Έτσι $1_A(x) = x$ για κάθε $x \in A$. Οι συναρτήσεις

$$P_1 : A \times B \rightarrow A, \quad (a, \beta) \xrightarrow{P_1} a$$

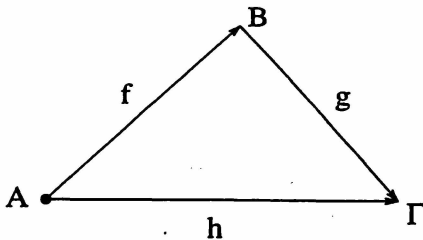
$$P_2 : A \times B \rightarrow B, \quad (a, \beta) \xrightarrow{P_2} \beta$$

λέγονται **προβολές** του καρτεσιανού γινομένου $A \times B$, η P_1 πρώτη προβολή και η P_2 δεύτερη προβολή.

Έστω δύο συναρτήσεις $f : A \rightarrow B$ και $g : B \rightarrow \Gamma$. Η συνάρτηση $h : A \rightarrow \Gamma$ με τιμή $h(x) = g(f(x))$ για κάθε $x \in A$, λέγεται **σύνθεση** των συναρτήσεων f, g και συμβολίζεται με $g \circ f$. Συνεπώς η σύνθεση των f, g είναι η συνάρτηση

$$g \circ f : A \rightarrow \Gamma \text{ με τιμή } (g \circ f)(x) = g(f(x)).$$

Το παρακάτω διάγραμμα λέγεται **αντιμεταθετικό**, αν $h = g \circ f$



$$h = g \circ f.$$

Πρόταση 1. Έστω οι συναρτήσεις $A \xrightarrow{f} B, B \xrightarrow{g} \Gamma, \Gamma \xrightarrow{h} \Delta$. Τότε

- i) $f \circ 1_A = f = 1_B \circ f$
- ii) $h \circ (g \circ f) = (h \circ g) \circ f$

Απόδειξη. Για κάθε $x \in A$ έχουμε $f \circ 1_A(x) = f(1_A(x)) = f(x)$ και οι συναρτήσεις $f \circ 1_A, f$ έχουν το ίδιο πεδίο ορισμού και πεδίο τιμών. Όμοια $1_B \circ f = f$.

- ii) Το πεδίο ορισμού της $h \circ (g \circ f)$ είναι το πεδίο ορισμού της $g \circ f$, συνεπώς το πεδίο ορισμού της f , δηλαδή το A . Όμοια και της $(h \circ g) \circ f$. Επιπλέον για κάθε $x \in A$,

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) \\ &= ((h \circ g) \circ f)(x) \end{aligned}$$

Άρα η σχέση (ii) αποδείχτηκε. $\square$

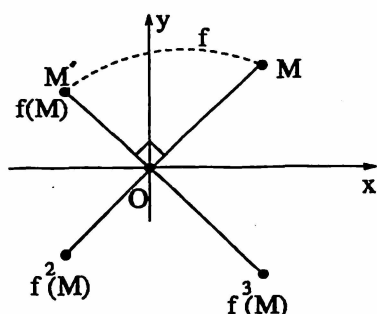
Παρατήρηση. Λόγω της ιδιότητας (ii) της σύνθεσης των συναρτήσεων, γράφουμε $f \circ g \circ h$ αντί $f \circ (g \circ h)$ ή $(f \circ g) \circ h$, αφού πρόκειται για ίσες συναρτήσεις.

Το σύνολο των συναρτήσεων $f : A \rightarrow B$ συμβολίζεται με B^A . Στο σύνολο A^A ορίζονται οι "δυνάμεις ως προς τη σύνθεση μιας συνάρτησης $f \in A^A$ ", όπως οι δυνάμεις ως προς τον πολλαπλασιασμό των πραγματικών αριθμών:

$$f^0 = 1_A, f^1 = f, f^2 = f \circ f, \dots, f^n = f \circ f^{n-1}.$$

Παράδειγμα 1. Έστω f η στροφή του επιπέδου κατά γωνία 90° γύρω

από την αρχή O . Τότε f^2 είναι η στροφή κατά γωνία 180° , f^3 η στροφή κατά 270° και f^4 η στροφή κατά 360° , δηλαδή η ταυτοτική συνάρτηση του επιπέδου.



Η συνάρτηση $f : A \rightarrow B$ λέγεται **αντίστροφη** της $g : B \rightarrow A$, αν

$$g \circ f = 1_A \text{ και } f \circ g = 1_B \quad (1)$$

Τότε και η g είναι αντίστροφη της f . Αν η f είναι αντίστροφη μιας συνάρτησης g , λέμε ότι η f **αντιστρέφεται**.

Η μία μόνο από τις παραπάνω σχέσεις (1) δεν εξασφαλίζει την αντιστροφή της συνάρτησης f .

Παράδειγμα 2. Έστω οι συναρτήσεις $f, g : \mathbb{N} \rightarrow \mathbb{N}$ με τιμές $f(n) = 2n$ και $g(2n) = n$, $g(2n+1) = 2n+1$.

Προφανώς $(g \circ f)(n) = g(2n) = n$, $g \circ f = 1_{\mathbb{N}}$. Όμως $(f \circ g)(2n+1) = f(2n+1) = 2(2n+1)$, δηλαδή $f \circ g \neq 1_{\mathbb{N}}$.

Πρόταση 2. Αν η συνάρτηση $f : A \rightarrow B$ αντιστρέφεται, έχει μια μόνο αντίστροφη συνάρτηση $g : B \rightarrow A$. Γράφουμε τότε $g = f^{-1}$.

Απόδειξη. Έστω ότι η f έχει δύο αντίστροφες συναρτήσεις $g, h : B \rightarrow A$. Τότε

$$g \circ f = 1_A = h \circ f, \quad f \circ g = 1_B = f \circ h.$$

Συνεπώς

$$h = h \circ 1_B = h \circ (f \circ g) = (h \circ f) \circ g = 1_A \circ g = g \quad \square$$

Πρόταση 3. Αν οι συναρτήσεις $g : A \rightarrow B$, $f : B \rightarrow \Gamma$ αντιστρέφονται, αντιστρέφεται και η συνάρτηση $f \circ g : A \rightarrow \Gamma$ και μάλιστα $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Απόδειξη. Έχουμε

$$\begin{aligned} (f \circ g) \circ (g^{-1} \circ f^{-1}) &= ((f \circ g) \circ g^{-1}) \circ f^{-1} = (f \circ (g \circ g^{-1})) \circ f^{-1} \\ &= (f \circ 1_B) \circ f^{-1} = f \circ f^{-1} = 1_\Gamma \end{aligned}$$

$$\begin{aligned} (g^{-1} \circ f^{-1}) \circ (f \circ g) &= g^{-1} \circ (f^{-1} \circ (f \circ g)) = g^{-1} \circ ((f^{-1} \circ f) \circ g) \text{ και} \\ &= g^{-1} \circ (1_B \circ g) = g^{-1} \circ g = 1_A \end{aligned}$$

άρα $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. □

Θεώρημα 1(αντιστροφής). Η συνάρτηση $f : A \rightarrow B$ αντιστρέφεται τότε και μόνο, όταν είναι αμφιμονοσήμαντη και επί.

Απόδειξη. Έστω ότι η f αντιστρέφεται. Υπάρχει τότε μια συνάρτηση $g : B \rightarrow A$ τέτοια, ώστε $g \circ f = 1_A$, $f \circ g = 1_B$ (1). Έστω ότι $f(x) = f(y)$ για $x, y \in A$. Τότε $(g \circ f)(x) = g(f(x)) = g(f(y)) = g \circ f(y)$, οπότε από την πρώτη των (1) παίρνουμε $1_A(x) = 1_A(y)$ ή $x = y$. Συνεπώς η f είναι αμφιμονοσήμαντη. Αν $\beta \in B$, έχουμε $f(g(\beta)) = (f \circ g)(\beta) = 1_B(\beta) = \beta$, δηλαδή το β είναι τιμή της f (στο $g(\beta)$), πράγμα που σημαίνει ότι η f είναι επί του B .

Αντίστροφα, έστω ότι η f είναι αμφιμονοσήμαντη και επί του B . Κάθε $y \in B$ είναι τιμή ενός μόνον $x \in A$. Έστω g η συνάρτηση με πεδίο ορισμού B και πεδίο τιμών A και τιμή στο $y \in B$ το μοναδικό $x \in A$ με $f(x) = y$. Έχουμε $g(y) = x$ ή $g(f(x)) = x$ ή $g \circ f = 1_A$. Ακόμη $f(g(y)) = y$ ή $f \circ g(y) = y$ ή $f \circ g = 1_B$. Άρα η g είναι αντίστροφή της f . □

Πόρισμα 1. Αν η συνάρτηση $f : A \rightarrow B$ αντιστρέφεται,

$$f(x) = y \Leftrightarrow x = f^{-1}(y)$$

Γιατί $f^{-1} = g$ και $f(x) = y \Leftrightarrow x = g(y)$ □

Παράδειγμα 3. Έστω η συνάρτηση $f : \mathbb{R} \rightarrow \mathbb{R}$ με τιμή $f(x) = 2x - 1$. Δείξτε ότι αντιστρέφεται και βρείτε την αντίστροφή της.

Λύση. Η συνάρτηση f είναι αμφιμονοσήμαντη, γιατί $f(x) = f(y)$ συνεπάγεται $2x - 1 = 2y - 1$ ή $x = y$. Είναι επί του $\mathbb{R}$, γιατί κάθε $y \in \mathbb{R}$ είναι τιμή της f στο x με $2x - 1 = y$ ή $x = \frac{y+1}{2}$. Επειδή $f(x) = y \Leftrightarrow x = \frac{y+1}{2}$, έχουμε $f^{-1}(y) = \frac{y+1}{2}$ για κάθε $y \in \mathbb{R}$ ή $f^{-1}(x) = \frac{x+1}{2}$.

Πρόταση 4. Έστω A, B δύο σύνολα με n στοιχεία και μια συνάρτηση $f: A \rightarrow B$. Οι παρακάτω προτάσεις είναι ισοδύναμες:

- i) Η f είναι αμφιμονοσήμαντη.
- ii) Η f είναι επί.

Απόδειξη i) $\Rightarrow$ ii) Έστω $A = \{a_1, a_2, \dots, a_n\}$. Τότε $f(a_1), f(a_2), \dots, f(a_n)$ είναι διάφορα στοιχεία του B . Αφού το πλήθος τους είναι n , έχουμε $B = \{f(a_1), f(a_2), \dots, f(a_n)\} = f(A)$, δηλαδή η f είναι επί.

ii) $\Rightarrow$ i) Έστω $A = \{a_1, a_2, \dots, a_n\}$. Τότε $B = \{f(a_i); i = 1, 2, \dots, n\}$, συνεπώς $f(a_i) \neq f(a_j)$ για $i \neq j$, ισοδύναμα για $a_i \neq a_j$. Άρα η f είναι αμφιμονοσήμαντη. $\square$

Πόρισμα. Αν τα σύνολα A, B έχουν το ίδιο πλήθος στοιχείων, τότε μια συνάρτηση $f: A \rightarrow B$ αντιστρέφεται, αν είναι αμφιμονοσήμαντη ή επί του B .

Έστω μια συνάρτηση $f: A \rightarrow B$. Αν $S \subseteq A$, $T \subseteq B$, ορίζουμε την εικόνα $f(S)$ του S και την "αντίστροφη" εικόνα $f^{-1}(T)$ του T από τις σχέσεις:

$$f(S) = \{f(s); s \in S\}, \quad f^{-1}(T) = \{a \in A; f(a) \in T\}$$

Πρέπει να επισημάνουμε ότι η αντίστροφη εικόνα ενός υποσυνόλου T του πεδίου τιμών ορίζεται για όλες τις συναρτήσεις f είτε έχουν αντίστροφο είτε όχι. Αν η συνάρτηση f αντιστρέφεται, το $f^{-1}(\{y\})$ είναι της μορφής $\{x\}$.

Πρόταση 5. Έστω μια συνάρτηση $f: A \rightarrow B$ και $X, Y \subseteq A$. Ισχύουν

1. $X \subseteq Y \Rightarrow f(X) \subseteq f(Y)$
2. $f(X \cup Y) = f(X) \cup f(Y)$
3. $f(X \cap Y) \subseteq f(X) \cap f(Y)$

Οι αποδείξεις είναι απλές και παραλείπονται. $\square$

Πρόταση 6. Έστω μια συνάρτηση $f: A \rightarrow B$, $S \subseteq A$ και $X, Y \subseteq B$. Τότε

1. $f(f^{-1}(X)) \subseteq X$.
2. $f^{-1}(f(S)) \supseteq S$.
3. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.

$$4. f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y).$$

Οι αποδείξεις είναι εύκολες και προτείνονται σαν ασκήσεις. $\square$

3. ΣΧΕΣΕΙΣ

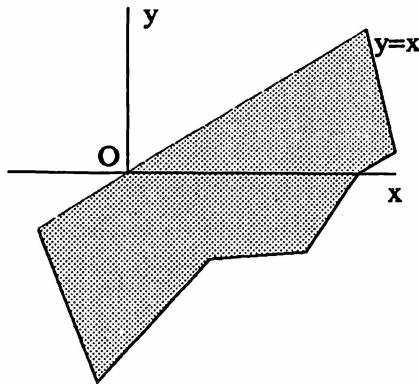
Έστω A, B δύο σύνολα. Κάθε υποσύνολο R του $A \times B$ λέγεται **διμελής σχέση** από το A στο B ή απλά **σχέση** από το A στο B . Μια διμελής σχέση από το A στο A λέγεται **σχέση** επί του A .

Αν $(a, \beta) \in R$, γράφουμε $aR\beta$ και διαβάζουμε "το a πληροί τη σχέση R με το β ".

Παράδειγμα 1. Έστω A ένα σύνολο $\neq \emptyset$ και $R = \{(x, x); x \in A\}$. Το R είναι υποσύνολο του $A \times A$, συνεπώς είναι μια σχέση επί του A . Προφανώς $(x, y) \in R$ τότε και μόνο, όταν $x = y$. Συνεπώς R είναι η σχέση ισότητας στο A .

Παράδειγμα 2. Έστω $A = \{2, 3, 4, 6\} \subseteq \mathbb{N}$ και $R = \{(2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}$, ένα υποσύνολο του $A \times A$. Είναι μια σχέση επί του A . Προφανώς $(x, y) \in R$ τότε και μόνο, όταν " x διαιρεί το y στο $\mathbb{N}$ ", συμβολικά x/y .

Παράδειγμα 3. Έστω η ευθεία $y = x$ στο επίπεδο $\mathbb{R} \times \mathbb{R}$ δύο αξόνων Ox, Oy , η διχοτόμος της γωνίας xOy . Το γραμμοσκιασμένο ημιεπίπεδο E είναι υποσύνολο του $\mathbb{R} \times \mathbb{R}$, συνεπώς είναι μια σχέση επί του $\mathbb{R}$. Προφανώς $(x, y) \in E$ τότε και μόνο, όταν $x \geq y$. Συνεπώς το ημιεπίπεδο E είναι η σχέση "διάταξης" των πραγματικών αριθμών.



Από τα παραπάνω παραδείγματα φαίνεται η γενικότητα της έννοιας της σχέσης επί ενός συνόλου, αφού με κατάλληλη εκλογή αυτού και της σχέσης παίρνουμε ως μερικές περιπτώσεις τις γνωστές μας "σχέσεις" ισότητας, διάταξης και διαιρετότητας.

Παράδειγμα 4. Έστω A, B δύο σύνολα $\neq \emptyset$, $E = A \times B$. Το σύνολο των σχέσεων από το A στο B είναι $\mathcal{P}(E)$. Δύο σχέσεις είναι τα υποσύνολα $\emptyset, E$.

Ποιοτικές ιδιότητες σχέσης

Μια σχέση R επί του συνόλου A λέγεται:

αυτοπαθητική, αν xRx για κάθε $x \in A$

συμμετρική, αν $xRy \Rightarrow yRx$

μεταβατική, αν $xRy, yRz \Rightarrow xRz$

αντισυμμετρική, αν $xRy, yRx \Rightarrow x = y$.

4. ΣΧΕΣΗ ΙΣΟΔΥΝΑΜΙΑΣ

Μια σχέση επί ενός συνόλου A λέγεται σχέση **ισοδυναμίας**, αν είναι αυτοπαθητική, συμμετρική και μεταβατική. Συνήθως συμβολίζεται με το σύμβολο $\sim$. Συνεπώς

1. $x \sim x$,
2. $x \sim y \Rightarrow y \sim x$
3. $x \sim y, y \sim z \Rightarrow x \sim z$.

Παράδειγμα 1. Έστω μια συνάρτηση $f : A \rightarrow B$. Ορίζουμε τη σχέση R επί του A ως εξής: $xRy \Leftrightarrow f(x) = f(y)$. Η σχέση αυτή είναι σχέση ισοδυναμίας επί του A .

Πραγματικά

- (i) xRx , γιατί $f(x) = f(x)$
- (ii) $xRy \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow yRx$
- (iii) $xRy, yRz \Rightarrow f(x) = f(y), f(y) = f(z) \Rightarrow f(x) = f(z) \Rightarrow xRz$

Παράδειγμα 2. Θεωρούμε γνωστή τη διαίρεση των ακεραίων: Ο ακέραιος m διαιρεί τον ακέραιο a (συμβολικά m/a), αν υπάρχει ακέραιος β τέτοιος ώστε $a = m\beta$.

Έστω $\mathbb{Z}$ το σύνολο των ακεραίων και m ένας ακέραιος θετικός. Ορίζουμε μια σχέση R_m επί του $\mathbb{Z}$ θέτοντας

$$aR_m\beta \Leftrightarrow m/a - \beta$$

Η σχέση R_m είναι σχέση ισοδυναμίας επί του $\mathbb{Z}$, γιατί

- i) aR_ma , αφού $m/a - a = 0$.
- ii) Αν $aR_m\beta$, τότε $m/a - \beta, a - \beta = m \cdot \gamma$ με $\gamma \in \mathbb{Z}$, $\beta - a = m(-\gamma)$, δηλαδή βR_ma .
- iii) Αν $aR_m\beta, \beta R_m\gamma$, τότε $m/a - \beta, m/\beta - \gamma$, συνεπώς $a - \beta = ma, \beta - \gamma = mb$ με $a, b \in \mathbb{Z}$, οπότε $a - \gamma = (a - \beta) + (\beta - \gamma) = ma + mb = m(a + b)$, δηλαδή $aR_m\gamma$.

Κλάσεις μιας σχέσης ισοδυναμίας.

Έστω E ένα σύνολο και $\sim$ μια σχέση ισοδυναμίας επί του E .

Ορισμός 1. Κλάση ενός στοιχείου $a \in E$ ως προς τη σχέση $\sim$ λέγεται το σύνολο

$$C_a = \{x \in E; x \sim a\}.$$

Επειδή $a \sim a$, η κλάση $C_a \neq \emptyset$.

Πρόταση 1. Αν $\beta \in C_a$, τότε $C_\beta = C_a$.

Απόδειξη. Έστω $x \in C_\beta$. Τότε $x \sim \beta$, $\beta \sim a$, συνεπώς $x \sim a$, $x \in C_a$, δηλαδή $C_\beta \subseteq C_a$. Έστω $y \in C_a$. Τότε $y \sim a$. Επειδή $\beta \sim a$, είναι $a \sim \beta$, οπότε $y \sim \beta$, δηλαδή $y \in C_\beta$ ή $C_a \subseteq C_\beta$. Άρα $C_\beta = C_a$. $\square$

Θεώρημα 1. Για οποιαδήποτε $a, \beta \in E$,

$$C_a \cap C_\beta = \emptyset \quad \text{ή} \quad C_a = C_\beta$$

Απόδειξη. Έστω $C_a \cap C_\beta \neq \emptyset$. Υπάρχει $\xi \in C_a \cap C_\beta$. Τότε $C_\xi = C_a$, $C_\xi = C_\beta$, άρα $C_a = C_\beta$. $\square$

Πόρισμα. Ένα οποιοδήποτε στοιχείο ανήκει σε μια μόνο κλάση. Κάθε κλάση ορίζεται από ένα στοιχείο της.

Γι' αυτό κάθε στοιχείο μιας κλάσης λέγεται αντιπρόσωπος αυτής.

Ορισμός 2. Διαμέριση ενός συνόλου E λέγεται μια οικογένεια υποσυνόλων $(A_i)_{i \in I}$ με τις ιδιότητες:

1. $A_i \neq \emptyset$
2. $A_i \cap A_j = \emptyset$ για $i \neq j$
3. $\cup_{i \in I} A_i = E$

Αν $\sim$ είναι μια σχέση ισοδυναμίας επί του συνόλου E , το σύνολο των διαφόρων κλάσεων C_a αποτελεί μια διαμέριση του E . Ισχύει και το αντίστροφο:

Πρόταση 2. Μια διαμέριση $(A_i)_{i \in I}$ του συνόλου E ορίζει μια μόνο σχέση ισοδυναμίας $\sim$ με κλάσεις τα σύνολα A_i .

Απόδειξη. Η σχέση $a \sim b \Leftrightarrow a, b \in A_j$, είναι σχέση ισοδυναμίας με κλάσεις τα σύνολα $A_i (i \in I)$. $\square$

Σύνολο πηλίκο

Ορισμός 3. Έστω μια σχέση ισοδυναμίας επί του συνόλου E . Το σύνολο των κλάσεων ως προς τη σχέση αυτή λέγεται σύνολο πηλίκο του E

με τη σχέση $\sim$ και συμβολίζεται με $E/\sim$. Συνεπώς

$$E/\sim = \{C_a; a \in E\}.$$

Παράδειγμα 3. Έστω $E = \mathbb{R}$ και η συνάρτηση $f : \mathbb{R} \rightarrow \mathbb{R}$ με τιμή $f(x) = x^2$. Ορίζουμε $x \sim y \Leftrightarrow f(x) = f(y)$. Η σχέση $\sim$ είναι σχέση ισοδυναμίας (βλ. παράδ.1). Βρίσκουμε την κλάση του $a \in E$. Είναι $x \sim a$ τότε και μόνο, όταν $x^2 = a^2$ ή $x = \pm a$. Συνεπώς η κλάση του a είναι $C_a = \{a, -a\}$ και το σύνολο πηλίκο $E/\sim$ είναι οι κλάσεις $C_0 = \{0\}$, $C_a = \{a, -a\}$ $a > 0$, δηλαδή $E/\sim = \{C_a; a \geq 0\}$.

Παράδειγμα 4. Έστω το σύνολο $\mathbb{Z}$ των ακεραίων, A το σύνολο των αρτίων και B το σύνολο των περιττών ακεραίων. Προφανώς $A \cap B = \emptyset$ και $A \cup B = \mathbb{Z}$. Συνεπώς $\{A, B\}$ είναι μια διαμέριση του $\mathbb{Z}$ και ορίζει μια σχέση ισοδυναμίας $\sim$ επί του $\mathbb{Z}$. Το σύνολο πηλίκο είναι $\mathbb{Z}/\sim = \{A, B\}$. Προφανώς, αν $a, \beta \in A$ ή $a, \beta \in B$, ο αριθμός $2/a - \beta$. Συνεπώς $a \sim \beta \Leftrightarrow 2/a - \beta$. Προφανώς A είναι η κλάση του μηδέν και B είναι η κλάση του 1.

Παράδειγμα 5. Έστω $\mathbb{Z}$ το σύνολο των ακεραίων και m ένας φυσικός αριθμός. Θεωρούμε τη σχέση $\sim$ (του παραδ.2) που ορίζεται ως εξής

$$a \sim \beta \Leftrightarrow m/\beta - a$$

Έχουμε τις κλάσεις:

$$C_0 = \{x \in \mathbb{Z}; x \sim 0\} = \{x \in \mathbb{Z}; m/x\} = \{am; a \in \mathbb{Z}\}$$

$$C_1 = \{x \in \mathbb{Z}; x \sim 1\} = \{x \in \mathbb{Z}; m/x - 1\} = \{am + 1; a \in \mathbb{Z}\}$$

$$\dots = \dots$$

$$C_{m-1} = \{x \in \mathbb{Z}; x \sim m-1\} = \{am + (m-1); a \in \mathbb{Z}\}.$$

Οι κλάσεις αυτές γράφονται $C_v = \{am + v; a \in \mathbb{Z}\}$ με $v = 0, 1, 2, \dots, m-1$. Είναι διάφορες ανά δύο, γιατί, αν $0 \leq v_1 < v_2 \leq m-1$, έχουμε $0 < v_2 - v_1 < m-1$, δηλαδή ο m δεν διαιρεί τη διαφορά $v_2 - v_1$ και $C_{v_1} \neq C_{v_2}$. Κάθε ακεραίος β ανήκει σε μια κλάση C_v , γιατί κάνοντας τη διαίρεση του β με τον m έχουμε $\beta = am + v$ με $0 \leq v \leq m-1$. Άρα οι κλάσεις είναι C_v με $v = 0, 1, 2, \dots, m-1$. Το σύνολο πηλίκο $\mathbb{Z}/\sim$ είναι $\{C_0, C_1, \dots, C_{m-1}\}$.

Συμβολισμοί, ορολογία

Αν $m/a - \beta$, αντί $a \sim \beta$ γράφουμε $a \equiv \beta \pmod{m}$. Η κλάση C_a συμβολίζεται με $\bar{a}$. Έτσι

$$\bar{0} = \{am; a \in \mathbb{Z}\}$$

$$\bar{1} = \{am + 1; a \in \mathbb{Z}\}$$

.....

$$\overline{m-1} = \{am + (m-1); a \in \mathbb{Z}\}$$

Το σύνολο ηλίκο $\mathbb{Z}/\sim$ συμβολίζεται με $\mathbb{Z}_m$. Άρα

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

Οι κλάσεις $\bar{0}, \bar{1}, \dots, \overline{m-1}$ λέγονται **ακέραιοι modulo m**. Ο ακέραιος $\bar{a}$ modulo m (ως προς μέτρο m) ή η κλάση του ακεραίου a modulo m είναι το σύνολο των ακεραίων, οι οποίοι διαιρούμενοι με το m αφήνουν το ίδιο υπόλοιπο. Π.χ. οι ακέραιοι 50, 122 ανήκουν στην κλάση $\bar{2}$ modulo 12, γιατί διαιρούμενοι με 12 δίνουν υπόλοιπο 2.

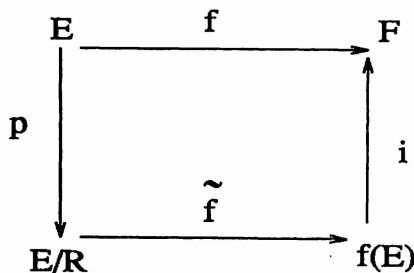
Ανάλυση συνάρτησης

Έστω μια συνάρτηση $f: E \rightarrow F$ και R η σχέση ισοδυναμίας $xRy \Leftrightarrow f(x) = f(y)$. Θεωρούμε τη συνάρτηση

$$\tilde{f}: E/R \rightarrow f(E), \quad X \mapsto \tilde{f}(X) = f(x) \text{ με } x \in X.$$

Η $\tilde{f}$ είναι, προφανώς, επί του $f(E)$ και επιπλέον αμφιμονοσήμαντη, γιατί, αν $\tilde{f}(X) = \tilde{f}(Y)$, έχουμε $f(x) = f(y)$ με $x \in X, y \in Y$, συνεπώς xRy , δηλαδή $X = Y$.

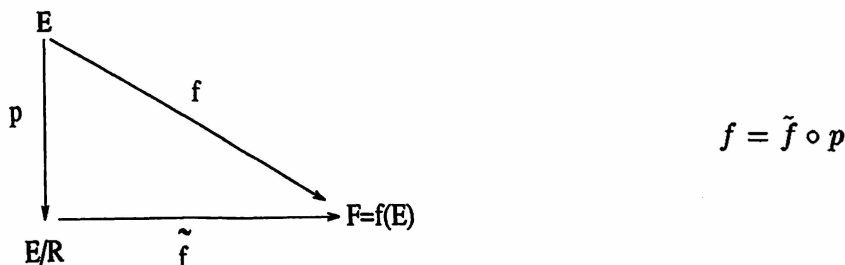
Έστω η συνάρτηση $P: E \rightarrow E/R$ με τιμή $P(x) =$ την κλάση του x ως προς τη σχέση ισοδυναμίας R , και i ο περιορισμός της ταυτοτικής του F στο $f(E)$. Το παρακάτω διάγραμμα είναι αντιμεταθετικό,



$$f = i \circ \tilde{f} \circ p$$

Η παράσταση αυτή της f σαν σύνθεση συναρτήσεων λέγεται **ανάλυση** αυτής (σε γινόμενο, αν καλέσουμε, όπως συνηθίζεται, τη σύνθεση $\phi \circ \sigma$ γινόμενο των ϕ, σ).

Αν η f είναι επί του F , τότε το παραπάνω διάγραμμα απλουστεύεται



5. ΣΧΕΣΗ ΔΙΑΤΑΞΗΣ

Έστω E ένα σύνολο $\neq \emptyset$. Μια σχέση R επί του E λέγεται **σχέση διάταξης**, αν είναι αυτοπαθητική, αντισυμμετρική και μεταβατική. Μια σχέση διάταξης συμβολίζεται με το σύμβολο " $\leq$ ". Συνεπώς " $\leq$ " είναι σχέση διάταξης επί του E , αν για όλα τα $x, y, z \in E$:

1. $x \leq x$
2. $x \leq y, y \leq x \Rightarrow x = y$
3. $x \leq y, y \leq z \Rightarrow x \leq z$

Γράφουμε $x < y$, αν $x \leq y$ και $x \neq y$.

Ένα σύνολο E λέγεται **διατεταγμένο**, αν έχει οριστεί μια σχέση διάταξης $\leq$ επί του E . Στην περίπτωση αυτή γράφουμε $(E, \leq)$.

Μια σχέση διάταξης $\leq$ επί του E λέγεται **ολική**, αν ισχύει η ιδιότητα

$$\forall x, y \in E \text{ ισχύει } x \leq y \text{ ή } y \leq x.$$

Επειδή η ιδιότητα αυτή ισοδυναμεί με $x < y$ ή $x = y$ ή $y < x$ λέγεται ιδιότητα τριχοτόμησης.

Ένα σύνολο E λέγεται **ολικά διατεταγμένο**, αν υπάρχει μια σχέση ολικής διάταξης επ' αυτού. Μια σχέση διάταξης που δεν είναι ολική θα λέγεται **σχέση μερικής διάταξης** ή απλά διάταξης.

Αν για τα στοιχεία x, y ισχύει η ιδιότητα της τριχοτόμησης, είναι δηλαδή $x \leq y$ ή $x \geq y$, θα λέγονται **συγκρίσιμα**. Ένα υποσύνολο του E , που είναι ολικά διατεταγμένο, λέγεται **αλυσίδα**.

Έστω $(E, \leq), (E', \leq')$ δύο διατεταγμένα σύνολα και μια συνάρτηση $f : E \rightarrow E'$. Η συνάρτηση f λέγεται

αύξουσα: Αν $x \leq y$ ($x, y \in E$) συνεπάγεται $f(x) \leq f(y)$

φθίνουσα: Αν $x \leq y$ ($x, y \in E$) συνεπάγεται $f(x) \geq f(y)$

γνήσια αύξουσα: Αν $x < y$ ($x, y \in E$) συνεπάγεται $f(x) < f(y)$

γνήσια φθίνουσα: Αν $x < y$ ($x, y \in E$) συνεπάγεται $f(x) > f(y)$

Παράδειγμα 1. Έστω E ένα σύνολο και $\mathcal{P}(E)$ το σύνολο των υποσυνόλων του. Η σχέση R επί του $\mathcal{P}(E)$, που ορίζεται από την ισότητα $R = \{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E); A \subseteq B\}$, δηλ. $ARB \Leftrightarrow A \subseteq B$ είναι μια σχέση μερικής διάταξης επί του $\mathcal{P}(E)$.

Πραγματικά, είναι :

1. αυτοπαθητική, αφού $A \subseteq A$

2. αντισυμμετρική, αφού $A \subseteq B, B \subseteq A \Rightarrow A = B$

3. μεταβατική, αφού $A \subseteq B, B \subseteq \Gamma \Rightarrow A \subseteq \Gamma$.

Η σχέση αυτή λέγεται σχέση του "περιέχεται" και δεν είναι ολική, γιατί για δύο ξένα π.χ. υποσύνολα A, B του E δεν ισχύει $A \subseteq B$ ή $B \subseteq A$.

Παράδειγμα 2. Στο σύνολο των φυσικών αριθμών $\mathbb{N}$ ορίζουμε τη σχέση R θέτοντας $xRy \Leftrightarrow x/y$ (στο $\mathbb{N}$), δηλαδή xRy τότε και μόνο, όταν υπάρχει $a \in \mathbb{N}$ με $y = ax$. Η σχέση αυτή είναι μια σχέση μερικής διάταξης, η οποία λέγεται σχέση διαιρετότητας επί του $\mathbb{N}$.

Πραγματικά, x/x , αφού $x = 1 \cdot x$, αν x/y και y/x , τότε $y = ax$ και $x = \beta y$ με $a, \beta \in \mathbb{N}$, οπότε $y = a\beta y$ ή $a\beta = 1$ ή $a = \beta = 1$, δηλαδή $x = y$. Τέλος, αν x/y , y/z , τότε x/z , γιατί $y = ax$ και $z = \beta y$, δηλαδή $z = \beta(ax) = (\beta a)x$. Επειδή $2 \nmid 3$ και $3 \nmid 2$, η σχέση διαιρετότητας $"/$ είναι σχέση μερικής διάταξης επί του $\mathbb{N}$.

Παράδειγμα 3. Έστω $\mathbb{N}$ το σύνολο των φυσικών αριθμών με σχέση διάταξης τη σχέση διαιρετότητας. Το σύνολο $A = \{1, 3, 3^2, \dots, 3^n, \dots\}$ είναι μια αλυσίδα, γιατί $3^m/3^{m+1}$ και άρα $3^m \leq 3^{m+1}$ ($m = 0, 1, 2, \dots$).

Διαστήματα

Έστω $(E, \leq)$ ένα διατεταγμένο σύνολο και $a, \beta \in E$. Ορίζουμε τα διαστήματα $[a, \beta], (a, \beta), [a, \beta), (a, \beta]$ ως εξής

$$[a, \beta] = \{x \in E; a \leq x \text{ και } x \leq \beta\}$$

$$(a, \beta) = \{x \in E; a < x \text{ και } x < \beta\}$$

$$[a, \beta) = \{x \in E; a \leq x \text{ και } x < \beta\}$$

$$(a, \beta] = \{x \in E; a < x \text{ και } x \leq \beta\}$$

Παράδειγμα 4. 'Εστω $A = \{a, \beta, \gamma\}$, $E = \mathcal{P}(A)$ και η σχέση διάταξης $X \leq Y \Leftrightarrow X \subseteq Y$ επί του E . 'Εχουμε

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{\beta\}, \{\gamma\}, \{a, \beta\}, \{a, \gamma\}, \{\beta, \gamma\}, \{a, \beta, \gamma\}\}$$

$$[\{a\}, \{a, \beta, \gamma\}] = \{\{a\}, \{a, \beta\}, \{a, \gamma\}, \{a, \beta, \gamma\}\}$$

$$(\{a\}, \{a, \beta, \gamma\}) = \{\{a, \beta\}, \{a, \gamma\}\}.$$

Παράδειγμα 5. 'Εστω $A = \{2, 3, 4, 6, 8\}$ και η σχέση διάταξης $x \leq y \Leftrightarrow x/y$ (στο $\mathbb{N}$). 'Εχουμε

$$[2, 6] = \{2, 6\}, [2, 8] = \{2, 4, 8\}, [3, 8] = \emptyset$$

Διάγραμμα Hasse

'Εστω E ένα διατεταγμένο σύνολο με τη σχέση $\leq$ και $x, y \in E$ με $x < y$. Λέμε ότι το y είναι επόμενο του x , αν

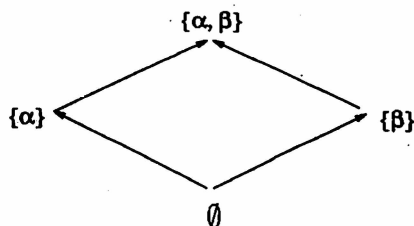
$$x \leq z \leq y \Rightarrow z = x \text{ ή } z = y$$

αν δηλαδή $[x, y] = \{x, y\}$. 'Όταν το y είναι επόμενο του x , γράφουμε ένα βέλος με αρχή το x και τέλος το y

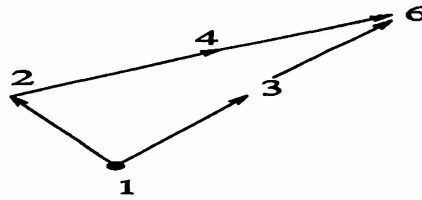


Αν δύο στοιχεία a, β δεν είναι συγκρίσιμα, δεν θέτουμε μεταξύ αυτών βέλος. Για κάθε διατεταγμένο σύνολο $E = \{a_1, a_2, \dots, a_n\}$ προκύπτει ένα διάγραμμα, που λέγεται διάγραμμα Hasse.

Παράδειγμα 6. 'Εστω $A = \{a, \beta\}$, $E = \mathcal{P}(A) = \{\emptyset, \{a\}, \{\beta\}, A\}$ και $\leq$ η σχέση του "περιέχεται": $X \leq Y \Leftrightarrow X \subseteq Y$. Το ζεύγος $(E, \leq)$ παριστάνεται από το παρακάτω διάγραμμα Hasse



Παράδειγμα 7. 'Εστω $E = \{1, 2, 3, 4, 6\}$ και η σχέση $x \leq y \Leftrightarrow x/y$ (στο $\mathbb{N}$). Στο ζεύγος $(E, \leq)$ αντιστοιχεί το παρακάτω διάγραμμα Hasse

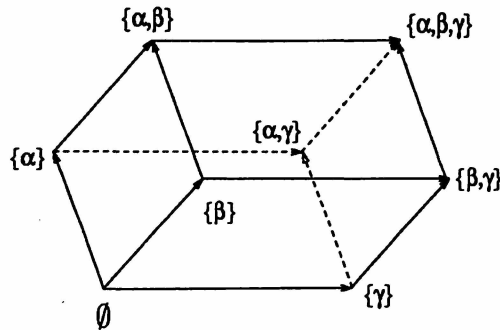


Παράδειγμα 8. Έστω $E = \{2, 4, 8, 16\}$ και η σχέση $x \leq y \Leftrightarrow x/y$ (στο $\mathbb{N}$). Το αντίστοιχο διάγραμμα Hasse είναι

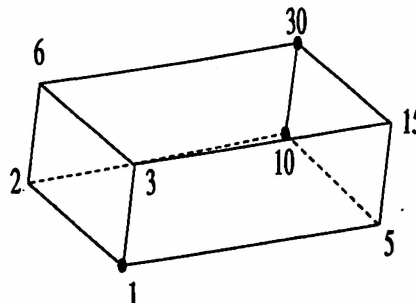


Η σχέση x/y είναι σχέση ολικής διάταξης επί του E .

Παράδειγμα 9. Έστω $A = \{a, \beta, \gamma\}$ και $\mathcal{P}(A)$ το σύνολο των υποσυνόλων του με σχέση διάταξης $X \leq Y \Leftrightarrow X \subseteq Y$. Το αντίστοιχο διάγραμμα Hasse είναι



Παράδειγμα 10. Έστω $E_{30} = \{x \in \mathbb{N}; x/30\}$ και η σχέση διάταξης $x \leq y \Leftrightarrow x/y$. Έχουμε $E = \{1, 2, 3, 6, 5, 10, 15, 30\}$. Το διάγραμμα Hasse στην περίπτωση αυτή είναι



Μεταξύ των διατεταγμένων συνόλων των παραδειγμάτων 9 και 10 υπάρχει μια αμφιμονοσήμαντη συνάρτηση $f: E_{30} \rightarrow \mathcal{P}(A)$

$$\begin{aligned} 1 &\rightarrow \emptyset \\ 2 &\rightarrow \{a\} \\ 3 &\rightarrow \{\beta\} \\ 5 &\rightarrow \{\gamma\} \\ 6 &\rightarrow \{a, \beta\} \\ 10 &\rightarrow \{a, \gamma\} \\ 15 &\rightarrow \{\beta, \gamma\} \\ 30 &\rightarrow \{a, \beta, \gamma\} \end{aligned}$$

τέτοια, ώστε $x \leq y \Leftrightarrow f(x) \leq f(y)$. Μια τέτοια συνάρτηση λέγεται **ισομορφισμός** των ζευγών $(E_{30}, /)$ και $(\mathcal{P}(A), \leq)$ ή των διατεταγμένων συνόλων $E_{30}, \mathcal{P}(A)$ με τις θεωρούμενες σχέσεις διατάξεων.

Γενικά, αν E, E' είναι δύο διατεταγμένα σύνολα και $\leq, \leq'$ οι σχέσεις διάταξης επ' αυτών, μια συνάρτηση $f: E \rightarrow E'$ λέγεται **ισομορφισμός** των διατεταγμένων συνόλων E, E' ως προς τις διατάξεις $\leq, \leq'$, όταν

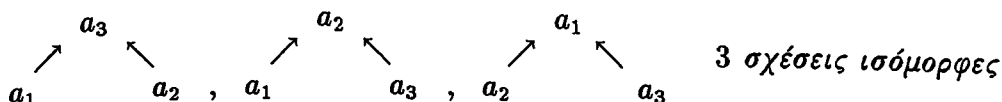
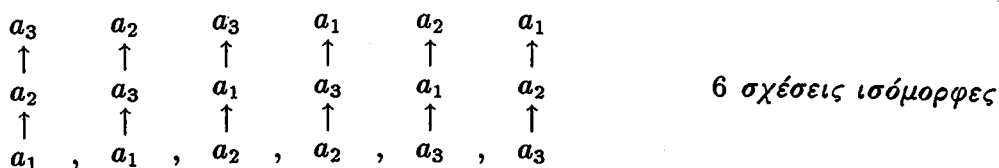
$$x \leq y \Leftrightarrow f(x) \leq' f(y)$$

και αντι-ισομορφισμός, όταν

$$x \leq y \Leftrightarrow f(x) \geq' f(y)$$

Οι σχέσεις $\leq, \leq'$ λέγονται τότε ισόμορφες αντίστοιχα αντι-ισόμορφες.

Παράδειγμα 11. Οι σχέσεις διάταξης επί ενός συνόλου A με τρία στοιχεία, $A = \{a, \beta, \gamma\}$ είναι:



$$\begin{array}{cccccc} a_3 & a_2 & a_1 & a_3 & a_1 & a_2 \\ | & | & | & | & | & | \\ a_1 & a_2 & a_3 & a_2 & a_3 & a_1 \end{array} \quad 6 \text{ σχέσεις ισόμορφες}$$

a_1, a_2, a_3 μία σχέση, αντίστοιχη της ισότητας.

Παρατήρηση. Αν Δ_n είναι το πλήθος των σχέσεων διατάξεων επί ενός συνόλου με n στοιχεία, γνωρίζουμε ότι

$$\Delta_2 = 3, \Delta_3 = 19, \Delta_4 = 219, \Delta_7 = 6.129.859 \quad (!)$$

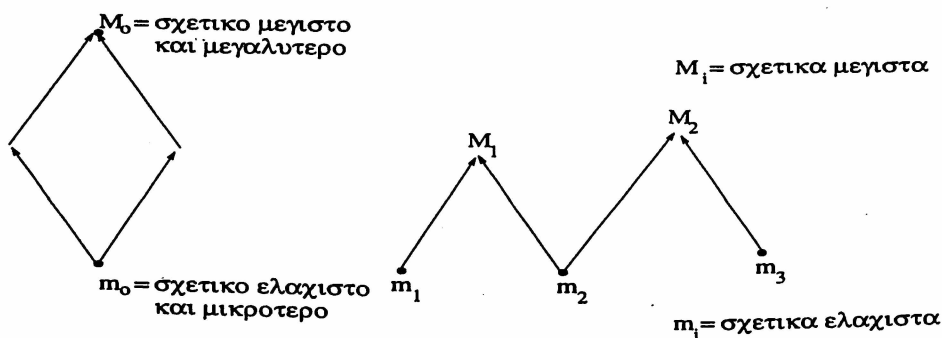
Το πρόβλημα υπολογισμού του Δ_n για τυχόν n είναι ένα ανοικτό πρόβλημα.

Ειδικά στοιχεία διατεταγμένου συνόλου

Έστω E ένα διατεταγμένο σύνολο με τη σχέση $\leq$. Ένα στοιχείο a λέγεται **μικρότερο** στοιχείο του E ή **μηδέν** του E , αν $a \in E$ και για κάθε $x \in E, a \leq x$. Το a θα λέγεται **μεγαλύτερο** στοιχείο του E ή **μονάδα** του E , αν $a \in E$ και για κάθε $x \in E, a \geq x$.

Ένα στοιχείο M του E λέγεται **σχετικά μέγιστο** (maximal) στοιχείο, αν δεν υπάρχει $a \in E$ με $a > M$. Συνεπώς το στοιχείο M είναι σχετικό μέγιστο στοιχείο του E , αν $M \in E$ και για κάθε $a \in E$ διάφορο του $M, a \not\geq M$. Αυτό σημαίνει ότι ή το a δεν συγκρίνεται με το M ή, αν συγκρίνεται, $a \leq M$.

Ένα στοιχείο m λέγεται **σχετικά ελάχιστο** (minimal) στοιχείο του E , αν δεν υπάρχει $a \in E$ με $a < m$. Στα παρακάτω διαγράμματα Hasse σημειώνονται τέτοια στοιχεία



Ένα στοιχείο μη συγκρίσιμο με κάποιο άλλο είναι σχετικό μέγιστο ή ελάχιστο.

Θεώρημα 1. Κάθε πεπερασμένο διατεταγμένο σύνολο E έχει τουλάχιστον ένα σχετικό μέγιστο και ένα σχετικό ελάχιστο στοιχείο. Αν υπάρχει ένα μόνο σχετικό μέγιστο(ή ελάχιστο), αυτό είναι το μεγαλύτερο(ή μικρότερο) στοιχείο του E .

Απόδειξη. Έστω $a \in E$. Αν το a_1 δεν είναι σχετικά μέγιστο, υπάρχει $a_2 \in E$ τέτοιο, ώστε $a_1 < a_2$. Αν το a_2 δεν είναι σχετικά μέγιστο, υπάρχει a_3 με $a_2 < a_3$, οπότε $a_1 < a_2 < a_3$. Με την υπόθεση ότι δεν υπάρχει σχετικά μέγιστο στοιχείο βρίσκουμε στοιχεία $a_4, \dots, a_n, \dots$ τέτοια, ώστε $a_1 < a_2 < a_3 < a_4 < \dots < a_n < \dots$. Αυτό είναι άτοπο, γιατί το E είναι πεπερασμένο.

Με τον ίδιο τρόπο αποδεικνύουμε ότι υπάρχει σχετικά ελάχιστο στοιχείο. Έστω M το μοναδικό σχετικά μέγιστο στοιχείο του E . Κάθε $a_1 \in E$ διάφορο του M δεν είναι σχετικά μέγιστο. Συνεπώς υπάρχει $a_2 \in E$ με $a_1 < a_2$. Συνεχίζοντας βρίσκουμε μια αλυσίδα $a_1 < a_2 < \dots < a_n$. Το a_n θα είναι σχετικά μέγιστο στοιχείο, συνεπώς $a_n = M$ και $a_1 < M$. Άρα το M είναι μεγαλύτερο στοιχείο του E . Όμοια προκύπτει ότι το μοναδικό σχετικά ελάχιστο στοιχείο είναι το μικρότερο στοιχείο. $\square$

Ανώτερο, κατώτερο πέρασ

Έστω A υποσύνολο ενός διατεταγμένου συνόλου E . Το στοιχείο S του E λέγεται **άνω φράγμα** του A , αν για κάθε $a \in A$, $a \leq S$. Το S λέγεται **κάτω φράγμα** του A , αν για κάθε $a \in A$, $a \geq S$. Ένα στοιχείο S του E λέγεται **άνω πέρασ** του A , αν είναι το μικρότερο στοιχείο του συνόλου των άνω φραγμάτων και συμβολίζεται με $\sup A$. Ένα στοιχείο I του E λέγεται **κάτω πέρασ** του A , αν είναι το μεγαλύτερο στοιχείο του συνόλου των κάτω φραγμάτων και συμβολίζεται με $\inf A$.

Παράδειγμα 12. Έστω $E = \{1, 2, 3, 4, 5, 6, 8, 9, 10\}$ και η σχέση διάταξης $x \leq y \Leftrightarrow x/y$ (στο $\mathbb{N}$). Αν $A = \{1, 2, 4, 8\}$, έχουμε $\inf A = 1$ και $\sup A = 8$. Αν $A = \{1, 2, 3, 4\}$, τότε $\inf A = 1$ και δεν υπάρχει το $\sup A$. Αν $A = \{a\}$, τότε $\inf A = a = \sup A$.

Θεώρημα 2. Αν υπάρχει το $\sup A$ ή το $\inf A$, είναι μοναδικό.

Απόδειξη. Είναι ανάλογη της απόδειξης του Θεωρ.1. $\square$

6. ΕΣΩΤΕΡΙΚΟΙ ΚΑΙ ΕΞΩΤΕΡΙΚΟΙ ΝΟΜΟΙ

Έστω E ένα σύνολο $\neq \emptyset$. Μια συνάρτηση $T : E \times E \rightarrow E$ λέγεται **διμελούς εσωτερικός νόμος** ή απλά **εσωτερικός νόμος** επί του E . Η εικόνα ενός στοιχείου $z = (x, y) \in E \times E$ έχουμε συμφωνήσει να συμβολίζεται με $T(z) = T((x, y))$. Θα παρεκκλίνουμε από αυτή τη συμφωνία και θα ακολουθήσουμε το συμβολισμό που σε πολλές περιπτώσεις έχει χρησιμοποιηθεί. Αντί $T((x, y))$ γράφουμε απλούστερα xTy . Για ένα εσωτερικό νόμο χρησιμοποιούμε και τους συμβολισμούς $+$, $\cdot$, $*$, $\dots$. Το ζεύγος (E, T) λέγεται **δομή** ενός εσωτερικού νόμου. Ένα υποσύνολο A του E λέγεται **κλειστό** ως προς το νόμο T , αν για όλα τα $a, \beta \in A$

$$aT\beta \in A.$$

Μια συνάρτηση $f : E \rightarrow E$ λέγεται **μονομελούς εσωτερικός νόμος** επί του E . Έστω A ένα σύνολο $\neq \emptyset$. Μια συνάρτηση $f : A \times E \rightarrow E$ λέγεται **εξωτερικός νόμος** επί του E με **τελεστές** τα στοιχεία του A .

Μια τριάδα $(E, \mathcal{N}, \Omega)$, όπου το E ένα σύνολο $\neq \emptyset$, $\mathcal{N}$ ένα σύνολο εσωτερικών και εξωτερικών νόμων επί του E και Ω ένα σύνολο σχέσεων επί του E , λέγεται **αλγεβρική δομή** επί του E .

Παράδειγμα 1. Η πρόσθεση $+$ και ο πολλαπλασιασμός στα σύνολα $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$ είναι εσωτερικοί νόμοι: $(x, y) \mapsto x + y$, $(x, y) \mapsto x \cdot y$.

Παράδειγμα 2. Έστω $E = \mathcal{P}(A)$ το σύνολο των υποσυνόλων ενός συνόλου A . Οι συναρτήσεις $(X, Y) \mapsto X \cup Y$, $(X, Y) \mapsto X \cap Y$ είναι εσωτερικοί νόμοι επί του E .

Παράδειγμα 3. Η σύνθεση "ο" των συναρτήσεων $f : E \rightarrow E$ είναι ένας εσωτερικός νόμος επί του συνόλου E^E . Στο ζεύγος $(f, g) \in E \times E$ αντιστοιχίζεται η συνάρτηση $f \circ g$.

Παράδειγμα 4. Έστω E το σύνολο των πινάκων $A = \begin{pmatrix} a & \beta \\ \gamma & \delta \end{pmatrix}$ με $a, \beta, \gamma, \delta \in \mathbb{R}$. Η συνάρτηση $f : \mathbb{R} \times E \rightarrow E$ με τιμή $f((\lambda, A)) = \begin{pmatrix} \lambda a & \lambda \beta \\ \lambda \gamma & \lambda \delta \end{pmatrix}$ είναι εξωτερικός νόμος επί του E με τελεστές τα στοιχεία του $\mathbb{R}$. Ο νόμος αυτός συμβολίζεται με "." και γράφουμε $f((\lambda, A)) = \lambda \cdot A$. Έτσι

$$(\lambda, A) \mapsto \lambda \cdot A \quad \therefore \mathbb{R} \times E \rightarrow E$$

Παράδειγμα 5. Έστω ένα πεπερασμένο σύνολο $X \neq \emptyset$ και X^* το σύνολο των πεπερασμένων ακολουθιών $X = x_1 x_2 \dots x_n$ στοιχείων $x_i \in X$. Τα

στοιχεία του X λέγονται γράμματα και τα στοιχεία του X^* λέξεις. Ορίζουμε έναν εσωτερικό νόμο επί του X^* θέτοντας

$$x \circ y = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$$

Παραθέτουμε δηλαδή τα γράμματα των λέξεων x, y με τη σειρά τους και φτιάχνουμε τη λέξη $x \circ y$. Το ζεύγος $(X^*, \circ)$ είναι μια δομή εσωτερικού νόμου, η οποία λέγεται ελεύθερη δομή παραγόμενη από το σύνολο X .

Παράδειγμα 6. Η συνάρτηση $f : \mathcal{P}(E) \rightarrow \mathcal{P}(E)$, η οποία στο υποσύνολο A του E αντιστοιχεί το συμπλήρωμά του A' είναι μονομελής εσωτερικός νόμος.

Πίνακας εσωτερικού νόμου

Αν το σύνολο E έχει n στοιχεία, έστω $E = \{a_1, a_2, \dots, a_n\}$, ένας εσωτερικός νόμος "*" επί του E ορίζεται από τον "πίνακα του Πυθαγόρα"

*	a_1	a_2	$\dots$	a_j	$\dots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Στην τομή της i -γραμμής
και j -στήλης βρίσκεται
το στοιχείο $a_i * a_j$

Παράδειγμα 7. Έστω $A = \{a, \beta\}$ και $E = \mathcal{P}(A)$. Η δομή (E, Δ) , όπου Δ η συμμετρική διαφορά ορίζεται από τον παρακάτω πίνακα

Δ	$\emptyset$	X	Y	A
$\emptyset$	$\emptyset$	X	Y	A
X	X	$\emptyset$	A	Y
Y	Y	A	$\emptyset$	X
A	A	Y	X	$\emptyset$

$$X = \{a\}$$

$$Y = \{\beta\}$$

$$\text{Πραγματικά, } X \Delta \emptyset = (X - \emptyset) \cup (\emptyset - X) = X$$

$$X \Delta X = (X - X) \cup (X - X) = \emptyset$$

$$X \Delta Y = (X - Y) \cup (Y - X) = X \cup Y = A$$

$$X \Delta A = (X - A) \cup (A - X) = \emptyset \cup Y = Y \text{ κ.λ.π}$$

Παράδειγμα 8. Έστω $\mathbb{Z}_3$ το σύνολο των ακεραίων modulo 3 (§4, Παρ.5), $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Οι πίνακες

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

ορίζουν δύο εσωτερικούς νόμους επί του $\mathbb{Z}_3$. Η δομή $(\mathbb{Z}_3, \oplus, \odot)$ έχει ανάλογες ιδιότητες της δομής $(\mathbb{R}, +, \cdot)$ των πραγματικών αριθμών (που δεν αναφέρονται στη διάταξη επί του $\mathbb{R}$). Οι πίνακες κατασκευάστηκαν με τους κανόνες

$$\bar{x} \oplus \bar{y} = \overline{x+y} \quad , \quad \bar{x} \odot \bar{y} = \overline{x \cdot y}$$

Μια αρνητική ενδεχομένως σκέψη του αναγνώστη περί της χρησιμότητας και των εφαρμογών τέτοιων δομών θα ήταν εσφαλμένη. Μπορούμε π.χ. να χρησιμοποιήσουμε τη δομή $(\mathbb{Z}_3, \oplus, \odot)$ για ν' αποδείξουμε ότι η εξίσωση $x^2 + 3y^2 = 302$ δεν δέχεται ακέραιες λύσεις. Πραγματικά, ας υποθέσουμε ότι η εξίσωση έχει ακέραιες λύσεις x, y . Τότε $\overline{x^2 + 3y^2} = \overline{x^2} \oplus \overline{3y^2} = \overline{x^2} \oplus \bar{0} = \bar{x}^2 = \bar{2}$. Όμως $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$ και $\bar{2}^2 = \bar{1}$, δηλαδή για κάθε $\bar{x} \in \mathbb{Z}_3$, $\bar{x}^2 \neq \bar{2}$ (όπως φαίνεται και από τον πίνακα του νόμου $\odot$). Άρα η εξίσωση δεν δέχεται ακέραιες ρίζες.

Επέκταση εσωτερικού νόμου του E στο $\mathcal{P}(E)$

Έστω $*$ ένας εσωτερικός νόμος επί του E . Αν $A, B \subseteq E$ ορίζουμε

$$A * B = \{a * b; a \in A \text{ και } b \in B\}$$

Στην περίπτωση που το A είναι το μονοσύνολο $\{x\}$ γράφουμε $\{x\} * B = x * B$ και ανάλογα $A * \{y\} = A * y$.

Παράδειγμα 9. Αν $m \in \mathbb{Z}$, το σύνολο $m \cdot \mathbb{Z} = \{m \cdot a; a \in \mathbb{Z}\}$, είναι δηλαδή όλα τα πολλαπλάσια του m .

Ποιοτικές ιδιότητες εσωτερικού νόμου

Οι ιδιότητες ενός εσωτερικού νόμου $*$ επί του συνόλου E , που είναι χρήσιμες στις εφαρμογές, είναι οι εξής:

1. Αντιμεταθετική ιδιότητα: $a * \beta = \beta * a$ για όλα τα $a, \beta \in E$.

Η ένωση, η τομή και η συμμετρική διαφορά έχουν την αντιμεταθετική ιδιότητα.

Ο πολλαπλασιασμός των πινάκων δεν έχει την αντιμεταθετική ιδιότητα, π.χ.

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

2. Προσεταιριστική ιδιότητα: $a * (\beta * \gamma) = (a * \beta) * \gamma$ για όλα τα $a, \beta, \gamma \in E$.

Η ένωση, η τομή και η συμμετρική διαφορά στο σύνολο $\mathcal{P}(E)$ έχουν την προσεταιριστική ιδιότητα. Ο εσωτερικός νόμος $(m, n) \xrightarrow{T} m^n$ στο σύνολο των φυσικών αριθμών $\mathbb{N}$ δεν έχει την προσεταιριστική ιδιότητα, π.χ.

$$2T(3T2) = 2T(3^2) = 2^{3^2} = 2^9$$

$$(2T3)T2 = 2^3T2 = (2^3)^2 = 2^6 \neq 2^9.$$

Αν ο εσωτερικός νόμος $*$ είναι προσεταιριστικός, γράφουμε $a * \beta * \gamma$ αντί $a * (\beta * \gamma)$ ή $(a * \beta) * \gamma$, γιατί δεν έχει σημασία ποιό από τ' αποτελέσματα $a * \beta$, $\beta * \gamma$ θα υπολογιστεί πρώτο, πού δηλαδή θα τεθούν παρενθέσεις. Όταν ο νόμος $*$ είναι προσεταιριστικός, ορίζουμε τις δυνάμεις

$$a^1 = a, a^2 = a * a, a^3 = a * a^2, \dots, a^n = a * a^{n-1}$$

δηλαδή $a^n = a * a * \dots * a$ (n φορές).

Π.χ. η ένωση, η τομή, η συμμετρική διαφορά, στο σύνολο $\mathcal{P}(E)$ έχουν την προσεταιριστική ιδιότητα. Επίσης η σύνθεση συναρτήσεων και το γινόμενο των πινάκων, έχουν την προσεταιριστική ιδιότητα. Ο εσωτερικός νόμος $*$ επί του συνόλου των ρητών $\mathbb{Q}$ που ορίζεται από την ισότητα $x * y = \frac{x + y}{2}$ δεν είναι προσεταιριστικός, γιατί για $x \neq z$

$$x * (y * z) = x * \frac{y + z}{2} = \frac{2x + y + z}{4},$$

$$(x * y) * z = \frac{x + y}{2} * z = \frac{x + y + 2z}{4} \neq x * (y * z)$$

3. Ουδέτερο στοιχείο του νόμου $*$ επί του E

- $e \in E$ λέγεται **ουδέτερο αριστερά** του νόμου $*$, αν $e * a = a$ για κάθε $a \in E$
- $e \in E$ λέγεται **ουδέτερο δεξιά** του νόμου $*$, αν $a * e = a$ για κάθε $a \in E$

- $e \in E$ λέγεται **ουδέτερο** του νόμου $*$, αν είναι ουδέτερο αριστερά και δεξιά, αν δηλαδή

$$e * a = a * e = a$$

για κάθε $a \in E$.

Παράδειγμα 10. α) Ουδέτερο της τομής στο σύνολο $\mathcal{P}(E)$ είναι το ίδιο το E : $A \cap E = E \cap A = A$ για κάθε $A \subseteq E$.

β) Ουδέτερο της ένωσης στο σύνολο $\mathcal{P}(E)$ είναι το κενό σύνολο $\emptyset$: $A \cup \emptyset = \emptyset \cup A = A$.

γ) Ουδέτερο της σύνθεσης στο σύνολο E^E είναι η ταυτοτική συνάρτηση 1_E του E : $f \circ 1_E = 1_E \circ f = f$ για κάθε συνάρτηση $f: E \rightarrow E$.

δ) Ο εσωτερικός νόμος $*$ επί του $\mathbb{Z}$ που ορίζεται από την ισότητα $a * b = a + b - 3ab - 1$ δεν έχει ουδέτερο στοιχείο, γιατί $a * e = a$ τότε και μόνο, όταν $a + e - 3ae - 1 = a$ ή $(1 - 3a)e = 1$, που ισχύει μόνο για $a = 0 (e = 1)$.

Πρόταση 1. Αν ένας εσωτερικός νόμος $*$ επί του E έχει ουδέτερο στοιχείο, αυτό είναι μοναδικό.

Απόδειξη. Αν ο νόμος $*$ έχει δύο ουδέτερα e, e' θα έχουμε $e * e' = e$, γιατί e' είναι ουδέτερο και $e * e' = e'$, γιατί e είναι ουδέτερο. Συνεπώς $e = e * e' = e'$. $\square$

4. Αντίστροφο στοιχείο ενός στοιχείου

Έστω $*$ ένας εσωτερικός νόμος επί του E με ουδέτερο e . Λέμε ότι ένα στοιχείο $a \in E$ αντιστρέφεται αριστερά ή ότι έχει **αντίστροφο αριστερά**, αν υπάρχει $a' \in E$ τέτοιο, ώστε $a' * a = e$. Το a' λέγεται τότε **αριστερό αντίστροφο** του a . Λέμε ότι το στοιχείο $a \in E$ αντιστρέφεται δεξιά ή ότι έχει **αντίστροφο δεξιά**, αν υπάρχει $a' \in E$ τέτοιο, ώστε $a * a' = e$. Το a' λέγεται τότε **δεξιό αντίστροφο** του a . Συνεπώς, αν

$$a * b = e$$

το a είναι αριστερό αντίστροφο του b και το b δεξιό αντίστροφο του a . Λέμε ότι το στοιχείο a **αντιστρέφεται** ή ότι είναι **αντιστρέψιμο**, αν υπάρχει $a' \in E$ τέτοιο, ώστε

$$a * a' = a' * a = e$$

Το a' λέγεται τότε **αντίστροφο** του a .

Ένα στοιχείο a λέγεται **ομαλό αριστερά** ή **δεξιά**, αν $a * x = a * y$ αντίστοιχα $x * a = y * a$ συνεπάγεται ότι $x = y$. Αν είναι ομαλό αριστερά και δεξιά, θα λέγεται **ομαλό**.

Κάθε αντιστρέψιμο στοιχείο a ως προς ένα προσεταιριστικό νόμο είναι ομαλό, γιατί αν a' το αντίστροφό του και $x * a = y * a$, έχουμε $(x * a) * a' = (y * a) * a'$ ή $x * (a * a') = y * (a * a')$ ή $x * e = y * e$ ή $x = y$. Όμοια $a * x = a * y$ συνεπάγεται $x = y$.

Αν ο νόμος δεν είναι προσεταιριστικός, ένα αντιστρέψιμο στοιχείο μπορεί να μην είναι ομαλό: Έστω $E = \{e, a, \beta\}$ και ο εσωτερικός νόμος $\cdot$ με πίνακα

$\cdot$	e	a	β
e	e	a	β
a	a	e	a
β	β	a	e

$$\begin{aligned} e &= \text{ουδέτερο} \\ a \cdot a &= e \text{ (} a \text{ αντιστρέψιμο)} \\ e \cdot a &= \beta \cdot a \neq e = \beta \end{aligned}$$

Παράδειγμα 11. i) Έστω ο εσωτερικός νόμος της σύνθεσης των συναρτήσεων $f: \mathbb{N} \rightarrow \mathbb{N}$. Η συνάρτηση $f: \mathbb{N} \rightarrow \mathbb{N}$ με τιμή $f(n) = n + 1$ δέχεται άπειρα αντίστροφα αριστερά, π.χ. κάθε συνάρτηση $g: \mathbb{N} \rightarrow \mathbb{N}$ με τιμή $g(1) = a \in \mathbb{N}$ και $g(n) = n - 1$ για $n > 1$ είναι αριστερό αντίστροφο του στοιχείου f , γιατί

$$g \circ f(n) = g(f(n)) = g(n + 1) = n = 1_{\mathbb{N}}(n) \text{ ή } g \circ f = 1_{\mathbb{N}}.$$

ii) Το στοιχείο $h \in \mathbb{N}^{\mathbb{N}}$ με

$$h(n) = \begin{cases} \frac{n}{2} & ; \quad n = \text{άρτιος} \\ \frac{n-1}{2} & ; \quad n = \text{περιττός} \end{cases}$$

δέχεται άπειρα αντίστροφα δεξιά. Π.χ., αν $a \in \mathbb{N}$ και

$$g_a(n) = \begin{cases} 2n & ; \quad \text{αν } a/n \\ 2n + 1 & ; \quad \text{αν } a \neq n \end{cases}$$

η συνάρτηση g_a είναι δεξιό αντίστροφο του h , γιατί

$$f \circ g_a(n) = \begin{cases} f(2n) & ; \quad a/n \\ f(2n + 1) & ; \quad a \neq n \end{cases} = \begin{cases} n & ; \quad a/n \\ n & ; \quad a \neq n \end{cases} = 1_{\mathbb{N}}$$

δηλαδή $f \circ g_a = 1_{\mathbb{N}}$. Για $a < \beta$, προφανώς $g_a \neq g_\beta$, γιατί $g_a(a) = 2a$ και $g_\beta(a) = 2a + 1$, συνεπώς $g_a(a) \neq g_\beta(a)$.

Παράδειγμα 12. Έστω E ένα σύνολο $\neq \emptyset$. Θεωρούμε στο E^E τον εσωτερικό νόμο της σύνθεσης.

- i) Το στοιχείο $f \in E^E$ αντιστρέφεται τότε και μόνο, όταν η f είναι αμφοιμονοσήμαντη και επί (Θεώρ.1§2).
 ii) Το στοιχείο $f \in E^E$ έχει αντίστροφο δεξιά, τότε και μόνο, όταν η f είναι επί.
 iii) Το στοιχείο $f \in E^E$ έχει αντίστροφο αριστερά, τότε και μόνο, όταν η f είναι αμφοιμονοσήμαντη.

Οι αποδείξεις προτείνονται σαν άσκηση.

Θεώρημα 1. Αν ο νόμος $*$ επί του E είναι προσεταιριστικός, κάθε στοιχείο $a \in E$ έχει το πολύ ένα αντίστροφο.

Απόδειξη. Έστω ότι κάποιο στοιχείο a έχει δύο ουδέτερα a', a'' και ότι e είναι το ουδέτερο του νόμου $*$. Τότε

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

Το αντίστροφο του στοιχείου a , όταν είναι μοναδικό, συμβολίζεται με a^{-1} . Ειδικά, όταν ο εσωτερικός νόμος συμβολίζεται με $+$, το αντίστροφο του a συμβολίζεται με $-a$ και λέγεται **αντίθετο** του a . $\square$

Πρόταση 2. Έστω $*$ ένας εσωτερικός νόμος επί του E με ουδέτερο στοιχείο. Αν τα στοιχεία $a, \beta \in E$ έχουν αντίστροφα στοιχεία, τότε τα στοιχεία $a^{-1}, a * \beta$ έχουν επίσης αντίστροφα στοιχεία και μάλιστα

$$(a^{-1})^{-1} = a, \quad (a * \beta)^{-1} = \beta^{-1} * a^{-1}.$$

Απόδειξη. Αφού το a^{-1} είναι αντίστροφο του a , έχουμε $a^{-1} * a = a * a^{-1} = e$. Βάσει του ορισμού, το αντίστροφο του a^{-1} υπάρχει και είναι a , δηλαδή $(a^{-1})^{-1} = a$. Επειδή

$$\begin{aligned} (a * \beta) * (\beta^{-1} * a^{-1}) &= ((a * \beta) * \beta^{-1}) * a^{-1} = (a * (\beta * \beta^{-1})) * a^{-1} \\ &= (a * e) * a^{-1} = a * a^{-1} = e \end{aligned}$$

και όμοια $(\beta^{-1} * a^{-1}) * (a * \beta) = e$, έπεται ότι το αντίστροφο $(a * \beta)^{-1}$ του $a * \beta$ είναι $\beta^{-1} * a^{-1}$. $\square$

Σημείωση. Αν ο εσωτερικός νόμος επί του E συμβολίζεται με $+$, το σύμπερασμα της πρότασης γράφεται

$$-(-a) = a, \quad -(a + \beta) = -\beta - a$$

5. Επιμεριστικότητα νόμου ως προς άλλο νόμο

Έστω E ένα σύνολο και $*, T$ δύο εσωτερικοί νόμοι επί του E . Λέμε ότι ο νόμος $*$ είναι **επιμεριστικός** ως προς το νόμο T από **αριστερά**, αν

$$a * (\beta T \gamma) = (a * \beta) T (a * \gamma)$$

και από **δεξιά**, αν

$$(a T \beta) * \gamma = (a * \gamma) T (\beta * \gamma)$$

Αν ο νόμος $*$ είναι επιμεριστικός ως προς τον T από αριστερά και δεξιά, λέμε ότι είναι **επιμεριστικός** ως προς τον T .

Παράδειγμα 13. Η τομή είναι επιμεριστική ως προς την ένωση, όπως και η ένωση ως προς την τομή (Θεώρ.1§1).

Η τομή είναι επιμεριστική ως προς τη συμμετρική διαφορά, όχι όμως και η ένωση, γιατί

$$A \cup (A \Delta \emptyset) = A \cup ((A - \emptyset) \cup (\emptyset - A)) = A \cup A = A$$

$$\text{και} \quad (A \cup A) \Delta (A \cup \emptyset) = A \Delta A = \emptyset$$

7. ΣΧΕΣΗ ΙΣΟΔΥΝΑΜΙΑΣ ΣΥΜΒΙΒΑΣΤΗ ΜΕ ΕΣΩΤΕΡΙΚΟ ΝΟΜΟ.

Έστω E ένα σύνολο, $*$ ένας εσωτερικός νόμος και $\sim$ μια σχέση ισοδυναμίας επί του E . Με $\bar{a}$ συμβολίζουμε την κλάση του $a \in E$ ως προς τη σχέση αυτή.

Η σχέση ισοδυναμίας $\sim$ λέγεται **συμβιβαστή** με το νόμο $*$, αν

$$x \sim a, y \sim \beta \Rightarrow x * y \sim a * \beta$$

Θεώρημα 1. Έστω $*$ ένας εσωτερικός νόμος επί του E και μια σχέση ισοδυναμίας $\sim$ επίσης επί του E συμβιβαστή με το νόμο $*$. Η συνάρτηση $(\bar{x}, \bar{y}) \mapsto \overline{x * y}$ του $E/\sim \times E/\sim$ στο $E/\sim$ είναι καλά ορισμένη και συνεπώς είναι ένας εσωτερικός νόμος επί του συνόλου πηλίκου $E/\sim$, τον οποίο συμβολίζουμε με το σύμβολο $\oplus$. Άρα ο εσωτερικός νόμος επί του $E/\sim$ είναι

$$\bar{x} \oplus \bar{y} = \overline{x * y}$$

Απόδειξη. Το στοιχείο $(\bar{x}, \bar{y})$ έχει περισσότερες παραστάσεις. Είναι $(\bar{x}, \bar{y}) = (\bar{a}, \bar{\beta})$ τότε και μόνο, όταν $\bar{x} = \bar{a}$ και $\bar{y} = \bar{\beta}$ ή $x \sim a$ και $y \sim \beta$. Έτσι στο

ίδιο στοιχείο $(\bar{x}, \bar{y})$ αντιστοιχίζονται τα στοιχεία $\overline{x * y}$ και $\overline{a * \beta}$. Ο όρος "η συνάρτηση f είναι καλά ορισμένη" σημαίνει ότι σε κάθε αρχέτυπο αντιστοιχίζεται με την f ένα μόνο στοιχείο. Συνεπώς πρέπει ν' αποδείξουμε ότι

$$(\bar{x}, \bar{y}) = (\bar{a}, \bar{\beta}) \Rightarrow \overline{x * y} = \overline{a * \beta} \quad (1)$$

οτι δηλαδή η τιμή της f είναι ανεξάρτητη από την παράσταση των κλάσεων $\bar{x}, \bar{y}$ ή την επιλογή των αντιπροσώπων των κλάσεων. Η (1) ισχύει, γιατί από την υπόθεση παίρνουμε ότι $x \sim a$ και $y \sim \beta$. Επειδή η σχέση ισοδυναμίας είναι συμβιβαστή με τον εσωτερικό νόμο, έχουμε $x * y \sim a * \beta$ δηλαδή $\overline{x * y} = \overline{a * \beta}$. $\square$

Πρόταση 1. Έστω $*$ ένας εσωτερικός νόμος επί του E και $\sim$ μια σχέση ισοδυναμίας επί του E συμβιβαστή με το νόμο $*$. Έστω $\oplus$ ο εσωτερικός νόμος στο σύνολο πηλίκο $\bar{x} \oplus \bar{y} = \overline{x * y}$. Τότε

- i) αν ο νόμος $*$ είναι αντιμεταθετικός ή προσεταιριστικός, θα είναι αντιμεταθετικός αντίστοιχα προσεταιριστικός και ο νόμος $\oplus$.
- ii) Αν ο νόμος $*$ έχει ουδέτερο στοιχείο το e , ο νόμος $\oplus$ έχει ουδέτερο το $\bar{e}$.
- iii) Αν το στοιχείο a έχει αντίστροφο στο E ως προς το νόμο $*$, το $\bar{a}$ έχει αντίστροφο ως προς το νόμο $\oplus$ στο $E/\sim$ το στοιχείο $\overline{a^{-1}}$.

Απόδειξη. i) Έστω ότι ο νόμος $*$ είναι αντιμεταθετικός. Για οποιαδήποτε $\bar{x}, \bar{y} \in E/\sim$ έχουμε

$$\bar{x} \oplus \bar{y} = \overline{x * y} = \overline{y * x} = \bar{y} \oplus \bar{x}$$

Αν ο νόμος $*$ είναι προσεταιριστικός, τότε

$$\begin{aligned} \bar{x} \oplus (\bar{y} \oplus \bar{z}) &= \overline{x * (\overline{y * z})} = \overline{x * (y * z)} = \overline{(x * y) * z} \\ &= \overline{x * y} \oplus \bar{z} = (\bar{x} \oplus \bar{y}) \oplus \bar{z} \end{aligned}$$

ii) Προφανώς $\bar{x} \oplus \bar{e} = \overline{x * e} = \bar{x}$ και $\bar{e} \oplus \bar{x} = \overline{e * x} = \bar{x}$.

iii) Έχουμε $\bar{a} \oplus \bar{a}^{-1} = \overline{a * a^{-1}} = \bar{e} = \bar{a}^{-1} \oplus \bar{a}$, άρα $(\bar{a})^{-1} = \bar{a}^{-1}$. $\square$

Πρόταση 2. Έστω $m \in \mathbb{N}$ και $\sim$ η σχέση ισοδυναμίας επί του $\mathbb{Z}$ με $a \sim \beta \Leftrightarrow m/a - \beta$. Η σχέση αυτή είναι συμβιβαστή με την πρόσθεση και τον πολλαπλασιασμό του $\mathbb{Z}$.

Απόδειξη. Έστω $x \sim a, y \sim \beta$. Τότε $m/x - a, m/y - \beta$, συνεπώς $x - a = mk, y - \beta = m\lambda$ με $k, \lambda \in \mathbb{Z}$, οπότε $(x + y) - (a + \beta) = m(k + \lambda)$, δηλαδή

$x + y \sim a + \beta$ και $x \cdot y = (a + mk) \cdot (\beta + m\lambda) = a\beta + m(k\beta + \lambda a + mk\lambda)$,
δηλαδή $x \cdot y \sim a \cdot \beta$. $\square$

Πρόταση 3. Στο σύνολο $\mathbb{Z}_m$ των ακεραίων modulo m ορίζονται δύο εσωτερικοί νόμοι $\oplus, \odot$ ως εξής:

$$\bar{x} \oplus \bar{y} = \overline{x + y} \quad , \quad \bar{x} \odot \bar{y} = \overline{x \cdot y}$$

- i) Οι νόμοι είναι αντιμεταθετικοί, προσεταιριστικοί, έχουν ουδέτερα στοιχεία τα $\bar{0}, \bar{1}$ και ο νόμος $\odot$ είναι επιμεριστικός ως προς το νόμο $\oplus$.
- ii) Κάθε στοιχείο $\bar{x}$ έχει αντίστροφο ως προς το νόμο $\oplus$, όχι όμως πάντοτε ως προς το νόμο $\odot$.

Απόδειξη. i) Οι ιδιότητες προκύπτουν από το θεωρ.1 και τις προτ.2,3. Ανεξάρτητα από τα θεωρήματα αυτά, αποδεικνύονται εύκολα.

- ii) Ότι το στοιχείο $\bar{x}$ δεν έχει πάντοτε αντίστροφο ως προς το δεύτερο νόμο φαίνεται από το εξής παράδειγμα: Στο $\mathbb{Z}_4$ έχουμε $\bar{2} \odot \bar{x} \neq \bar{1}$ για κάθε $\bar{x} \in \mathbb{Z}_4$, αφού $\bar{2} \odot \bar{0} = \bar{0}$, $\bar{2} \odot \bar{1} = \bar{2}$, $\bar{2} \odot \bar{2} = \bar{0}$, $\bar{2} \odot \bar{3} = \bar{2}$. Συνεπώς το $\bar{2}$ δεν έχει αντίστροφο ως προς το νόμο $\odot$. Το στοιχείο $\bar{3}$ έχει αντίστροφο ως προς το νόμο $\odot$, γιατί $\bar{3} \odot \bar{3} = \bar{9} = \bar{1}$, δηλαδή $(\bar{3})^{-1} = \bar{3}$. $\square$

Σημείωση. Θα δούμε ότι το στοιχείο $\bar{a} \in \mathbb{Z}_m$ έχει αντίστροφο ως προς το νόμο $\odot$ τότε και μόνο, όταν ο μόνος κοινός διαιρέτης των a, m είναι η μονάδα.

Παράδειγμα 14. Στο $\mathbb{Z}_5$ έχουμε $\bar{2} \oplus \bar{3} = \bar{5} = \bar{0}$ και $\bar{2} \odot \bar{3} = \bar{6} = \bar{1}$. Στο $\mathbb{Z}_8$ έχουμε $\bar{2} \oplus \bar{7} = \bar{9} = \bar{1}$ και $\bar{2} \odot \bar{7} = \bar{14} = \bar{6}$.

Παράδειγμα 15. Δείξτε ότι στο $\mathbb{Z}_3$ η εξίσωση $x^2 = \bar{2}$ δεν έχει λύση. Έχουμε $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{4} = \bar{1}$, δηλαδή για κάθε $x \in \mathbb{Z}_3$, $x^2 \neq \bar{2}$. Άρα η εξίσωση δεν έχει λύση, δηλαδή το $\bar{2}$ δεν έχει "τετραγωνική" ρίζα στο $\mathbb{Z}_3$.

8. ΦΥΣΙΚΟΙ ΑΡΙΘΜΟΙ

Δεχόμαστε ότι υπάρχει ένα σύνολο $\mathbb{N}$ με τις εξής ιδιότητες:

- i) Είναι διατεταγμένο.
- ii) Κάθε υποσύνολο του $\mathbb{N}$ μη κενό έχει μικρότερο στοιχείο*
- iii) Το $\mathbb{N}$ δεν έχει μεγαλύτερο στοιχείο.

* Ένα διατεταγμένο σύνολο, του οποίου κάθε υποσύνολο έχει μικρότερο στοιχείο, λέγεται καλώς διατεταγμένο και η αντίστοιχη διάταξη καλή διάταξη.

iv) Κάθε φραγμένο υποσύνολο του $\mathbb{N}$ έχει μεγαλύτερο στοιχείο.

Ένα σύνολο με τις ιδιότητες i)-iv) λέγεται σύνολο φυσικών αριθμών.

- Προφανώς το $\mathbb{N}$ είναι ολικά διατεταγμένο, γιατί αν $m, n \in \mathbb{N}$, το υποσύνολο $\{m, n\}$ έχει κατά το αξίωμα (ii) μικρότερο στοιχείο, συνεπώς $m \leq n$ ή $m \geq n$ καθόσον το μικρότερο στοιχείο του $\{m, n\}$ είναι το m αντίστοιχα n .
- Το $\mathbb{N}$ δέχεται, αφού $\mathbb{N} \subseteq \mathbb{N}$, μικρότερο στοιχείο (αξίωμα ii). Το συμβολίζουμε με 1.
- Υπάρχει μια γνήσια αύξουσα και αμφιμονοσήμαντη συνάρτηση f του $\mathbb{N}$ στο $\mathbb{N}$.

Έστω $n \in \mathbb{N}$, $A(n) = \{m \in \mathbb{N}; m > n\}$. Κατά την ιδιότητα iii) $A(n) \neq \emptyset$. Έχει συνεπώς μικρότερο στοιχείο (ii). Το συμβολίζουμε με n^* και το ονομάζουμε **επόμενο** του n . Η συνάρτηση

$$f: \mathbb{N} \rightarrow \mathbb{N} \text{ με } f(n) = n^*$$

είναι αμφιμονοσήμαντη και γνήσια αύξουσα. Το n λέγεται προηγούμενο του n^* .

Θεώρημα 1. Έστω $A \subseteq \mathbb{N}$ τέτοιο, ώστε $1 \in A$ και $f(A) \subseteq A$. Τότε $A = \mathbb{N}$.

Απόδειξη. Έστω $A \neq \mathbb{N}$. Το συμπλήρωμα A' του A είναι $\neq \emptyset$, συνεπώς έχει μικρότερο στοιχείο, έστω το m . Επειδή $1 \in A$, $m > 1$. Υπάρχει $n \in \mathbb{N}$, ώστε $n^* = m$. Τότε $n \in A$, $n^* = f(n) \in A$, δηλαδή $n^* = m \in A$, πράγμα άτοπο, αφού $m \in A'$. $\square$

Το θεώρημα αυτό χρησιμοποιείται για την απόδειξη προτάσεων των οποίων η αλήθεια εξαρτάται από ένα φυσικό αριθμό n . Η αποδεικτική αυτή μέθοδος λέγεται **μέθοδος της επαγωγής** και εφαρμόζεται ως εξής:

Έστω $\Pi(n)$ μια πρόταση της οποίας η αλήθεια εξαρτάται από το φυσικό n . Αν

- 1° $\Pi(1)$ είναι αληθής.
- 2° $\Pi(n)$ αληθής $\Rightarrow \Pi(n^*)$ αληθής

η πρόταση είναι αληθής για κάθε φυσικό n . Γιατί το σύνολο $A = \{n \in \mathbb{N}; \Pi(n) \text{ αληθής}\}$ πληρεί τις υποθέσεις του θεωρήματος και συνεπώς $A = \mathbb{N}$. Η επαγωγή δεν χρησιμοποιείται μόνο σαν αποδεικτική μέθοδος, αλλά και για ορισμό συναρτήσεων και εννοιών.

Ορισμός 1. Ορίζουμε τον εσωτερικό νόμο της πρόσθεσης $+$ επί του $\mathbb{N}$ θέτοντας

$$n + 1 = n^* \quad , \quad n + m^* = (n + m)^*$$

Η πρόσθεση $+$ είναι ορισμένη επί του $\mathbb{N} \times \mathbb{N}$.

Πραγματικά, είναι ορισμένη σ' ένα υποσύνολο $\mathbb{N} \times A$, όπου $A \subseteq \mathbb{N}$. Προφανώς $1 \in A$ και αν $m \in A$, τότε $m^* \in A$ και συνεπώς $A = \mathbb{N}$.

Ορισμός 2. Ορίζουμε τον εσωτερικό νόμο του πολλαπλασιασμού $\cdot$ επί του $\mathbb{N}$ θέτοντας

$$n \cdot 1 = n \quad , \quad n \cdot m^* = n \cdot m + n$$

Στη συνέχεια μπορούμε ν' αποδείξουμε όλες τις γνωστές ιδιότητες των πράξεων της πρόσθεσης, του πολλαπλασιασμού και της διάταξης στο σύνολο των φυσικών αριθμών.

9. ΑΚΕΡΑΙΟΙ, ΡΗΤΟΙ ΑΡΙΘΜΟΙ

Αν a, β είναι δύο φυσικοί αριθμοί, δεν υπάρχει πάντοτε φυσικός x τέτοιος, ώστε $a + x = \beta$. Η εξίσωση αυτή έχει λύση στο σύνολο $\mathbb{N}$ μόνο, όταν $a < \beta$. Η λύση αυτή είναι μοναδική και γράφεται $x = \beta - a$. Αν το x είναι λύση και της εξίσωσης $a' + x = \beta'$, θα έχουμε $\beta - a = \beta' - a'$ ή $a + \beta' = \beta + a'$. Η λύση όμως x ορίζεται μονοσήμαντα από το ζεύγος (a, β) . Συνεπώς $(a, \beta) = (a', \beta')$ τότε και μόνο, όταν $a + \beta' = \beta + a'$. Αυτές οι παρατηρήσεις μας οδηγούν στην εξής κατασκευή του συνόλου $\mathbb{Z}$ των ακεραίων αριθμών από το σύνολο των φυσικών αριθμών:

Στο σύνολο $\mathbb{N} \times \mathbb{N}$ ορίζουμε μια σχέση ισοδυναμίας $\sim$ θέτοντας

$$(a, \beta) \sim (a', \beta') \Leftrightarrow a + \beta' = \beta + a'$$

Το σύνολο πηλίκο $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$ λέγεται σύνολο ακεραίων αριθμών. Ο ορισμός μεταξύ των ακεραίων αριθμών και η ταύτιση του συνόλου των φυσικών αριθμών με ένα υποσύνολο του $\mathbb{Z}$ πραγματοποιούνται ως εξής: 'Εστω $(\overline{a}, \overline{\beta})$ η κλάση του $(a, \beta) \in \mathbb{N} \times \mathbb{N}$ ως προς τη σχέση ισοδυναμίας $\sim$ και δύο ακεραίοι

$$x = (\overline{a}, \overline{\beta}) \quad , \quad x' = (\overline{a'}, \overline{\beta'})$$

Ορίζουμε

$$\begin{aligned} x + x' &= (\overline{a + a'}, \overline{\beta + \beta'}) \\ x \cdot x' &= (\overline{aa' + \beta\beta'}, \overline{a\beta' + \beta a'}) \end{aligned}$$

Αποδεικνύουμε ότι το άθροισμα $x + x'$ και το γινόμενο $x \cdot x'$ είναι ανεξάρτητα από την επιλογή των αντιπροσώπων των x, x' . Έστω π.χ. $x = (\overline{a_1, \beta_1})$, $x' = (\overline{a'_1, \beta'_1})$. Τότε

$$a + \beta_1 = \beta + a_1, \quad a' + \beta'_1 = \beta' + a'_1$$

$$\text{ή} \quad (a + \beta_1) + (a' + \beta'_1) = (\beta + a_1) + (\beta' + a'_1)$$

$$\text{ή} \quad (a + a') + (\beta_1 + \beta'_1) = (\beta + \beta') + (a_1 + a'_1)$$

δηλαδή $(\overline{a + a', \beta_1 + \beta'_1}) = (\overline{a_1 + a'_1, \beta_1 + \beta'_1})$. Ανάλογα αποδεικνύεται η ανεξαρτησία του γινομένου $x \cdot x'$ από την επιλογή των αντιπροσώπων των κλάσεων x, x' .

Πρόταση 1. Ισχύουν οι παρακάτω ιδιότητες των πράξεων των ακεραίων αριθμών

$$\text{i)} \quad x + y = y + x, \quad x \cdot y = y \cdot x$$

$$\text{ii)} \quad x + (y + z) = (x + y) + z, \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

iii) Ουδέτερο της πρόσθεσης είναι το $0 = (\overline{n, n})$ και του πολλαπλασιασμού το $\bar{1} = (\overline{n+1, n})$.

iv) Η εξίσωση $x + z = y$ με $x, y \in \mathbb{Z}$ έχει πάντοτε μια μόνο λύση $z \in \mathbb{Z}$.

$$\text{v)} \quad x \cdot (y + z) = x \cdot y + x \cdot z$$

Οι αποδείξεις δεν παρουσιάζουν δυσκολία.

$$\begin{aligned} \text{Π.χ.} \quad \bar{1} \cdot x &= (\overline{n+1, n}) \cdot (\overline{a, \beta}) = (\overline{(n+1)a + n\beta, (n+1)\beta + na}) \\ &= (\overline{na + a + n\beta, n\beta + \beta + na}) \\ &= (\overline{a, \beta}) = x \end{aligned}$$

$$\text{γιατί } (na + a + n\beta) + \beta = (n\beta + \beta + na) + a. \quad \square$$

Ταυτίζουμε το σύνολο των φυσικών αριθμών $\mathbb{N}$ με το υποσύνολο $\mathbb{Z}^+$ του $\mathbb{Z}$ που αποτελείται από τα στοιχεία $(\overline{n+1, 1})$ με $n \in \mathbb{N}$. Η συνάρτηση $n \mapsto (\overline{n+1, 1})$ είναι αμφιμονοσήμαντη, γιατί

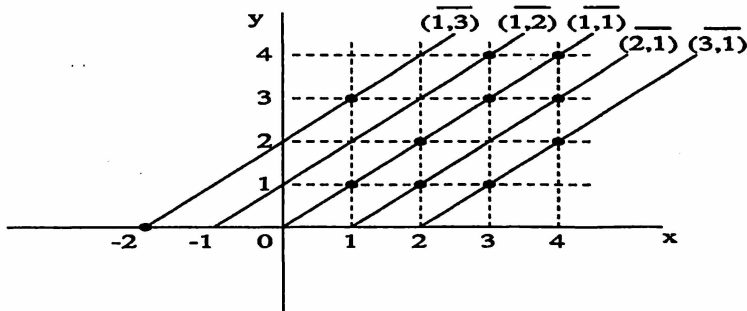
$$(\overline{n+1, 1}) = (\overline{m+1, 1}) \Rightarrow (n+1) + 1 = 1 + (m+1) \Rightarrow n = m.$$

και επι πλέον, πράγμα πολύ σημαντικό,

$$f(n + m) = f(n) + f(m)$$

$$f(n \cdot m) = f(n) \cdot f(m)$$

δηλαδή η f διατηρεί τ' αποτελέσματα των πράξεων. Για το λόγο αυτό ταυτίζουμε το φυσικό n με τον ακέραιο $(\overline{n+1}, 1)$. Έτσι $1 = (\overline{2}, 1) = (\overline{n+1}, 1)$, $2 = (\overline{3}, 1), \dots, n = (\overline{n+1}, 1)$. Στο παρακάτω σχήμα παριστάνουμε τις κλάσεις $(\overline{1}, 1), (\overline{2}, 1), (\overline{3}, 1), (\overline{1}, 2)$. Κάθε κλάση είναι ένα σύνολο σημείων του $\mathbb{N} \times \mathbb{N}$ που βρίσκονται σε ευθεία παράλληλη της διχοτόμου της γωνίας xOy .



Οι ακέραιοι $(\overline{a}, \beta), (\beta, \overline{a})$ είναι αντίθετοι, γιατί

$$(\overline{a}, \beta) + (\beta, \overline{a}) = (\overline{a + \beta}, \beta + \overline{a}) = 0$$

Ένας οποιοσδήποτε ακέραιος έχει μια από τις τρεις μορφές

$$(\overline{n}, \overline{n}) = 0, (\overline{m+n}, \overline{n}) = m, (\overline{n}, \overline{m+n}) = -m \quad \text{με } m \in \mathbb{N}.$$

Συνεπώς

$$\mathbb{Z} = \{\dots -3, -2, -1, 0, 1, 2, 3, \dots\}$$

Οι κανόνες των προσήμων $a(-\beta) = (-a)\beta = -a\beta$, $(-a)(-\beta) = a\beta$ προκύπτουν εύκολα.

Διάταξη στο $\mathbb{Z}$

Με τη βοήθεια της διάταξης $\leq$ στο $\mathbb{N}$ ορίζουμε μια σχέση διάταξης επί του $\mathbb{Z}$ θέτοντας

$$(\overline{a}, \beta) \leq (\overline{a'}, \beta') \Leftrightarrow a + \beta' \leq \beta + a'$$

Είναι εύκολο ν' αποδείξουμε ότι η σχέση αυτή είναι καλά ορισμένη και ότι έχει όλες τις ιδιότητες της διάταξης των ακεραίων αριθμών, που είναι γνωστές από το Λύκειο.

Ρητοί αριθμοί

Το σύνολο των ρητών αριθμών $\mathbb{Q}$ κατασκευάζεται από το σύνολο των ακεραίων $\mathbb{Z}$ ως εξής: Αν $\mathbb{Z}^* = \mathbb{Z} - \{0\}$, ορίζουμε στο $\mathbb{Z} \times \mathbb{Z}^*$ μια σχέση ισοδυναμίας $\sim$ θέτοντας

$$(a, \beta) \sim (a', \beta') \Leftrightarrow a\beta' = a'\beta$$

Το πηλίκο $\mathbb{Z} \times \mathbb{Z}^* / \sim$ είναι το σύνολο των ρητών αριθμών $\mathbb{Q}$. Η κλάση του (a, β) συμβολίζεται με $\frac{a}{\beta}$. Οι πράξεις της πρόσθεσης και του πολλαπλασιασμού στο σύνολο των ρητών ορίζονται από τις ισότητες:

$$\frac{a}{\beta} + \frac{\gamma}{\delta} = \frac{a\delta + \beta\gamma}{\beta\delta}, \quad \frac{a}{\beta} \cdot \frac{\gamma}{\delta} = \frac{a \cdot \gamma}{\beta \cdot \delta}$$

Εύκολα επαληθεύονται οι γνωστές ιδιότητες των πράξεων των ρητών αριθμών. Η συνάρτηση $n \mapsto \frac{n}{1}$ είναι αμφιμονοσήμαντη και διατηρεί τ' αποτελέσματα των πράξεων. Γι' αυτό γράφουμε $n = \frac{n}{1}$. Προφανώς $1 = \frac{1}{1} = \frac{m}{m}$. Κάθε ρητός $\frac{m}{n} \neq 0$, έχει αντίστροφο, μάλιστα $(\frac{m}{n})^{-1} = \frac{n}{m}$, γιατί

$$\frac{m}{n} \cdot \frac{n}{m} = \frac{m \cdot n}{n \cdot m} = 1.$$

Διάταξη στο $\mathbb{Q}$

Ορίζουμε $\frac{a}{\beta} > 0 \Leftrightarrow a\beta > 0$. Η σχέση

$$\frac{a}{\beta} \geq \frac{\gamma}{\delta} \Leftrightarrow \frac{a}{\beta} - \frac{\gamma}{\delta} > 0 \quad \text{ή} \quad \frac{a}{\beta} = \frac{\gamma}{\delta}$$

είναι μια σχέση διάταξης επί του $\mathbb{Q}$ με όλες τις γνωστές ιδιότητες.

10. ΠΛΗΘΑΡΙΘΜΟΙ

Θ' ασχοληθούμε στην παράγραφο αυτή με "ποσοτικές" ιδιότητες των συνόλων: Πόσα στοιχεία έχει ένα σύνολο; Πότε δύο σύνολα A, B έχουν το αυτό "πλήθος" στοιχείων; Τα σύνολα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ έχουν το ίδιο "πλήθος" στοιχείων;

Σε προηγούμενη παράγραφο χρησιμοποιήσαμε τον όρο πεπερασμένο σύνολο. Κατά την κοινή αντίληψη ένα σύνολο A είναι πεπερασμένο, όταν

μπορούμε ν' απαριθμήσουμε τα στοιχεία του χρησιμοποιώντας τους φυσικούς αριθμούς $1, 2, \dots, n$, οπότε λέμε ότι το σύνολο A έχει n στοιχεία. Στα μαθηματικά αυτό σημαίνει ότι υπάρχει μια συνάρτηση $f: A \rightarrow \{1, 2, \dots, n\}$ αμφιμονοσήμαντη και επί. Αν και το σύνολο B έχει n στοιχεία, υπάρχει μια αμφιμονοσήμαντη και επί συνάρτηση $g: B \rightarrow \{1, 2, \dots, n\}$. Τότε η g αντιστρέφεται και η συνάρτηση $h = g^{-1} \circ f: A \rightarrow B$ είναι αμφιμονοσήμαντη και επί. Η παρατήρηση αυτή μας οδηγεί στον εξής ορισμό:

Ορισμός 1. Λέμε ότι δύο σύνολα A, B έχουν το ίδιο "πλήθος" στοιχείων ή ότι είναι **ισοδύναμα**, αν υπάρχει μια συνάρτηση $f: A \rightarrow B$ αμφιμονοσήμαντη και επί. Γράφουμε τότε $A \sim B$.

Η σχέση $\sim$ είναι μια σχέση ισοδυναμίας μεταξύ των συνόλων, γιατί

- i) $A \sim A$
- ii) $A \sim B \Rightarrow B \sim A$
- iii) $A \sim B, B \sim \Gamma \Rightarrow A \sim \Gamma$

Η ιδιότητα (i) ισχύει, αφού η ταυτοτική συνάρτηση $1_A: A \rightarrow A$ είναι αμφιμονοσήμαντη και επί. Η (ii) ισχύει, γιατί, αν η $f: A \rightarrow B$ είναι αμφιμονοσήμαντη και επί, η $f^{-1}: B \rightarrow A$ είναι επίσης αμφιμονοσήμαντη και επί, αφού αντιστρέφεται. Τέλος, αν οι συναρτήσεις $A \xrightarrow{f} B, B \xrightarrow{g} \Gamma$ είναι αμφιμονοσήμαντες και επί, η $g \circ f: A \rightarrow \Gamma$ είναι αμφιμονοσήμαντη και επί, γιατί αντιστρέφεται.

Ορισμός 2. Η κλάση ισοδυναμίας στην οποία ανήκει ένα σύνολο A λέγεται **πληθάριθμος** του A (cardinal number of A) και συμβολίζεται με $\text{Card} A$ ή $|A|$, αν δεν δημιουργείται σύγχυση.

Ορισμός 3. Ένα σύνολο A λέγεται **αριθμήσιμο**, αν είναι ισοδύναμο με το σύνολο των φυσικών αριθμών.

Πρόταση 1. Τα σύνολα των ακεραίων $\mathbb{Z}$ και των ρητών $\mathbb{Q}$ είναι αριθμήσιμα:

$$\mathbb{Z} \sim \mathbb{N}, \quad \mathbb{Q} \sim \mathbb{N}.$$

Απόδειξη. Η συνάρτηση $f: \mathbb{Z} \rightarrow \mathbb{N}$ με τιμή

$$f(n) = \begin{cases} 2n & ; \quad n > 0 \\ -2n + 1 & ; \quad n \leq 0 \end{cases}$$

είναι αμφιμονοσήμαντη και επί. Φαίνεται αμέσως από τον πίνακα των τιμών της

x	...	-3	-2	-1	0	1	2	3	4	...
$f(x)$	...	7	5	3	1	2	4	6	8	...

□

Θ' αποδείξουμε τώρα ότι $\mathbb{Q} \sim \mathbb{N}$. Αρκεί ν' αποδείξουμε ότι $\mathbb{Q} \sim \mathbb{Z}$, αφού $\mathbb{Z} \sim \mathbb{N}$. Κάθε ρητός γράφεται υπό τη μορφή $\frac{m}{n}$, όπου $n > 0$ και οι m, n δεν έχουν κοινό διαιρέτη. Θεωρούμε τη συνάρτηση $g : \mathbb{Q} \rightarrow \mathbb{Z}$ με τιμή

$$g\left(\frac{m}{n}\right) = \begin{cases} 2^{m-1}(2n-1) & ; \quad m > 0, n > 0 \\ 0 & ; \quad m = 0 \\ 2^{m-1}(2n+1) & ; \quad m > 0, n < 0 \end{cases}$$

Εύκολα επαληθεύουμε ότι η συνάρτηση g είναι αμφιμονοσήμαντη και επί. Θα χρησιμοποιήσουμε για την απόδειξη τη γνωστή ιδιότητα των ακεραίων κατά την οποία κάθε ακέραιος γράφεται υπό την μορφή $2^a \cdot \beta$, όπου a φυσικός και β περιττός φυσικός.

Πρόταση 2. $\{1, 2, \dots, n\} \sim \{1, 2, \dots, m\} \Leftrightarrow n = m$.

Απόδειξη. Παρατηρούμε ότι, αν $A \sim B$ και $(a, \beta) \in A \times B$, τότε $A - \{a\} \sim B - \{\beta\}$. Πραγματικά, υπάρχει μια συνάρτηση f του A επί του B αμφιμονοσήμαντη. Η συνάρτηση $g : A - \{a\} \rightarrow B - \{\beta\}$ με τιμή

$$g(x) = \begin{cases} f(x) & ; \quad x \neq f^{-1}(\beta) \\ f(a) & ; \quad x = f^{-1}(\beta) \end{cases}$$

είναι αμφιμονοσήμαντη και επί. Στη συνέχεια αποδεικνύουμε ότι, όταν $m \neq n$, $\mathbb{N}_m \not\sim \mathbb{N}_n$. Έστω

$$A = \{n \in \mathbb{N} ; \mathbb{N}_m \not\sim \mathbb{N}_n \text{ για } 1 \leq m < n\}.$$

Προφανώς $1 \in A$, γιατί δεν υπάρχει $m < 1$ με $\mathbb{N}_m \not\sim \mathbb{N}_n$. Έστω ότι $n \in A$. Θ' αποδείξουμε ότι $n+1 \in A$. Έστω $m < n+1$. Προφανώς $\mathbb{N}_1 \not\sim \mathbb{N}_{n+1}$, γιατί $\mathbb{N}_1 = \{1\}$ και $\mathbb{N}_{n+1} = \{1, 2, \dots, n+1\}$. Αν $\mathbb{N}_m \sim \mathbb{N}_{n+1}$, θα είχαμε $\mathbb{N}_{m-1} \sim \mathbb{N}_n$ πράγμα άτοπο, αφού $n \in \mathbb{N}$ και $m < n+1$ συνεπάγεται $m-1 < n$. Άρα $n+1 \in A$, $A = \mathbb{N}$ και $\mathbb{N}_m \not\sim \mathbb{N}_n$, όταν $m < n$. Έτσι $\mathbb{N}_m \not\sim \mathbb{N}_n$ για $m \neq n$. $\square$

Ορισμός 4. Ένα σύνολο A λέγεται **πεπερασμένο**, αν είναι ισοδύναμο μ' ένα σύνολο $\{1, 2, \dots, n\}$ με $n \in \mathbb{N}$. Σύμφωνα με την πρόταση 2 ο n ορίζεται μονοσήμαντα. Αν ένα σύνολο δεν είναι πεπερασμένο, λέγεται **άπειρο** σύνολο.

Πρόταση 3. Κάθε άπειρο σύνολο A έχει ένα υποσύνολο αριθμήσιμο.

Απόδειξη. Ορίζουμε μια συνάρτηση $f : \mathbb{N} \rightarrow A$ ως εξής:

$$\begin{aligned} f(1) &= a_1 \in A, \\ f(2) &= a_2 \in A - \{a_1\} \\ &\dots\dots\dots \\ f(n) &= a_n \in A - \{a_1, a_2, \dots, a_{n-1}\}. \end{aligned}$$

Προφανώς η f είναι αμφιμονοσήμαντη και επί του υποσυνόλου $\{a_1, a_2, \dots, a_n, \dots\}$ του A . Άρα το υποσύνολο αυτό του A είναι αριθμήσιμο. $\square$

Αν $A \sim \{1, 2, \dots, n\}$ ο πληθάριθμος του A συμβολίζεται με n . Ο πληθάριθμος του $\mathbb{N}$ συμβολίζεται με $\aleph_0$ (αλέφ μηδέν). Αφού τα σύνολα $\mathbb{Z}, \mathbb{Q}$ είναι αριθμήσιμα έχουμε

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$$

Υπάρχει σύνολο, το οποίο δεν είναι αριθμήσιμο:

Πρόταση 4. Το σύνολο των συναρτήσεων $f : \mathbb{N} \rightarrow \{0, 1\}$ δεν είναι αριθμήσιμο.

Απόδειξη. Ας υποθέσουμε ότι το σύνολο αυτό είναι αριθμήσιμο. Τα στοιχεία του θα παρίστανται με το σύνολο $F = \{f_1, f_2, \dots, f_n, \dots\}$. Θεωρούμε τη συνάρτηση $g : \mathbb{N} \rightarrow \{0, 1\}$, η οποία ορίζεται ως εξής:

$$g(n) = \begin{cases} 1 & ; \text{ αν } f_n(n) = 0 \\ 0 & ; \text{ αν } f_n(n) = 1 \end{cases}$$

Προφανώς $g \notin F$, γιατί, αν $g = f_m \in F$, θα είχαμε $g(m) = f_m(m)$, πράγμα ασυμβίβαστο με τον ορισμό της g . $\square$

Πρόταση 5. Το σύνολο των πραγματικών αριθμών δεν είναι αριθμήσιμο.

Απόδειξη. Βλέπε "Πραγματική Ανάλυση, Δ.Σ." Ο πληθάριθμος του $\mathbb{R}$ συμβολίζεται με c και λέγεται "δύναμη του συνεχούς". $\square$

Πρόταση 6. Το σύνολο $\mathbb{N} \times \mathbb{N}$ είναι αριθμήσιμο.

Απόδειξη. Αριθμούμε τα στοιχεία του $\mathbb{N} \times \mathbb{N}$ ακολουθώντας τα βέλη στο παρακάτω σχήμα

πολυωνύμων βαθμού m και άθροισμα απολύτων τιμών των συντελεστών n . Το σύνολο αυτό είναι πεπερασμένο. Επειδή $\mathbb{Z}[x] = \bigcup_{(m,n) \in \mathbb{N} \times \mathbb{N}} P(m,n)$ και το $\mathbb{N} \times \mathbb{N}$ είναι αριθμήσιμο, το $\mathbb{Z}[x]$ είναι αριθμήσιμο. $\square$

Εφαρμογή 2. Ένας πραγματικός αριθμός λέγεται αλγεβρικός, αν είναι ρίζα ενός πολυωνύμου με συντελεστές ακεραίους. Θ' αποδειχτεί ότι το σύνολο των αλγεβρικών αριθμών είναι αριθμήσιμο.

Απόδειξη. Κάθε ρητός $\rho = \frac{m}{n}$ είναι αλγεβρικός, γιατί είναι ρίζα του πολυωνύμου $n \cdot x - m = 0$. Έτσι το σύνολο των αλγεβρικών αριθμών είναι άπειρο. Το πλήθος των πραγματικών ριζών ενός πολυωνύμου δεν υπερβαίνει το βαθμό του. Έστω $\{P_1(x), P_2(x), \dots, P_n(x), \dots\}$ το σύνολο των πολυωνύμων με συντελεστές ακεραίους (εφαρμογή 1). Συνεπώς το σύνολο A_i των αλγεβρικών αριθμών που είναι ρίζες του πολυωνύμου $P_i(x)$ είναι πεπερασμένο. Άρα το σύνολο $\bigcup_1^\infty A_i$ είναι αριθμήσιμο. $\square$

11. ΠΡΑΞΕΙΣ ΚΑΙ ΔΙΑΤΑΞΗ ΠΛΗΘΑΡΙΘΜΩΝ

Ορισμός 1. Έστω A, B δύο σύνολα. Το άθροισμα και το γινόμενο των πληθαρίσμων $\text{Card } A, \text{Card } B$ ορίζεται ως εξής:*

$$\text{Card } A + \text{Card } B = \text{Card } (A \cup B), \text{ αν } A \cap B = \emptyset$$

$$\text{Card } A \cdot \text{Card } B = \text{Card } (A \times B).$$

Οι ορισμοί είναι ανεξάρτητοι από την εκλογή των A, B .

Πρόταση 1. Αν $A \sim A', B \sim B'$, τότε

- i) $A \cup B \sim A' \cup B'$, όταν $A \cap B = A' \cap B' = \emptyset$
- ii) $A \times B \sim A' \times B'$

Απόδειξη. i) Έστω $f: A \rightarrow A', g: B \rightarrow B'$ αμφιμονοσήμαντες και επί.

Εύκολα προκύπτει ότι η συνάρτηση $h: A \cup B \rightarrow A' \cup B'$ με τιμή

$$h(x) = \begin{cases} f(x) & ; x \in A \\ g(x) & ; x \in B \end{cases}$$

είναι αμφιμονοσήμαντη και επί. Άρα

$$\text{Card } (A \cup B) = \text{Card } (A' \cup B') = \text{Card } A' + \text{Card } B'.$$

* Αν $A \cap B \neq \emptyset$, θεωρούμε τα σύνολα $A \times \{q\}, \{q\} \times B$, όπου $q \notin A \cup B$, τα οποία είναι ξένα μεταξύ τους και $A \sim A \times \{q\}, B \sim \{q\} \times B$.

- ii) Όμοια η συνάρτηση $h : A \times B \rightarrow A' \times B'$ με τιμή $h(a, \beta) = (f(a), g(\beta))$ είναι αμφιμονοσήμαντη και επί, συνεπώς

$$\text{Card } A \times B = \text{Card } A' \times B' = \text{Card } A' \cdot \text{Card } B' \quad \square$$

Παράδειγμα. Είναι

$$\aleph_0 + \aleph_0 = \aleph_0, \quad \aleph_0 \cdot \aleph_0 = \aleph_0$$

Πραγματικά, έστω A το σύνολο των αρτίων και B το σύνολο των περιττών φυσικών. Έχουμε $\mathbb{N} \sim A$, γιατί η συνάρτηση $f : \mathbb{N} \rightarrow A$ με τιμή $f(n) = 2n$ είναι αμφιμονοσήμαντη και επί και $\mathbb{N} \sim B$, γιατί η συνάρτηση $g : \mathbb{N} \rightarrow B$ με τιμή $g(n) = 2n+1$ είναι αμφιμονοσήμαντη και επί. Επειδή $A \cup B = \mathbb{N}$ και $A \cap B = \emptyset$, έπεται $\aleph_0 + \aleph_0 = \aleph_0$. Η σχέση $\aleph_0 \cdot \aleph_0 = \aleph_0$ προκύπτει από την πρότ. 8§ 10.

Πόρισμα. Αν A, B είναι πεπερασμένα σύνολα ξένα μεταξύ τους,

$$|A \cup B| = |A| + |B|$$

$$|A \times B| = |A| \cdot |B|$$

Ανεξάρτητα της προηγούμενης πρότασης οι παραπάνω ιδιότητες για τα πεπερασμένα σύνολα αποδεικνύονται ως εξής:

Πρόταση 2. Αν $|A| = n$, $|B| = m$, τότε

i) $|A \cup B| = n + m$

ii) $|A \times B| = n \cdot m$

Απόδειξη. i) Έστω $A \sim \mathbb{N}_n$, $B \sim \mathbb{N}_m$, $A \cap B = \emptyset$ και ότι οι συναρτήσεις $f : A \rightarrow \mathbb{N}_n$, $g : B \rightarrow \mathbb{N}_m$ είναι αμφιμονοσήμαντες και επί. Η συνάρτηση $h : A \cup B \rightarrow \mathbb{N}_{m+n}$ με τιμή

$$h(x) = \begin{cases} f(x) & ; x \in A \\ g(x) + n & ; x \in B \end{cases}$$

είναι αμφιμονοσήμαντη και επί. Άρα $|A \cup B| = n + m = |A| + |B|$.

- ii) Κάνουμε επαγωγή ως προς m : Έχουμε

$$A \times (B \cup \{\beta\}) = (A \times B) \cup (A \times \{\beta\})$$

Συνεπώς

$$|A \times (B \cup \{\beta\})| = |A \times B| + |A \times \{\beta\}| = nm + n = n(m+1). \quad \square$$

Πρόταση 3. Αν A, B είναι δύο πεπερασμένα σύνολα, τότε

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Απόδειξη. Εκφράζουμε το σύνολο $A \cup B$ ως ένωση τριών συνόλων που ανά δύο είναι ξένα μεταξύ τους : Έχουμε

$$\begin{aligned} A \cup B &= [(A - A \cap B) \cup (A \cap B)] \cup [(A \cap B) \cup (B - A \cap B)] \\ &= (A - A \cap B) \cup (A \cap B) \cup (B - A \cap B) \end{aligned} \quad (1)$$

Αλλά $|X| = |Y| + |X - Y|$, γιατί $Y \cup (X - Y) = X$ και τα σύνολα $Y, X - Y$ είναι ξένα μεταξύ τους. Συνεπώς από την (1) παίρνουμε

$$\begin{aligned} |A \cup B| &= |A - A \cap B| + |A \cap B| + |B - A \cap B| \\ &= (|A| - |A \cap B|) + |A \cap B| + (|B| - |A \cap B|) \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

□

Εφαρμογή. Το 47% του πληθυσμού μιας περιοχής ψήφισε σε τοπικές εκλογές και το 75% σε εθνικές εκλογές. Ποιό το ελάχιστο ποσοστό που ψήφισε και στις δύο εκλογές;

Απάντηση. Έστω A, B τα σύνολα των ανθρώπων που ψήφισαν στις τοπικές αντίστοιχα γενικές εκλογές. Αν n ο συνολικός αριθμός των ψηφισάντων, έχουμε

$$|A \cup B| \leq n \text{ και } |A \cup B| = |A| + |B| - |A \cap B|$$

Συνεπώς $n \geq \frac{47n}{100} + \frac{75n}{100} - |A \cap B|$. Άρα $|A \cap B| \geq \frac{22n}{100}$, δηλαδή το ζητούμενο ποσοστό είναι 22%.

Ορισμός 2. $\text{Card } A^{\text{Card } B} = \text{Card } (A^B)$

Είναι εύκολο ν' αποδείξουμε ότι ο πληθάνριθμος του δεύτερου μέλους είναι ανεξάρτητος των A, B :

Έστω $A_1 \sim A$ και $B_1 \sim B$. Υπάρχουν συναρτήσεις $f: A_1 \rightarrow A$, $g: B_1 \rightarrow B$ αμφιμονοσήμαντες και επί. Έστω $h \in A^B$. Τότε $f^{-1} \circ h \circ g \in A_1^{B_1}$, αφού $B_1 \xrightarrow{g} B \xrightarrow{h} A \xrightarrow{f^{-1}} A_1$. Η συνάρτηση $h \xrightarrow{f^{-1} \circ h \circ g} A_1^{B_1}$ του A^B στο $A_1^{B_1}$ είναι αμφιμονοσήμαντη και επί. Άρα $A^B \sim A_1^{B_1}$. □

Αποδεικνύουμε την ισότητα $\text{Card } A^{\text{Card } B} = \text{Card } (A^B)$ για πεπερασμένα σύνολα:

Πρόταση 4. Έστω A, B δύο πεπερασμένα σύνολα, $|A| = m, |B| = n$. Τότε $|A^B| = m^n$.

Απόδειξη. Κάνουμε επαγωγή ως προς n : Για $n = 1$, έχουμε $B = \{q\}$ και το πλήθος των συναρτήσεων $f : B \rightarrow A = \{a_1, a_2, \dots, a_m\}$ είναι m . Υποθέτουμε ότι το συμπέρασμα ισχύει για n . Έστω $B = \{\beta_1, \beta_2, \dots, \beta_{n+1}\}$ ένα σύνολο με $n+1$ στοιχεία και μια συνάρτηση $f : B \rightarrow A$. Η συνάρτηση f ορίζεται από τον περιορισμό της $\bar{f}$ στο σύνολο $B - \{\beta_{n+1}\} \equiv B_1$ και την τιμή της $f(\beta_{n+1}) \in A$. Για κάθε $\bar{\sigma} : B_1 \rightarrow A$ υπάρχουν m συναρτήσεις $\sigma : B \rightarrow A$ με περιορισμό επί του B_1 την $\bar{\sigma}$. Συνεπώς

$$|A^B| = |A^{B_1}| \cdot m = m^n \cdot m = m^{n+1}.$$

Άρα η πρόταση αποδείχτηκε. $\square$

Πόρισμα. Το πλήθος των εσωτερικών νόμων επί ενός συνόλου A με n στοιχεία είναι n^{n^2} .

Γιατί οι εσωτερικοί νόμοι επί του A είναι οι συναρτήσεις $f : A \times A \rightarrow A$, συνεπώς το πλήθος τους είναι $|A^{A \times A}| = |A|^{|A \times A|} = n^{n^2}$.

Διάταξη πληθαρίσμων

Έστω A, B δύο σύνολα με πληθάριθμους a, β . Ορίζουμε

$$\begin{aligned} a \leq \beta &\Leftrightarrow A \sim B_1, \text{ όπου } B_1 \subseteq B \\ a < \beta &\Leftrightarrow a \leq \beta \text{ και } A \not\sim B \end{aligned}$$

Προφανώς η σχέση $\leq$ είναι αυτοπαθητική και μεταβατική. Το θεώρημα που ακολουθεί αποδεικνύει ότι είναι και αντισυμμετρική. Άρα η σχέση $\leq$ είναι μια σχέση διάταξης μεταξύ των πληθαρίσμων.

Θεώρημα (Bernstein). Αν a, β είναι πληθάριθμοι και $a \leq \beta, \beta \leq a$, τότε $a = \beta$.

Απόδειξη.* Έστω X, Y δύο σύνολα με $\text{Card } X = a, \text{Card } Y = \beta$. Αφού $a \leq \beta$ και $\beta \leq a$, υπάρχουν δύο αμφιμονοσήμαντες συναρτήσεις $f : X \rightarrow Y$ και $g : Y \rightarrow X$. Θεωρούμε τη συνάρτηση $\varphi : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ με τιμή $\varphi(A) = X - g(Y - f(A))$. Αν $A \subseteq B \subseteq X$, προφανώς $\varphi(A) \subseteq \varphi(B)$. Έστω

$$F = \{A \in \mathcal{P}(X); A \subseteq \varphi(A)\}, \quad T = \bigcup_{A \in F} A.$$

* παραλείπεται σε πρώτη ανάγνωση.

Αν $A \in F$, τότε $A \subseteq T$, συνεπώς $A \subseteq \varphi(A) \subseteq \varphi(T)$ και

$$T = \bigcup_{A \in F} A \subseteq \bigcup_{A \in F} \varphi(A) = \varphi\left(\bigcup_{A \in F} A\right) = \varphi(T)$$

δηλαδή $T \subseteq \varphi(T)$, $\varphi(T) \subseteq \varphi(\varphi(T))$, οπότε $\varphi(T) \in F$, $\varphi(\varphi(T)) \subseteq \varphi(T)$ και άρα $\varphi(T) = T$. Από τον ορισμό της φ παίρνουμε

$$T = X - g(Y - f(T)) \quad , \quad X - T = g(Y - f(T))$$

Η συνάρτηση $h : X \rightarrow Y$ με τιμή

$$h(x) = \begin{cases} f(x) & : x \in T \\ g^{-1}(x) & ; x \in X - T \end{cases}$$

είναι αμφιμονοσήμαντη και επί. □

Για κάθε πληθάρημο υπάρχει μεγαλύτερος πληθάρημος σύμφωνα με το θεώρημα που ακολουθεί:

Θεώρημα (Cantor). Για κάθε σύνολο A ισχύει

$$\text{Card } A < \text{Card } \mathcal{P}(A)$$

Απόδειξη.* Αν $A = \emptyset$, έχουμε $\text{Card } \mathcal{P}(A) = 1 > \text{Card } A = 0$. Έστω $A \neq \emptyset$. Η συνάρτηση $f : A \rightarrow \mathcal{P}(A)$ με τιμή $f(x) = \{x\}$ είναι αμφιμονοσήμαντη, συνεπώς $\text{Card } A \leq \text{Card } \mathcal{P}(A)$. Ας υποθέσουμε ότι $\text{Card } A = \text{Card } \mathcal{P}(A)$. Υπάρχει μια συνάρτηση $g : A \rightarrow \mathcal{P}(A)$ αμφιμονοσήμαντη και επί. Έστω $B = \{x \in A; x \notin g(x)\}$. Αφού η g είναι επί, έχουμε $B = g(y)$ με $y \in A$. Υπάρχουν δύο δυνατότητες: i) $y \in B$ ii) $y \notin B$. Στην πρώτη περίπτωση $y \notin g(y) = B$, άτοπο και στη δεύτερη $y \in g(y) = B$, πάλι άτοπο. □

Πόρισμα. Υπάρχουν άπειροι πληθάρημοι $> \aleph_0$. Γιατί

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \dots$$

Θεώρημα. Για κάθε σύνολο E , $\mathcal{P}(E) \sim \{0, 1\}^E$.

Απόδειξη. Για κάθε υποσύνολο A του E ορίζουμε μια συνάρτηση $f_A : E \rightarrow \{0, 1\}$ ως εξής:

$$f_A(x) = \begin{cases} 1 & ; x \in A \\ 0 & ; x \in E - A \end{cases}$$

* παραλείπεται σε πρώτη ανάγνωση.

Η συνάρτηση f_A λέγεται **χαρακτηριστική** συνάρτηση του A . Η ορολογία δικαιολογείται από το γεγονός ότι δύο υποσύνολα A, B του E είναι ίσα τότε και μόνο, όταν $f_A = f_B$. Πραγματικά, αν $A \neq B$, υπάρχει στοιχείο x που ανήκει στο ένα μόνο από τα σύνολα A, B , έστω το A . Τότε $f_A(x) = 1, f_B(x) = 0$ δηλαδή $f_A \neq f_B$. Προφανώς ισχύει και το αντίστροφο. Η συνάρτηση $h : \mathcal{P}(E) \rightarrow \{0, 1\}^E$ με τιμή $h(A) = f_A$ είναι συνεπώς αμφιμονοσήμαντη. Είναι και επί του $\{0, 1\}^E$, γιατί, αν $g : E \rightarrow \{0, 1\}$, έχουμε $f_{g^{-1}(1)} = g$. Πραγματικά, αν $x \in g^{-1}(1)$, είναι $g(x) = 1 = f_{g^{-1}(1)}(x)$ και αν $x \notin g^{-1}(1)$, $g(x) = 0 = f_{g^{-1}(1)}(x)$. Έτσι $f_{g^{-1}(1)} = g$ και το συμπέρασμα αποδείχτηκε. $\square$

Αποδεικνύεται ότι $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$. Συνεπώς $\aleph_0 < c$. Ο Cantor θεμελιωτής της θεωρίας συνόλων, έθεσε το ερώτημα αν υπάρχει πληθάριθμος a με $\aleph_0 < a < c$. Μέχρι σήμερα δεν έχει αποδειχτεί κάτι τέτοιο. Η υπόθεση ότι δεν υπάρχει πληθάριθμος μεταξύ του πληθαρίθμου των φυσικών αριθμών και του συνόλου των πραγματικών αριθμών είναι γνωστή ως "υπόθεση του συνεχούς". Το 1963 ο Cohen απέδειξε ότι οι υποθέσεις "μεταξύ των πληθαρίθμων των συνόλων

$$\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})) = \mathcal{P}^2(\mathbb{N}), \dots, \mathcal{P}^n(\mathbb{N}), \dots$$

δεν υπάρχουν άλλοι πληθάριθμοι" είναι ανεξάρτητες των συνήθων αξιωμάτων της θεωρίας των συνόλων.

12. ΒΑΣΙΚΕΣ ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ

Στην προσπάθεια ταξινόμησης της γνώσης διακρίνουμε συστήματα αντικειμένων, καταγράφουμε τις ιδιότητες των μοντέλων αυτών και στη συνέχεια αναφερόμαστε σ' αυτά κάθε φορά που θέλουμε να μελετήσουμε άλλα συστήματα που παρουσιάζουν ομοιότητες.

Θα θεωρήσουμε συστήματα αντικειμένων που αν και έχουν πολλές κοινές ιδιότητες με τα συστήματα των ακεραίων ή πραγματικών αριθμών και με τα διανύσματα, είναι τελείως διάφορα.

Τα αλγεβρικά μοντέλα που συναντάμε συχνά και πρέπει κατ' αρχή να μελετήσουμε είναι οι ομάδες, οι δακτύλιοι, τα σώματα και οι διανυσματικοί χώροι.

Η προσθετική δομή $(\mathbb{Z}, +)$ των ακεραίων αριθμών παρουσιάζει μεταξύ των άλλων τις παρακάτω ιδιότητες

1. Αν $x, y \in \mathbb{Z}$, $x + y \in \mathbb{Z}$
2. $x + (y + z) = (x + y) + z$
3. Υπάρχει ένα στοιχείο "0" τέτοιο, ώστε $x + 0 = 0 + x = x$ για κάθε $x \in \mathbb{Z}$.
4. Για κάθε ακέραιο x υπάρχει ακέραιος x' τέτοιος, ώστε $x + x' = x' + x = 0$

Μια δομή $(G, *)$ λέγεται **ομάδα**, αν παρουσιάζει τις ίδιες ακριβώς ιδιότητες 1-4 με την πρόσθεση των ακεραίων, αν δηλαδή

- i) $x, y \in G \Rightarrow x * y \in G$
- ii) $x * (y * z) = (x * y) * z$
- iii) Υπάρχει $e \in G$ τέτοιο, ώστε $x * e = e * x = x$ για κάθε $x \in G$
- iv) Για κάθε $x \in G$, υπάρχει $x' \in G$ τέτοιο, ώστε $x * x' = x' * x = e$.

Παραδείγματα. Οι παρακάτω δομές είναι ομάδες

- 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$
- 2) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$
- 3) $(\mathbb{Z}_m, +)$, $(\mathcal{P}(E), \Delta)$
- 4) $(S_E, \circ)$, όπου S_E το σύνολο των συναρτήσεων $f : E \rightarrow E$ που αντιστρέφονται (είναι αμφιμονοσήμαντες και επί) και ο η σύνθεση μεταξύ συναρτήσεων.
- 5) $(M_{n \times n}, \cdot)$, όπου $M_{n \times n}$ είναι οι τετραγωνικοί πραγματικοί πίνακες $n \times n$ και $A \cdot B$ το γινόμενο δύο πινάκων $A, B \in M_{n \times n}$.

Μια ομάδα $(G, *)$ λέγεται **αβελιανή** ή **αντιμεταθετική**, αν για όλα τα $a, \beta \in G$

$$a * \beta = \beta * a$$

Τα παραδείγματα 1-3 είναι ομάδες αντιμεταθετικές, ενώ τα 4-5 είναι ομάδες μη αντιμεταθετικές (όταν το E έχει περισσότερα από δύο στοιχεία και $n \geq 2$).

Το σύνολο των ακεραίων ως προς την πρόσθεση και τον πολλαπλασιασμό $(\mathbb{Z}, +, \cdot)$ έχει μεταξύ των άλλων τις εξής ιδιότητες:

- i) $(\mathbb{Z}, +)$ είναι ομάδα αντιμεταθετική
- ii) $x, y \in \mathbb{Z} \Rightarrow x \cdot y \in \mathbb{Z}$
- iii) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- iv) $x \cdot (y + z) = x \cdot y + y \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z$

Μια δομή $(R, \#, \bullet)$ λέγεται **δακτύλιος**, αν έχει τις ιδιότητες i-iv, αν δηλαδή:

- I. $(R, \#)$ είναι ομάδα αντιμεταθετική.

II. $(R, \bullet)$ είναι δομή ενός εσωτερικού νόμου προσεταιριστικού:

$$\begin{aligned} x, y \in R &\Rightarrow x \bullet y \in R \\ x \bullet (y \bullet z) &= (x \bullet y) \bullet z \end{aligned}$$

III. Ο δεύτερος νόμος $\bullet$ είναι επιμεριστικός ως προς τον πρώτο:

$$x \bullet (y \# z) = x \bullet y \# x \bullet z, (x \# y) \bullet z = x \bullet z \# y \bullet z$$

Ο δακτύλιος $(R, \#, \bullet)$ λέγεται μοναδιαίος, αν ο δεύτερος νόμος έχει ουδέτερο, αν δηλαδή υπάρχει $e \in R$, τέτοιο, ώστε για κάθε $x \in R$

$$x \bullet e = e \bullet x = x$$

Λέγεται αντιμεταθετικός, αν $x \bullet y = y \bullet x$ για όλα τα $x, y \in R$.

Παραδείγματα.

- 1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
- 2) $(\mathbb{Z}_m, +, \cdot)$, $(\mathcal{P}(E), \Delta, \cap)$
- 3) $(M_{n \times n}, +, \cdot)$, όπου $M_{n \times n}$ οι πραγματικοί πίνακες $n \times n$ και $+$, $\cdot$ η πρόσθεση και ο πολλαπλασιασμός αυτών.

Το σύνολο των πραγματικών αριθμών $(\mathbb{R}, +, \cdot)$ είναι ένας μοναδιαίος δακτύλιος και για κάθε $x \neq 0$ υπάρχει $x' \in \mathbb{R}$ τέτοιο, ώστε $x \cdot x' = x' \cdot x = 1$. Ένας δακτύλιος $(R, +, \cdot)$ με τις δύο αυτές ιδιότητες λέγεται σώμα. Έτσι σώμα λέγεται ένας δακτύλιος $(K, +, \cdot)$, ο οποίος είναι μοναδιαίος $\neq (0)$ και κάθε $x \neq 0$ έχει αντίστροφο στοιχείο ως προς το δεύτερο νόμο. Το μοναδιαίο στοιχείο του νόμου " $\cdot$ " λέγεται μονάδα του σώματος. Αν ο δακτύλιος είναι αντιμεταθετικός, το σώμα λέγεται αντιμεταθετικό.

Παραδείγματα.

- 1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
- 2) $(\mathbb{Z}_3, +, \cdot)$, $(\mathbb{Z}_5, +, \cdot)$, γενικά $(\mathbb{Z}_m, +, \cdot)$ με m πρώτο αριθμό (βλ. Κεφ. 1§)
- 3) $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, όπου $\mathbb{Q}(\sqrt{2}) = \{a + \beta\sqrt{2}; a, \beta \in \mathbb{Q}\}$ και $+$, $\cdot$ η πρόσθεση και ο πολλαπλασιασμός πραγματικών αριθμών.
- 4) Το σύνολο των πινάκων

$$\begin{pmatrix} a & \beta \\ -\beta & a \end{pmatrix}, \quad a, \beta \in \mathbb{R}$$

είναι σώμα αντιμεταθετικό.

Μέχρι τώρα είδαμε δομές που αποτελούνται από ένα σύνολο και ένα ή δύο εσωτερικούς νόμους επί του εαυτού του. Θα θεωρήσουμε στη συνέχεια δομές που αποτελούνται από ένα εσωτερικό και ένα εξωτερικό νόμο.

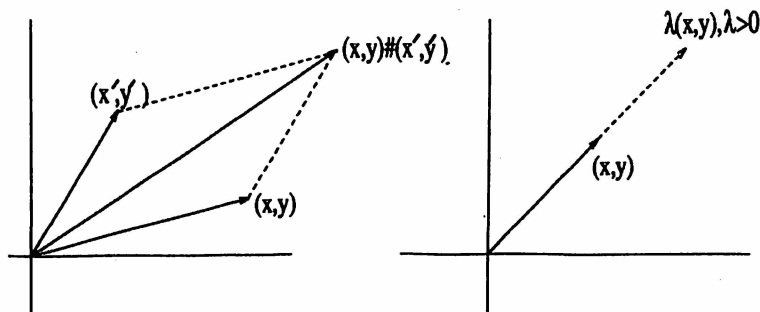
Έστω $(V, +)$ μια δομή, K ένα σώμα και $*$ μια συνάρτηση του $K \times V$ στο V της οποίας την τιμή στο $(\lambda, x) \in K \times V$ συμβολίζουμε με $\lambda * x$. Μια τέτοια συνάρτηση λέγεται εξωτερικός νόμος επί του V με τελεστές τα στοιχεία του K (§6).

Η δομή $(V, \#, *)$ λέγεται *** διανυσματικός χώρος** (αριστερά) επί του σώματος $(K, +, \cdot)$, αν

- I. $(V, \#)$ είναι ομάδα αντιμεταθετική
- II. Ο εξωτερικός νόμος $*$ έχει τις ιδιότητες
 - i) $\lambda * (x \# y) = (\lambda * x) \# (\lambda * y)$
 - ii) $(\lambda + \mu) * x = (\lambda * x) \# (\mu * x)$
 - iii) $\lambda * (\mu * x) = (\lambda \cdot \mu) * x$
 - iv) $1 * x = x$, όπου 1 η μονάδα του σώματος.

Παράδειγμα 1. Έστω $V = \mathbb{R} \times \mathbb{R}$ με εσωτερικό νόμο $(x, y) \# (x', y') = (x + x', y + y')$, $K = \mathbb{R}$ και ο εξωτερικός νόμος $*$ επί του V που ορίζεται από την ισότητα $\lambda * (x, y) = (\lambda \cdot x, \lambda \cdot y)$. Είναι εύκολο να επαληθεύσουμε ότι $(V, \#, *)$ είναι ένας διανυσματικός χώρος επί του σώματος $\mathbb{R}$.

Ο διανυσματικός αυτός χώρος ταυτίζεται με το σύνολο των ελεύθερων διανυσμάτων του επιπέδου: Ο εσωτερικός νόμος $\#$ είναι η πρόσθεση των διανυσμάτων και ο εξωτερικός νόμος $*$ το γινόμενο πραγματικού αριθμού επί διάνυσμα.



Παράδειγμα 2. Έστω $(K, +, \cdot)$ ένα σώμα, n ένας φυσικός και $V = K^n = K \times K \times \cdots \times K$. Ορίζουμε ένα εσωτερικό νόμο $\#$ επί του V και

* περισσότερα βλ. ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ Δ. Στρατηγόπουλου

ένα εξωτερικό * από τις ισότητες

$$(x_1, x_2, \dots, x_n) \# (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$\lambda * (x_1, x_2, \dots, x_n) = (\lambda \cdot x_1, \lambda \cdot x_2, \dots, \lambda \cdot x_n)$$

Εύκολα επαληθεύουμε ότι $(K^n, \#, *)$ είναι ένας διανυσματικός χώρος επί του σώματος K . Τα στοιχεία του K^n είναι πίνακες $1 \times n$. Το παράδειγμα αυτό γενικεύεται ως εξής:

Παράδειγμα 3. Έστω V το σύνολο των πινάκων $m \times n$ με στοιχεία από ένα σώμα $(K, +, \cdot)$. Το V ως προς την πρόσθεση των πινάκων και το γινόμενο στοιχείου του K επί πίνακα, είναι διανυσματικός χώρος επί του σώματος K .

13. ΑΝΤΙΝΟΜΙΕΣ, ΑΞΙΩΜΑΤΑ ΣΤΗ ΘΕΩΡΙΑ ΣΥΝΟΛΩΝ

Ο Cantor (1845-1918) θεωρείται ο θεμελιωτής της θεωρίας των συνόλων, η οποία παίζει μεγάλο ρόλο σε όλους σχεδόν τους κλάδους των Μαθηματικών.

Γρήγορα παρατηρήθηκαν, πρώτα από τον Burali-Forti το 1897, αντινομίες που ονομάστηκαν **παράδοξα** της θεωρίας.

Είναι όμως δυνατόν να εξαλείψουμε τις αντινομίες αυτές με αυστηρή αξιωματική θεμελίωση της θεωρίας συνόλων. Θ' αναφέρουμε δύο παράδοξα:

Παράδοξο Cantor. Έστω E το σύνολο όλων των συνόλων. Κάθε υποσύνολο του E είναι στοιχείο του E . Συνεπώς $\mathcal{P}(E) \subseteq E$ και άρα $|\mathcal{P}(E)| \leq |E|$. Αυτό αντιφάσκει με το θεώρημα Cantor κατά το οποίο $|E| < |\mathcal{P}(E)|$.

Παράδοξο Russel. Έστω E το σύνολο όλων των συνόλων που δεν είναι στοιχεία του εαυτού τους, δηλαδή $E = \{X; X \notin X\}$. Ερώτηση: $E \in E$ ή $E \notin E$; Αν $E \notin E$, τότε από τον ορισμό του E , $E \in E$. Αν $E \in E$, τότε πάλι από τον ορισμό του E , $E \notin E$. Άρα σε κάθε περίπτωση καταλήγουμε σε αντίφαση.

Το παράδοξο αυτό του Russel είναι ανάλογο του εξής λαϊκού παραδόξου: Σ' ένα χωριό υπάρχει ένας κουρέας, ο οποίος κουρεύει μόνο όσους δεν κουρεύονται μόνοι τους. Ποιος κουρεύει τον κουρέα;

Γρήγορα αναγνωρίστηκε η ανάγκη να περιληφθεί στο σύνολο των αξιωμάτων της θεωρίας των συνόλων ένα αξίωμα, γνωστό σαν αξίωμα **επιλογής** χωρίς το οποίο πολλά συμπεράσματα μένουν αναπόδεικτα. Αυτό το αξίωμα "χονδρικά" μας λέει το εξής: Αν $(A_i)_{i \in I}$ είναι μια μη κενή οικογένεια υποσυνόλων του B , υπάρχει μια συνάρτηση $f : \{A_i\}_{i \in I} \rightarrow B$ με $f(A_i) \in A_i$ για κάθε $i \in I$.

Μερικές συνέπειες του αξιώματος αυτού είναι τα παρακάτω θεωρήματα:

Θεώρημα καλής διάταξης Σε κάθε σύνολο υπάρχει μια σχέση καλής διάταξης.

Θεώρημα ή λήμμα Zorn Έστω X μια μη κενή οικογένεια μερικά διατεταγμένων συνόλων στην οποία κάθε ολικά διατεταγμένο υποσύνολο έχει άνω φράγμα στο X . Τότε το X περιέχει ένα τουλάχιστο στοιχείο *maximal*. Βασικό θεώρημα στη θεωρία συνόλων είναι το εξής:

Θεώρημα Είναι ισοδύναμα τα εξής:

- i) Αξίωμα επιλογής
- ii) Θεώρημα καλής διάταξης
- iii) Λήμμα Zorn

Τα θέματα αυτά είναι αρκετά δύσκολα και αποτελούν το περιεχόμενο ειδικού μαθήματος που δεν απευθύνεται σε πρωτοετείς φοιτητές.

14. ΑΛΓΕΒΡΑ BOOLE

Θα ορίσουμε στη γενική περίπτωση, την 'Αλγεβρα Boole. Μερικές περιπτώσεις, είναι η 'Αλγεβρα των συνόλων, Η Λογική των προτάσεων και η άλγεβρα των κυκλωμάτων διακοπών.

Ορισμός 1. 'Αλγεβρα Boole είναι μια δομή $(K, \wedge, \vee, ')$ που αποτελείται από ένα σύνολο K , δύο διμελείς εσωτερικούς νόμους $\wedge, \vee$ και ένα μονομελή $(')$ με τις παρακάτω ιδιότητες:

1. Προσεταιριστική ιδιότητα των νόμων $\wedge, \vee$:

$$A \wedge (B \wedge \Gamma) = (A \wedge B) \wedge \Gamma \quad , \quad A \vee (B \vee \Gamma) = (A \vee B) \vee \Gamma$$

2. Αντιμεταθετική ιδιότητα των νόμων $\wedge, \vee$

$$A \wedge B = B \wedge A \quad , \quad A \vee B = B \vee A$$

3. Επιμεριστική του ενός των νόμων $\wedge, \vee$ ως προς τον άλλο

$$A \wedge (B \vee \Gamma) = (A \wedge B) \vee (A \wedge \Gamma) \quad , \quad A \vee (B \wedge \Gamma) = (A \vee B) \wedge (A \vee \Gamma)$$

4. Υπάρχουν ουδέτερα για τους εσωτερικούς νόμους $\wedge, \vee$

$$A \vee 0 = A \quad , \quad A \wedge 1 = A$$

Το ουδέτερο του νόμου $\vee$ λέγεται **μηδέν** της 'Άλγεβρας Boole και του νόμου $\wedge$ **μονάδα**.

5. Ο μονομελής εσωτερικός νόμος $A \mapsto A'$ έχει τις ιδιότητες:

$$A \wedge A' = 0, \quad A \vee A' = 1.$$

Το στοιχείο A' λέγεται **συμπλήρωμα** του A .

Πρόταση 1. Υπάρχει ένας μόνο μονομελής εσωτερικός νόμος, με τις ιδιότητες 5, δηλαδή το συμπλήρωμα A' του A ορίζεται μονοσήμαντα.

Απόδειξη. Έστω ότι B, Γ είναι συμπληρώματα του A' . Τότε

$$A \wedge B = A \wedge \Gamma = 0 \quad \text{και} \quad A \vee B = A \vee \Gamma = 1$$

Έχουμε προφανώς

$$\begin{aligned} B &= B \vee 0 = B \vee (A \wedge \Gamma) = (B \vee A) \wedge (B \vee \Gamma) \\ &= (A \vee B) \wedge (B \vee \Gamma) = 1 \wedge (B \vee \Gamma) = B \vee \Gamma \end{aligned}$$

και όμοια $\Gamma = \Gamma \vee B$. Συνεπώς $B = \Gamma$. □

Παρατήρηση 1. Αν στα αξιώματα της 'Άλγεβρας Boole εναλλάξουμε τους νόμους $\wedge, \vee$ και τις μονάδες τους $0, 1$, παίρνουμε τα ίδια αξιώματα, συνεπώς μια άλγεβρα Boole. Έτσι αν μια πρόταση προκύπτει από τα αξιώματα Boole, θα ισχύει και η πρόταση που προκύπτει από αυτή με την εναλλαγή των νόμων $\wedge, \vee$ και των μονάδων τους. Η ιδιότητα αυτή λέγεται **αρχή του δυϊσμού**.

Παράδειγμα 1. Για κάθε σύνολο E , $(\mathcal{P}(E), \cap, \cup, ')$ είναι μια άλγεβρα Boole.

Παράδειγμα 2. Έστω $E = \{0, 1\}$. Οι παρακάτω πίνακες ορίζουν μια άλγεβρα Boole

A	B	$A \wedge B$	$A \vee B$	A	A'
0	0	0	0	0	1
0	1	0	1	1	0
1	0	0	1		
1	1	1	1		

Παράδειγμα 3. (Θεωρούμε γνωστές τις έννοιες του μέγιστου κοινού διαιρέτη μ.κ.δ (a, b) και ελάχιστου κοινού πολλαπλάσιου ε.κ.π (a, b) δύο

φυσικών αριθμών). Έστω $K = \{1, 2, 5, 10, 11, 22, 55, 110\}$ το σύνολο των θετικών διαιρετών του 110, και $x' = \frac{110}{x}$ για κάθε $x \in K$. Η δομή $(K, \mu.χ.δ(a, \beta), \varepsilon.χ.π(a, \beta), ')$ είναι μια άλγεβρα Boole.

Απόδειξη. Το μηδέν της άλγεβρας είναι το στοιχείο $1 \in K$, γιατί $\varepsilon.χ.π(1, x) = x$ για κάθε $x \in K$. Η μονάδα της άλγεβρας είναι το 110, γιατί $\mu.χ.δ(110, x) = x$ για κάθε $x \in K$. Αποδεικνύουμε την επιμεριστικότητα του νόμου "μ.χ.δ" ως προς το νόμο "ε.χ.π", ότι δηλαδή

$$\mu.χ.δ(x, \varepsilon.χ.π(y, z)) = \varepsilon.χ.π(\mu.χ.δ(x, y), \mu.χ.δ(x, z)) \quad (1)$$

Είναι εύκολο να δούμε ότι αυτή είναι η επιμεριστική ιδιότητα που αναφέραμε, αν γράψουμε $\mu.χ.δ(a, \beta) = a * \beta$ και $\varepsilon.χ.π(a, \beta) = aT\beta$ οπότε η (1) γράφεται $x * (yTz) = (x * y)T(x * z)$.

Έστω ότι

$$x = 2^{a_2} 5^{a_5} 11^{a_{11}}, \quad y = 2^{\beta_2} 5^{\beta_5} 11^{\beta_{11}}, \quad z = 2^{\gamma_2} 5^{\gamma_5} 11^{\gamma_{11}},$$

με $0 \leq a_i, 0 \leq \beta_i, 0 \leq \gamma_i$. Τότε

$$\varepsilon.χ.π(y, z) = 2^{\max(\beta_2, \gamma_2)} 5^{\max(\beta_5, \gamma_5)} 11^{\max(\beta_{11}, \gamma_{11})}$$

και

$$\mu.χ.δ(x, \varepsilon.χ.π(y, z)) = 2^{\min(a_2, \max(\beta_2, \gamma_2))} 5^{\min(a_5, \max(\beta_5, \gamma_5))} 11^{\min(a_{11}, \max(\beta_{11}, \gamma_{11}))}$$

Το δεύτερο μέλος της (1) γράφεται

$$\begin{aligned} \varepsilon.χ.π\left(2^{\min(a_2, \beta_2)} 5^{\min(a_5, \beta_5)} 11^{\min(a_{11}, \beta_{11})}, 2^{\min(a_2, \gamma_2)} 5^{\min(a_5, \gamma_5)} 11^{\min(a_{11}, \gamma_{11})}\right) \\ = 2^{\max(\min(a_2, \beta_2), \min(a_2, \gamma_2))} 5^{\max(\min(a_5, \beta_5), \min(a_5, \gamma_5))} 11^{\max(\min(a_{11}, \beta_{11}), \min(a_{11}, \gamma_{11}))} \end{aligned}$$

Επειδή για $p = 2, 5, 11$ είναι

$$\min(a_p, \max(\beta_p, \gamma_p)) = \max(\min(a_p, \beta_p), \min(a_p, \gamma_p))$$

η (1) ισχύει. Ανάλογα αποδεικνύεται και η επιμεριστικότητα του νόμου "ε.χ.π" ως προς το νόμο "μ.χ.δ".

Οι υπόλοιπες ιδιότητες προκύπτουν εύκολα. □

Θεώρημα 1. Έστω $(K, \wedge, \vee, ')$ μια άλγεβρα Boole και $A, B, \Gamma \in K$. Τότε

- i) $A \wedge 0 = 0$, $A \vee 1 = 1$
- ii) $A \wedge (A \vee B) = A$, $A \vee (A \wedge B) = A$
- iii) $A \wedge A = A$, $A \vee A = A$
- iv) $(A \wedge B)' = A' \vee B'$, $(A \vee B)' = A' \wedge B'$
- v) $(A')' = A$

Απόδειξη. i) $A \wedge 0 = (A \wedge 0) \vee 0 = (A \wedge 0) \vee (A \wedge A') = A \wedge (0 \vee A') = A \wedge A' = 0$

Η δεύτερη σχέση προκύπτει με την αρχή του διϊσμού:

$$A \vee 1 = (A \vee 1) \wedge 1 = (A \vee 1) \wedge (A \vee A') = A \vee (1 \wedge A') = A \vee A' = 1$$

- ii) $A \wedge (A \vee B) = (A \vee 0) \wedge (A \vee B) = A \vee (0 \wedge B) = A \vee 0 = A$

Ανάλογα αποδεικνύεται η δεύτερη σχέση

- iii) $A = A \wedge 1 = A \wedge (A \vee A') = (A \wedge A) \vee (A \wedge A') = A \wedge A \vee 0 = A \wedge A$

- iv) Θ' αποδείξουμε ότι $A' \wedge B'$ είναι $(A \wedge B)'$. Έχουμε

$$\begin{aligned} (A \wedge B) \wedge (A' \vee B') &= [(A \wedge B) \wedge A'] \vee [(A \wedge B) \wedge B'] \\ &= [(A \wedge A') \wedge B] \vee [A \wedge (B \wedge B')] \\ &= [0 \wedge B] \vee [A \wedge 0] \\ &= 0 \vee 0 \\ &= 0 \end{aligned}$$

και

$$\begin{aligned} (A \wedge B) \vee (A' \vee B') &= [A \vee (A' \vee B')] \wedge [B \vee (A' \vee B')] \\ &= [(A \vee A') \vee B'] \wedge [(B \vee B') \vee A'] \\ &= [(1 \vee B') \wedge [1 \vee A']] \\ &= 1 \wedge 1 \\ &= 1 \end{aligned}$$

Επειδή το συμπλήρωμα A' ορίζεται μονοσήμαντα από το A (πρότ.1), έπεται το συμπέρασμα.

Η δεύτερη σχέση προκύπτει με την αρχή του διϊσμού.

- v) Προκύπτει από τον ορισμό και το μονοσήμαντο του συμπληρώματος. $\square$

Διάταξη σε άλγεβρα Boole

Στην άλγεβρα των συνόλων, που όπως είδαμε είναι μια άλγεβρα Boole, η σχέση του "περιέχεσθαι", $\subseteq$ είναι μια σχέση μερικής διάταξης. Προφανώς

$$A \subseteq B \Leftrightarrow A \cap B = A$$

Η ιδιότητα αυτή μας οδηγεί στον ορισμό μιας σχέσης διάταξης $\leq$ σε τυχούσα άλγεβρα Boole $(\mathcal{B}, \wedge, \vee, ')$: Αν $A, B \in \mathcal{B}$, ορίζουμε

$$A \leq B \Leftrightarrow A \wedge B = A$$

Πρόταση 2. Έστω $(\mathcal{B}, \wedge, \vee, ')$ μια άλγεβρα Boole. Αν $A, B, \Gamma \in \mathcal{B}$, έχουμε

- i) $A \leq A$
- ii) $A \leq B, B \leq A \Rightarrow A = B$
- iii) $A \leq B, B \leq \Gamma \Rightarrow A \leq \Gamma$

Απόδειξη. i) Είναι $A \wedge A = A$, συνεπώς $A \leq A$.

ii) Έχουμε $A \wedge B = A$ και $B \wedge A = B$, συνεπώς $A = A \wedge B = B \wedge A = B$.

iii) Αν $A \wedge B = A$ και $B \wedge \Gamma = B$, έχουμε $A \wedge \Gamma = (A \wedge B) \wedge \Gamma = A \wedge (B \wedge \Gamma) = A \wedge B = A$, άρα $A \leq \Gamma$. $\square$

Πρόταση 3. Σε μια άλγεβρα Boole $(\mathcal{B}, \wedge, \vee, ')$ ισχύουν οι ιδιότητες:

- i) $A \wedge B \leq A$
- ii) $A \leq A \vee B$
- iii) $A \leq \Gamma, B \leq \Gamma \Rightarrow A \vee B \leq \Gamma$
- iv) $A \leq B \Leftrightarrow A \wedge B' = 0$
- v) $0 \leq A \leq 1$ για κάθε $A \in \mathcal{B}$.

Απόδειξη. i) $(A \wedge B) \wedge A = (A \wedge A) \wedge B = A \wedge B$, συνεπώς $A \wedge B \leq A$.

ii) $A \wedge (A \vee B) = A$, δηλαδή $A \leq A \vee B$.

iii) $(A \vee B) \wedge \Gamma = (A \wedge \Gamma) \vee (B \wedge \Gamma) = A \vee B$.

iv) Αν $A \leq B$, τότε $A \wedge B = A$ και $A \wedge B' = A \wedge B \wedge B' = A \wedge 0 = 0$. Αν $A \wedge B' = 0$, τότε

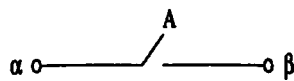
$$A = A \wedge 1 = A \wedge (B \vee B') = (A \wedge B) \vee (A \wedge B') = (A \wedge B) \vee 0 = A \wedge B$$

συνεπώς $A \leq B$.

v) $0 \wedge A = 0$ και $A \wedge 1 = A$ για κάθε $A \in \mathcal{B}$. $\square$

15. ΚΥΚΛΩΜΑΤΑ ΔΙΑΚΟΠΤΩΝ

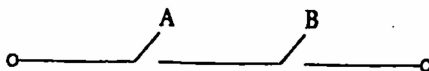
Ένας διακόπτης A συμβολίζεται όπως στο σχήμα 1



σχ.1

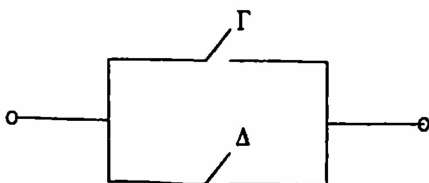
Στο διακόπτη A αντιστοιχίζουμε την τιμή 1, αν είναι κλειστός, αν δηλαδή διέρχεται ρεύμα από το α στο β και την τιμή 0 αν είναι ανοικτός, οπότε δεν διέρχεται ρεύμα από το α στο β .

Οι δύο διακόπτες A, B



σχ.2

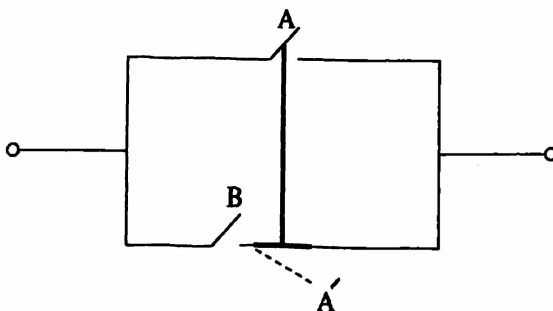
λέμε ότι είναι συνδεδεμένοι σε σειρά. Οι διακόπτες Γ, Δ



σχ.3

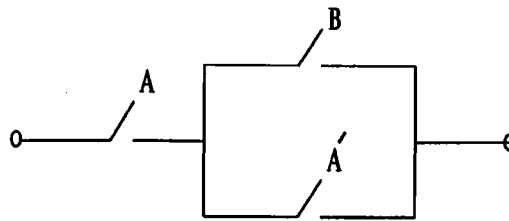
λέμε ότι είναι συνδεδεμένοι παράλληλα. Ένα σύνολο διακοπών συνδεδεμένων σε σειρά ή παράλληλα αποτελούν ένα κύκλωμα διακοπών. Θ' αναλύσουμε απλά κυκλώματα διακοπών με μια είσοδο ρεύματος και μια έξοδο. Το κύκλωμα του σχ.2 γράφεται $A \wedge B$ και του σχ.3 γράφεται $\Gamma \vee \Delta$.

Αν δύο διακόπτες ενός κυκλώματος είναι ταυτόχρονα κλειστοί ή ανοικτοί συμβολίζονται με το ίδιο γράμμα. Αν ένας διακόπτης είναι ανοικτός, όταν ο A είναι κλειστός και αντίστροφα, συμβολίζεται με το γράμμα A' .



σχ.4

Το κύκλωμα του σχήματος 4 γράφεται $(B \wedge A') \vee A$. Το παρακάτω κύκλωμα



σχ.5

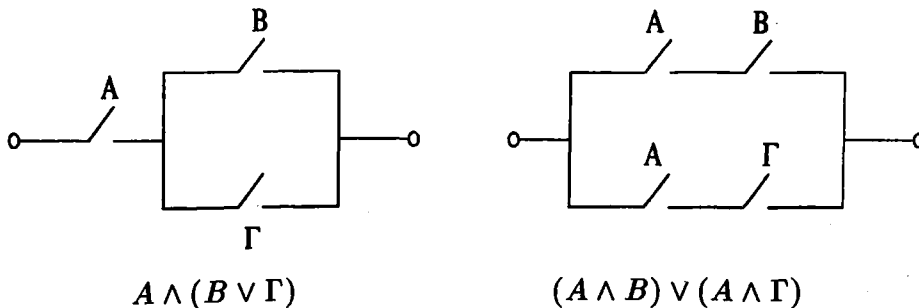
γράφεται $A \wedge (B \vee A')$. Σ' ένα κύκλωμα, από το οποίο περνά ρεύμα, αντιστοιχίζεται το 1, στην αντίθετη περίπτωση το 0.

Οι παρακάτω πίνακες αντιστοιχούν στα κυκλώματα $A \wedge B$ και $A \vee B$

A	B	$A \wedge B$	A	B	$A \vee B$	A	A'
1	1	1	1	1	1	1	0
1	0	0	1	0	1	0	1
0	1	0	0	1	1		
0	0	0	0	0	0		

Πίνακες 6

Δύο κυκλώματα K_1, K_2 που αποτελούνται από τους ίδιους διακόπτες $A, B, \dots$ λέγονται ισοδύναμα και γράφουμε $K_1 = K_2$, αν περνά ρεύμα και από τα δύο ή από κανένα. Τα παρακάτω κυκλώματα είναι ισοδύναμα



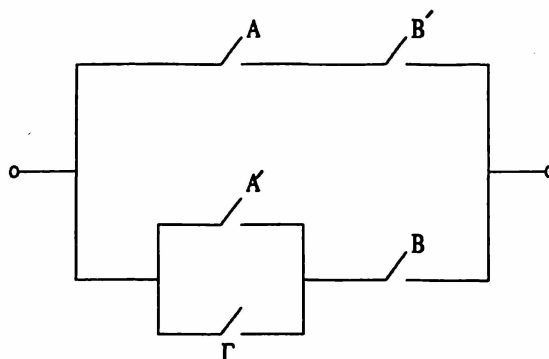
Το γεγονός αυτό εκφράζει την επιμεριστικότητα της σύνδεσης σε σειρά $\wedge$ ως προς την παράλληλη σύνδεση $\vee$.

Με τη βοήθεια των πινάκων 6 αποδεικνύεται το

Θεώρημα 1. Η άλγεβρα των κυκλωμάτων των διακοπών είναι μια άλγεβρα Boole.

Με τη βοήθεια των πινάκων αληθείας βρίσκουμε, αν ένα κύκλωμα διαρρέεται από ρεύμα ή όχι.

Παράδειγμα 1. Θεωρούμε το κύκλωμα



Περιγράφεται από τον τύπο $(A \wedge B') \vee [(A' \vee \Gamma) \wedge B]$ που λέγεται πολυώνυμο Boole.

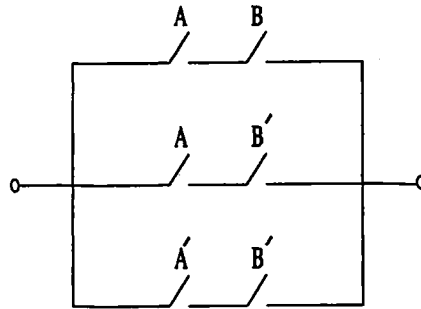
Ο πίνακας αληθείας είναι

A	B	Γ	A'	B'	$A \wedge B'$	$A' \vee \Gamma$	$(A' \vee \Gamma) \wedge B$	$(A \wedge B') \vee [(A' \vee \Gamma) \wedge B]$
1	1	1	0	0	0	1	1	1
1	1	0	0	0	0	0	0	1
1	0	1	0	1	1	1	0	1
1	0	0	0	1	1	0	0	1
0	1	1	1	0	0	1	1	1
0	1	0	1	0	0	1	1	1
0	0	1	1	1	0	1	0	0
0	0	0	1	1	0	1	0	0

Το κύκλωμα διαρρέεται από ρεύμα, όταν

- i) Οι διακόπτες A, B, Γ είναι κλειστοί ή
- ii) οι A, Γ κλειστοί ή
- iii) ο A κλειστός και B ανοικτός ή
- iv) B, Γ κλειστοί ή
- v) ο B κλειστός και A ανοικτός

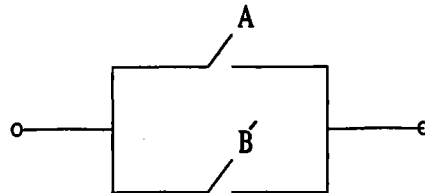
Παράδειγμα 2. Να κατασκευάσετε ένα απλό κύκλωμα ισοδύναμο του κυκλώματος



Λύση. Το αντίστοιχο πολυώνυμο Boole είναι $f = (A \wedge B) \vee (A \wedge B') \vee (A' \wedge B')$. Γράφεται

$$\begin{aligned} f &= [A \wedge (B \vee B')] \vee (A' \wedge B') \\ &= (A \wedge 1) \vee (A' \wedge B') \\ &= A \vee (A' \wedge B') \\ &= (A \vee A') \wedge (A \vee B') \\ &= 1 \wedge (A \vee B') \\ &= A \vee B'. \end{aligned}$$

Άρα ένα ισοδύναμο κύκλωμα είναι το εξής



16. ΔΙΑΤΑΞΕΙΣ, ΜΕΤΑΘΕΣΕΙΣ, ΣΥΝΔΥΑΣΜΟΙ

Έστω n ένας φυσικός. Το γινόμενο $1 \cdot 2 \cdots n$, συμβολίζεται με $n!$ (n παραγοντικό). Ορίζουμε ακόμη $0! = 1$, $1! = 1$.

Θεώρημα 1. Το πλήθος των αμφιμονοσήμαντων συναρτήσεων $f : \{1, 2, \dots, m\} \rightarrow \{1, 2, \dots, n\}$ με $m \leq n$ είναι $\frac{n!}{(n-m)!}$.

Απόδειξη. Θέτουμε $N_m = \{1, 2, \dots, m\}$ και κάνουμε επαγωγή ως προς m . Το πλήθος των συναρτήσεων $f : N_1 = \{1\} \rightarrow N_n$ είναι n και είναι όλες αμφιμονοσήμαντες. Επειδή για $m = 1$, $\frac{n!}{(n-m)!} = \frac{n!}{(n-1)!} = n$, το θεώρημα ισχύει για $m = 1$. Έστω ότι ισχύει για τον φυσικό m . Μια συνάρτηση $f : N_{m+1} \rightarrow N_n$ ορίζεται από τον περιορισμό της $\bar{f}$ στο N_m και την τιμή της

$f(m+1)$. Αν η f είναι αμφιμονοσήμαντη, θα είναι αμφιμονοσήμαντη και η $\bar{f}$. Από μια αμφιμονοσήμαντη συνάρτηση $\bar{f} : \mathbb{N}_m \rightarrow \mathbb{N}_n$ προκύπτουν $n - m$ αμφιμονοσήμαντες συναρτήσεις $f : \mathbb{N}_{m+1} \rightarrow \mathbb{N}_n$ αφού οι δυνατές επιλογές της τιμής $f(m+1)$ είναι $n - m$. Άρα υπάρχουν

$$\frac{n!}{(n-m)!}(n-m) = \frac{n!}{(n-m-1)!} = \frac{n!}{(n-(m+1))!}$$

αμφιμονοσήμαντες συναρτήσεις $f : \mathbb{N}_{m+1} \rightarrow \mathbb{N}_n$. $\square$

Πόρισμα 1. Αν E, F είναι δύο σύνολα με m αντίστοιχα n στοιχεία ($m \leq n$), το πλήθος των αμφιμονοσήμαντων συναρτήσεων $f : E \rightarrow F$ είναι $\frac{n!}{(n-m)!}$.

Γιατί είναι ανεξάρτητο από το είδος των στοιχείων των E, F .

Πόρισμα 2. Το πλήθος των αμφιμονοσήμαντων συναρτήσεων $f : \mathbb{N}_n \rightarrow \mathbb{N}_n$ είναι $n!$

Γιατί $m = n$ και $\frac{n!}{(n-m)!} = \frac{n!}{0!} = n!$

Οι αμφιμονοσήμαντες συναρτήσεις $f : \mathbb{N}_n \rightarrow \mathbb{N}_n$ είναι και επί του $\mathbb{N}_n$. Κάθε τέτοια συνάρτηση λέγεται **μετάθεση** του συνόλου $\mathbb{N}_n$ και είναι ένας τρόπος γραφής των στοιχείων του $\mathbb{N}_n$ σε σειρά.

Μια συνάρτηση $f : \{a_1, a_2, \dots, a_m\} \rightarrow \{\beta_1, \beta_2, \dots, \beta_n\}$ ορίζεται από τις τιμές της

$$f(a_1) = \beta_{i_1}, f(a_2) = \beta_{i_2}, \dots, f(a_m) = \beta_{i_m}$$

Γι' αυτό ταυτίζεται με τον πίνακα

$$\begin{pmatrix} a_1 & a_2 & \dots & a_m \\ \beta_{i_1} & \beta_{i_2} & \dots & \beta_{i_m} \end{pmatrix} = \begin{pmatrix} a_i \\ f(a_i) \end{pmatrix} \quad (1)$$

όπου $\beta_{i_j} \in F = \{\beta_1, \beta_2, \dots, \beta_n\}$. Αν η συνάρτηση f είναι αμφιμονοσήμαντη, έχουμε $\beta_{i_j} \neq \beta_{i_k}$ για $i_j \neq i_k$, συνεπώς στη γραμμή

$$\beta_{i_1} \beta_{i_2} \dots \beta_{i_m}$$

του πίνακα (1) δεν επαναλαμβάνεται το ίδιο στοιχείο του F .

Μια επιλογή m στοιχείων από τα n στοιχεία του F με ορισμένη σειρά λέγεται μια **διάταξη** των n στοιχείων του F ανά m . Μια διάταξη μπορεί να θεωρηθεί σαν μια αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}_m \rightarrow F$.

Το πλήθος των διατάξεων των n στοιχείων ανά m συμβολίζεται με Δ_m^n . Κατά το θεώρημα έχουμε

$$\Delta_m^n = \frac{n!}{(n-m)!}$$

Παράδειγμα 1. Κατά πόσους τρόπους μπορούμε να μοιράσουμε 5 διαφορετικά βιβλία σε 3 μαθητές;

Αν α, β, γ οι μαθητές και $\beta_1, \beta_2, \dots, \beta_5$ τα βιβλία, κάθε τρόπος διανομής αυτών στους μαθητές είναι μια αμφιμονοσήμαντη συνάρτηση $f: \{\alpha, \beta, \gamma\} \rightarrow \{\beta_1, \beta_2, \dots, \beta_5\}$, μια διάταξη δηλαδή των 5 ανά 3. 'Αρα οι διάφοροι τρόποι διανομής των βιβλίων είναι $\Delta_3^5 = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 4 \cdot 5 = 20$.

Θεώρημα 2. Έστω E ένα σύνολο με n στοιχεία. Τα υποσύνολα A του E με m στοιχεία ($m \leq n$) είναι πλήθους

$$\frac{n!}{m!(n-m)!}$$

Απόδειξη. Έστω $A \subseteq E$ με m στοιχεία. Οι διατάξεις των στοιχείων του A ανά m είναι $m!$ και του E είναι $\frac{n!}{(n-m)!}$. Οι $m!$ διατάξεις των στοιχείων του A ορίζουν το ίδιο υποσύνολο A του E . 'Αρα τα διάφορα υποσύνολα του E με m στοιχεία, είναι $\frac{n!}{(n-m)!} : m! = \frac{n!}{m!(n-m)!}$. $\square$

Κάθε υποσύνολο του E με m στοιχεία λέγεται ένας **συνδυασμός** των n ανά m . Το πλήθος των συνδυασμών των n στοιχείων του E ανά m συμβολίζεται με $\binom{n}{m}$. Κατά το θεώρημα έχουμε

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

Παράδειγμα 2. Με 10 αριθμούς πόσες στήλες στο παιχνίδι του ΛΟΤ-ΤΟ συμπληρώνονται;

Κάθε στήλη είναι μια εξάδα από τους 10 αριθμούς. Συνεπώς συμπληρώνονται

$$\binom{10}{6} = \frac{10!}{6!(10-6)!} = \frac{10!}{6!4!} = \frac{7 \cdot 8 \cdot 9 \cdot 10}{1 \cdot 2 \cdot 3 \cdot 4} = 420$$

στήλες.

Πρόταση 1. Ισχύει $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$.

Απόδειξη. Έχουμε

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-1-m)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= (n-1)! \left[\frac{n-m}{m!(n-m)!} + \frac{m}{m!(n-m)!} \right] \\ &= \frac{n!}{m!(n-m)!} = \binom{n}{m} \end{aligned}$$

□

ΑΣΚΗΣΕΙΣ

1. Ν' αποδείξετε ότι

- i) $A \subseteq B \Leftrightarrow A \cap B' = \emptyset$
- ii) $A \cup B = B, A' \cap B = \emptyset \Rightarrow A = B$
- iii) $A - (A - B) = A \cap B$
- iv) $(A - \Gamma) \cup (B - \Gamma) = A \cup B - \Gamma$
- v) $A \cup (A \cup B)' = A \cup B$

2. Αν $A, B \subseteq E$, βρείτε τα σύνολα A, B , όταν

$$\text{i) } A \subseteq A', \text{ ii) } A' \subseteq A', \text{ iii) } A \subseteq B, A' \subseteq B.$$

3. Γράψτε τα στοιχεία του συνόλου $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

4. Να λύσετε την εξίσωση $A \cap X = B$ στο σύνολο $\mathcal{P}(E)$.

5. Όμοια την εξίσωση $A = X - B$.

6. Ν' αποδείξετε ότι η συνάρτηση $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ με τιμή $f(m, n) = \frac{(m+n-2)(m+n-1)}{2} + m$ αντιστρέφεται και ότι έχει αντίστροφη τη συνάρτηση $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ με $g(m) = \left(m - \frac{n(n+1)}{2}, \frac{n(n+3)}{2} - m \right)$ για $\frac{n(n+1)}{2} \leq m \leq \frac{n(n+3)}{2}$.

7. Έστω οι συναρτήσεις $f : E \rightarrow F, g : F \rightarrow G, h : G \rightarrow E$. Αν οι συναρτήσεις $h \circ g \circ f, f \circ h \circ g$ είναι επί και η συνάρτηση $g \circ f \circ h$ αμφιμονοσήμαντη, ν' αποδείξετε ότι και οι τρεις συναρτήσεις f, g, h είναι αμφιμονοσήμαντες.

8. Ν' αποδείξετε ότι $A \Delta (B \cap \Gamma) = (A \Delta B) \cap (A \Delta \Gamma)$ τότε και μόνο, όταν $A \cap B = A \cap \Gamma$.

9. Δείξτε ότι η συνάρτηση $f : E \rightarrow F$ είναι αμφιμονοσήμαντη τότε και μόνο, όταν για όλα τα $A, B \subseteq E$ ισχύει $f(A \cap B) = f(A) \cap f(B)$.

10. Δείξτε ότι η $f : E \rightarrow F$ είναι επί του F τότε και μόνο, όταν για κάθε $B \subseteq F$ ισχύει $f(f^{-1}(B)) = B$.

11. Δείξτε ότι η συνάρτηση $f : E \rightarrow F$ είναι αμφιμονοσήμαντη τότε και μόνο, όταν $f^{-1}(f(A)) = A$ για κάθε $A \subseteq E$.

12. Έστω $A, B \subseteq E$ και η συνάρτηση $f : \mathcal{P}(E) \rightarrow \mathcal{P}(A) \times \mathcal{P}(B)$ με τιμή $f(X) = (X \cap A, X \cap B)$. Δείξτε ότι

- i) η f είναι αμφιμονοσήμαντη $\Leftrightarrow A \cap B = E$
- ii) η f είναι επί $\Leftrightarrow A \cap B = \emptyset$

13. Έστω $A, B \subseteq E$ και η συνάρτηση $f : \mathcal{P}(E) \rightarrow \mathcal{P}(E)$ με τιμή $f(X) = A \cup (B \cap X)$. Βρείτε τη συνάρτηση $f^2 = f \circ f$ και απλοποιήστε τη μορφή της.

14. Έστω $E = \mathbb{R}^R$. Στο σύνολο E ορίζουμε τη σχέση R θέτοντας $fRg \Leftrightarrow \lim_{x \rightarrow 0} \frac{f(x) - g(x)}{x} = 0$. Δείξτε ότι η σχέση R είναι σχέση ισοδυναμίας. Οι συναρτήσεις $x \mapsto x^2$, $x \mapsto x^2 + x$ είναι ισοδύναμες με τη συνάρτηση $x \mapsto x$;

15. Στο $\mathbb{R}^2$ ορίζουμε τη σχέση R ως εξής: $(x, y)R(u, v) \Leftrightarrow x - y = u - v$. Δείξτε ότι η R είναι μια σχέση ισοδυναμίας επί του $\mathbb{R}^2$ και βρείτε την κλάση του (x_0, y_0) .

16. Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε τη σχέση R ως εξής: $xRy \Leftrightarrow x^2 = y^2$. Δείξτε ότι είναι μια σχέση ισοδυναμίας και βρείτε τις κλάσεις.

17. Έστω R, R' δύο σχέσεις ισοδυναμίας επί του συνόλου E . Δείξτε ότι $R \cap R'$ είναι μια σχέση ισοδυναμίας επί του E . Αν $E = \mathbb{Z}$ και R_m η σχέση επί του $\mathbb{Z}$ με $aR_m b \Leftrightarrow m/a - b$, βρείτε τη σχέση $R_2 \cap R_3$.

18. Έστω $B \subseteq E$ και R η σχέση επί του $\mathcal{P}(E)$ που ορίζεται ως εξής: $XY \Leftrightarrow X \cap B = Y \cap B$. Δείξτε ότι R είναι μια σχέση ισοδυναμίας επί του $\mathcal{P}(E)$ και βρείτε μια αμφιμονοσήμαντη συνάρτηση f του $\mathcal{P}(E)/R$ επί του $\mathcal{P}(E)$.

19. Βρείτε τις ακέραιες λύσεις x, y των εξισώσεων

i. $3x + 5y = 8$

ii. $43x + 17y = 95$

20. Έστω ο αριθμός $A = a_n a_{n-1} \dots a_1 a_0$ στο δεκαδικό σύστημα αρίθμησης με ψηφία $a_i \in [0, 9] \cap \mathbb{Z}$. Ν' αποδείξετε τους παρακάτω κανόνες διαιρετότητας

i) $9/A \Leftrightarrow 9/a_0 + a_1 + \dots + a_n$

ii) $3/A \Leftrightarrow 3/a_0 + a_1 + \dots + a_n$

iii) $11/A \Leftrightarrow 11/a_0 - a_1 + \dots + (-1)^n a_n$

iv) $12/A \Leftrightarrow 12/a_0 - 2a_1 + 4(a_2 + \dots + a_n)$

v) $4/A \Leftrightarrow 4/a_0 + 2a_1$

21. Έστω R_1 μια διμελής σχέση από το E στο F και R_2 μια διμελής σχέση από το F στο G . Ορίζουμε τις σχέσεις $R = R_2 \circ R_1$ και R_2^{-1} ως εξής:

$$\begin{aligned} xRz &\Leftrightarrow \exists y \in F \text{ με } xR_1y \text{ και } yR_2z \\ yR_2^{-1}x &\Leftrightarrow xR_2y \end{aligned}$$

Έτσι η $R_2 \circ R_1$ είναι μια σχέση από το E στο G και η R_2 από το F στο E . Ν' αποδείξετε, αν $\Delta = \{(x, y); x = y\}$, ότι η R είναι:

i) αυτοπαθητική $\Leftrightarrow \Delta \subseteq R$

ii) αντισυμμετρική $\Leftrightarrow R \cap R^{-1} = \Delta$

iii) συμμετρική $\Leftrightarrow R^{-1} = R$

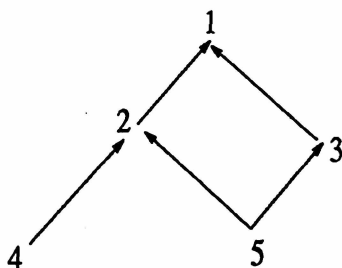
- iv) μεταβατική $\Leftrightarrow R \circ R \subseteq R$ N' αποδείξετε ακόμη ότι:
 v) $(R^{-1})^{-1} = R$, $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$
 vi) $T \circ (R \cup S) = (T \circ R) \cup (T \circ S)$
 vii) $R_3 \circ (R_2 \circ R_1) = (R_3 \circ R_2) \circ R_1$

22. Αν οι σχέσεις R, S είναι σχέσεις ισοδυναμίας ν' αποδείξετε ότι η $R \circ S$ είναι σχέση ισοδυναμίας τότε και μόνο, όταν $R \circ S = S \circ R$.

23. Έστω E_{18} το σύνολο των θετικών διαιρετών του 18 διατεταγμένο με τη σχέση " x/y ". Γράψτε το διάγραμμα Hasse.

Όμοια για το σύνολο των θετικών διαιρετών του 24.

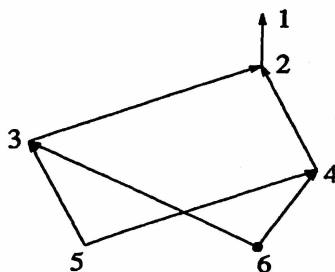
24. Έστω $A = \{1, 2, 3, 4, 5\}$ με σχέση διάταξης



Έστω B η οικογένεια των ολικώς διατεταγμένων υποσυνόλων του A με 2 ή περισσότερα στοιχεία διατεταγμένα με τη σχέση του "περιέχεται". Γράψτε το διάγραμμα Hasse για το διατεταγμένο σύνολο $(B, \subseteq)$.

25. Δίνονται τα σύνολα $A = \{2, 3, \dots\}$, $B = \{2, 3, \dots, 19\}$. Βρείτε τα στοιχεία minimal και maximal.

26. Έστω το σύνολο $E = \{1, 2, 3, 4, 5, 6\}$ με διάταξη



Θεωρούμε το σύνολο $A = \{2, 3, 4\}$. Βρείτε τα στοιχεία του E που είναι άνω πέρας του A και επίσης τα στοιχεία που είναι κάτω πέρας. Υπάρχουν τα $\sup E$ και $\inf E$;

27. Έστω A, B δύο πεπερασμένα σύνολα με m αντίστοιχα n στοιχεία. Δείξτε ότι υπάρχουν 2^{mn} σχέσεις από το A στο B . Κάθε σχέση R από το A στο B παρίσταται με ένα $M_R = (\mu_{ij})$, $1 \leq i \leq m$, $1 \leq j \leq n$ που ορίζεται ως εξής: Αν

$A = \{a_1, a_2, \dots, a_m\}$, $B = \{\beta_1, \beta_2, \dots, \beta_n\}$ θέτουμε

$$\mu_{ij} = \begin{cases} 1 & ; \quad \text{αν } (a_i, \beta_j) \in R \\ 0 & ; \quad \text{αν } (a_i, \beta_j) \notin R \end{cases}$$

Βρείτε τους πίνακες των σχέσεων $\emptyset, A \times B$.

28. Αν το σύνολο E είναι ολικά διατεταγμένο, δείξτε ότι

$$\inf \{a, \sup\{\beta, \gamma\}\} = \sup \{\inf\{a, \beta\}, \inf\{a, \gamma\}\}$$

29. Αν $A \sim B$, δείξτε ότι $\mathcal{P}(A) \sim \mathcal{P}(B)$.

30. Αν το σύνολο E έχει n στοιχεία, βρείτε το άθροισμα $\sum_{X \in \mathcal{P}(E)} |X|$.

31. Δείξτε ότι δύο οποιαδήποτε ανοικτά διαστήματα του $\mathbb{R}$ είναι ισοδύναμα σύνολα.

32. Αν a, β, γ πληθάρημοι, ν' αποδείξετε ότι

1. $a + \beta = \beta + a$, $a \cdot \beta = \beta \cdot a$
2. $a + (\beta + \gamma) = (a + \beta) + \gamma$, $a \cdot (\beta \cdot \gamma) = (a \cdot \beta) \cdot \gamma$
3. $a^\beta \cdot a^\gamma = a^{\beta+\gamma}$
4. $(a^\beta)^\gamma = a^{\beta\gamma}$
5. $(a \cdot \beta)^\gamma = a^\gamma \cdot \beta^\gamma$

33. Αν A, B, Γ είναι τρία πεπερασμένα σύνολα, δείξτε ότι

$$|A \cup B \cup \Gamma| = |A| + |B| + |\Gamma| - |A \cap B| - |A \cap \Gamma| - |B \cap \Gamma| + |A \cap B \cap \Gamma|.$$

34. Σε μια έρευνα ανακοινώθηκε ότι σε σύνολο 1000 μαθητών, 800 μιλούν Αγγλικά, 250 Γαλλικά, 350 Ισπανικά, ενώ 136 Αγγλικά και Γαλλικά, 240 Αγγλικά και Ισπανικά και 30 Γαλλικά και Ισπανικά. Πόσοι μαθητές μιλούν και τις τρεις γλώσσες;

35. Έστω $G = \{x \in \mathbb{Q}; x \neq -\frac{1}{2}\}$. Δείξτε ότι η συνάρτηση $(a, \beta) \mapsto a + \beta + 2a\beta$ είναι εσωτερικός νόμος στο G και ότι το G είναι ομάδα αντιμεταθετική ως προς το νόμο αυτό.

36. Έστω $(G, \cdot)$ μια αντιμεταθετική ομάδα με ουδέτερο e . Αν $c \in G, c \neq e$ και $a * \beta = a \cdot \beta \cdot c$, δείξτε ότι $(G, *)$ είναι ομάδα αντιμεταθετική.

37. Έστω $E = (-c, c)$ με $c \in \mathbb{R}, c > 0$. Αν $x, y \in E$, θέτουμε $x * y = \frac{x+y}{1+xy/c^2}$. Δείξτε ότι $(E, *)$ είναι ομάδα.

38. Έστω $a, \beta \in \mathbb{R}$ και $E = \{f_{a,\beta} : \mathbb{R} \rightarrow \mathbb{R}; f_{a,\beta}(x) = ax + \beta\}$. Δείξτε ότι $(E, +, \circ)$ είναι σώμα μη αντιμεταθετικό (σημείωση: $\circ$ είναι η σύνθεση συναρτήσεων και $+$ η πρόσθεση συναρτήσεων του $\mathbb{R}$ στο $\mathbb{R}$).

39. Έστω E το σύνολο των πινάκων $M_{a,\beta} = \begin{pmatrix} a & \beta \\ -\beta & a \end{pmatrix}$ με $a, \beta \in \mathbb{R}$. Δείξτε ότι το E ως προς την πρόσθεση και τον πολλαπλασιασμό των πινάκων είναι σώμα. Να λύσετε στο σώμα αυτό την εξίσωση $X^2 + I = \theta$. Δείξτε ότι η συνάρτηση $f : \mathbb{C} \rightarrow E$ με τιμή $f(a + \beta i) = M_{a,\beta}$ έχει τις ιδιότητες $f(z + z') = f(z) + f(z')$, $f(zz') = f(z)f(z')$.

40. Στο σύνολο $E = \mathbb{Z} \times \mathbb{Z}$ ορίζουμε δύο εσωτερικούς νόμους $+, \cdot$ θέτοντας

$$(a, \beta) + (a', \beta') = (a + a', \beta + \beta'), \quad (a, \beta) \cdot (a', \beta') = (aa', 0)$$

Δείξτε ότι $(E, +, \cdot)$ είναι δακτύλιος.

41. Ένας δακτύλιος $(B, +, \cdot)$ λέγεται δακτύλιος του Boole, αν $x^2 = x$ για κάθε $x \in B$. Δείξτε ότι

- Κάθε δακτύλιος του Boole είναι αντιμεταθετικός.
- Σε κάθε δακτύλιο Boole είναι $x + x = 0$, $(x + y)xy = 0$
- Σε κάθε δακτύλιο Boole η σχέση $x \leq y \Leftrightarrow xy = x$ είναι μια σχέση διάταξης και ότι κάθε υποσύνολο $\{a, \beta\}$ έχει άνω και κάτω πέρας.

42. Αν $(K, +, \cdot)$ είναι σώμα και a, β δύο στοιχεία του με $a \cdot \beta \neq \beta \cdot a$, δείξτε ότι

- $a = [\beta - (a - 1)^{-1}\beta(a - 1)][a^{-1}\beta a - (a - 1)^{-1}\beta(a - 1)]^{-1}$
- $a = [1 - (a - 1)^{-1}\beta^{-1}(a - 1)\beta][a^{-1}\beta^{-1}a\beta - (a - 1)^{-1}\beta^{-1}(a - 1)\beta]^{-1}$

Γιατί υποθέτουμε ότι $a\beta \neq \beta a$;

43. Βρείτε το πλήθος των αντιμεταθετικών εσωτερικών νόμων σ' ένα σύνολο με n στοιχεία.

44. Έστω M_{01} το σύνολο των πινάκων με στοιχεία 0 ή 1. Στο σύνολο $\{0, 1\}$ ορίζουμε δύο διμελής εσωτερικούς νόμους $\cup, \cap$ και ένα μονομελή $(')$ ως εξής

$$\begin{aligned} 0' &= 1, \quad 1' = 0 \\ 0 \cup 0 &= 0, \quad 0 \cup 1 = 1 \cup 0 = 1 \cup 1 = 1 \\ 0 \cap 0 &= 0 \cap 1 = 1 \cap 0 = 0, \quad 1 \cap 1 = 1 \end{aligned}$$

Ορίζουμε ακόμη μια σχέση διάταξης:

$$0 \leq 0, \quad 0 \leq 1, \quad 1 \leq 1, \quad 1 \not\leq 0$$

Αν $X = (x_{ij})$, $Y = (y_{ij}) \in M_{01}$ ορίζουμε

$$X \cup Y = (x_{ij} \cup y_{ij}), \quad X \cap Y = (x_{ij} \cap y_{ij}) \quad \text{και} \quad X \leq Y$$

αν για κάθε i και j είναι $x_{ij} \leq y_{ij}$. Αν R, S είναι δύο σχέσεις από το σύνολο A στο B και M_R, M_S οι πίνακες αυτών (άσκ.27), δείξτε ότι

$$\begin{aligned} M_{R \cup S} &= M_R \cup M_S \\ M_{R \cap S} &= M_R \cap M_S \\ M_R \leq M_S &\Leftrightarrow R \subseteq S \end{aligned}$$

45. Να υπολογιστούν τα αθροίσματα

$$S_1 = \sum_{X, Y \subseteq E} |X \cap Y|, \quad S_2 = \sum_{X, Y \subseteq E} |X \cup Y|$$

όπου $|E| = n \geq 1$.

46. Όμοια, να υπολογιστούν τα αθροίσματα

$$A = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \min(i, j), \quad B = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \max(i, j)$$

Υπενθυμίζεται ότι : $\sum_1^n k = \frac{n(n+1)}{2}, \quad \sum_1^n k^2 = \frac{n(n+1)(2n+1)}{6}$

47. Να υπολογίσετε τα αθροίσματα

$$\begin{aligned} &\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots \\ &\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \dots \\ &\binom{n}{2} + \binom{n}{5} + \binom{n}{8} + \dots \end{aligned}$$

48. Βρείτε το πλήθος των συναρτήσεων $f : [1, m] \rightarrow [1, n]$ που είναι αύξουσες και αμφιμονοσήμαντες.

49. Βρείτε τα σύνολα των λύσεων $(x_1, \dots, x_n)$

α) της ανισότητας $x_1 + x_2 + \dots + x_m \leq n$ με $x_i \in \mathbb{N}$ για $1 \leq i \leq m$

β) της εξίσωσης $x_1 + x_2 + \dots + x_m = n$ με $x_i \in \mathbb{N}$ για $1 \leq i \leq m$.

50. Να υπολογίσετε τα αθροίσματα

$$\begin{aligned} A &= 1 \cdot \binom{n}{1} + 2 \cdot \binom{n}{2} + \dots + m \cdot \binom{n}{m} = \sum_{k=1}^n k \binom{n}{k} \\ B &= (-1)^1 1 \binom{n}{1} + (-1)^2 2 \binom{n}{2} + \dots + (-1)^m m \binom{n}{m} = \sum_{k=1}^n (-1)^k k \binom{n}{k} \end{aligned}$$

1 | Διαιρετότητα στους ακεραίους

Στην § 9 του προηγούμενου κεφαλαίου κατασκευάσαμε το σύνολο των ακεραίων αριθμών $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ από το σύνολο των φυσικών αριθμών.

Αποδείξαμε ότι είναι ένας μοναδιαίος και αντιμεταθετικός δακτύλιος χωρίς διαιρέτες του μηδενός, ότι δηλαδή ορίζονται δύο εσωτερικοί νόμοι $+$, $\cdot$ με τις παρακάτω ιδιότητες:

1. $a + \beta \in \mathbb{Z}$, $a \cdot \beta \in \mathbb{Z}$ για όλα τα $a, \beta \in \mathbb{Z}$
2. $a + (\beta + \gamma) = (a + \beta) + \gamma$, $a \cdot (\beta \cdot \gamma) = (a \cdot \beta) \cdot \gamma$ για όλα τα $a, \beta, \gamma \in \mathbb{Z}$
3. Υπάρχουν ουδέτερα των νόμων $+$, $\cdot$, τα οποία συμβολίζουμε με 0 αντίστοιχα 1:

$$a + 0 = a + a = a, \quad a \cdot 1 = 1 \cdot a = a \quad \text{για κάθε } a \in \mathbb{Z}$$

4. $a + \beta = \beta + a$, $a \cdot \beta = \beta \cdot a$ για όλα τα $a, \beta \in \mathbb{Z}$
5. Για κάθε $a \in \mathbb{Z}$ υπάρχει το αντίθετο $-a$:

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

6. $a \cdot (\beta + \gamma) = a \cdot \beta + a \cdot \gamma$

$$7. a\beta = 0 \Rightarrow a = 0 \text{ ή } \beta = 0$$

Στο δακτύλιο $(\mathbb{Z}, +, \cdot)$ ορίζεται και μια σχέση ολικής διάταξης $\leq$ με τις ιδιότητες:

$$8. a \geq \beta \Rightarrow a + \gamma \geq \beta + \gamma$$

$$9. a \geq \beta, \gamma > 0 \Rightarrow a \cdot \gamma \geq \beta \cdot \gamma$$

$$10. a \geq \beta, \gamma < 0 \Rightarrow a \cdot \gamma \leq \beta \cdot \gamma$$

$$11. a > 0, \beta > 0 \Rightarrow a + \beta > 0, a \cdot \beta > 0$$

Η διαφορά $a - \beta$ δύο ακεραίων a, β ορίζεται στο $\mathbb{Z}$ ως εξής: $a - \beta = a + (-\beta)$.

1. ΔΙΑΙΡΕΣΗ ΑΚΕΡΑΙΩΝ

Θεώρημα 1. Έστω a, m δύο ακέραιοι, $m \neq 0$. Υπάρχει ένα μόνο ζεύγος ακεραίων (q, v) τέτοιων, ώστε

$$a = qm + v, \quad 0 \leq v < |m|$$

Απόδειξη. Αν $m = 1$, τότε $q = a$ και $v = 0$. Έστω $m > 1$. Θέτουμε $A = \{a - xm; x \in \mathbb{Z}\}$. Προφανώς $a \in A$ για $x = 0$ και $a - am = a(1 - m) \in A$. Ο αριθμός $a(1 - m)$ είναι > 0 για $a < 0$. Έτσι το σύνολο A περιέχει ακεραίους θετικούς. Έστω v ο ελάχιστος ακέραιος ≥ 0 που ανήκει στο σύνολο A . Αν $v = a - qm$, έχουμε $a - (q + 1)m = a - qm - m = v - m < 0$. Συνεπώς

$$a = qm + v \quad \text{με} \quad 0 \leq v < m = |m|.$$

δηλαδή οι ακέραιοι q, v έχουν τις ιδιότητες που θέλουμε.

Αποδεικνύουμε τη μοναδικότητα των q, v : Έστω ότι

$$a = q'm + v' \quad \text{με} \quad 0 \leq v' < m.$$

και ότι $q' < q$. Τότε

$$a - q'm = v' \geq a - (q - 1)m = v + m \geq m$$

πράγμα άτοπο, αφού $v' < m$. Όμοια $q < q'$ είναι αδύνατο. Άρα $q = q'$ και $v = a - qm = v'$.

Έστω $m < 0$. Τότε υπάρχουν μοναδικοί ακέραιοι q', v' τέτοιои, ώστε $a = q'(-m) + v'$ με $0 \leq v' < -m$, γιατί $-m > 0$. Συνεπώς $a = (-q')m + v' = qm + v$ με $q = -q' \in \mathbb{Z}$, $0 \leq v < -m = |m|$. $\square$

Η εύρεση των q, v λέγεται **διαίρεση** του a με τον m . Το a λέγεται **πηλίκιο** και το v **υπόλοιπο** της διαίρεσης του a με τον m .

Ο ακέραιος a λέγεται **διαιρέτης** του β , αν το υπόλοιπο της διαίρεσης του β με τον a είναι $v = 0$, αν δηλαδή υπάρχει ακέραιος q τέτοιος, ώστε $\beta = qa$. Γράφουμε τότε a/β (a διαιρεί το β). Αν $\beta \neq 0$, οι ακέραιοι $\pm\beta, \pm 1$ είναι διαιρέτες του β . Λέγονται **τετριμμένοι** διαιρέτες του β .

Πρόταση 1. Ισχύουν

- i) $a/a \cdot \beta$
- ii) $a/\beta, \beta/\gamma \Rightarrow a/\gamma$
- iii) $a/\beta, a > 0, \beta > 0 \Rightarrow a \leq \beta$
- iv) $a/\beta, a/\gamma \Rightarrow a/\beta\lambda + \gamma\mu$ για όλα τα $\lambda, \mu \in \mathbb{Z}$
- v) $a/\beta \Rightarrow \pm a/\pm \beta$

Απόδειξη. i) Γιατί $a \cdot \beta = q \cdot a$ με $q = \beta$. ii) Έχουμε $\beta = qa, \gamma = q'\beta$, συνεπώς $\gamma = (q'q)a$. iii) Είναι $\beta = qa$ με $a > 0, \beta > 0$. Συνεπώς $q > 0$ ή $q \geq 1$, οπότε $\beta = qa \geq a$. iv) Έχουμε $\beta = qa, \gamma = q'a$, συνεπώς $\lambda\beta + \mu\gamma = \lambda qa + \mu q'a = (\lambda q + \mu q')a$, δηλαδή $a/\lambda\beta + \mu\gamma$. v) Προφανές. $\square$

Ορισμός 1. Ένας ακέραιος p λέγεται **πρώτος** ακέραιος, αν οι μόνοι διαιρέτες του p είναι οι τετριμμένοι διαιρέτες $\pm p, \pm 1$. Οι πρώτοι κατά σειρά ακέραιοι πρώτοι > 1 είναι

2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 37, ...

Υπάρχει ένας απλός τρόπος να κατασκευάσουμε τον πίνακα των θετικών πρώτων αριθμών, που αναφέρεται από τον Ερατοσθένη: Γράφουμε τους φυσικούς αριθμούς σε μια σειρά

1, 2, 3, ...

Διαγράφουμε τους αριθμούς που έχουν διαιρέτη το 2 εξαιρέσει του 2:

1, 2, 3, 5, 7, 9, ...

Στη συνέχεια διαγράφουμε όλους τους αριθμούς που έχουν διαιρέτη το 3 εξαιρέσει του 3

1, 2, 3, 5, 7, 11, 13, ...

κ.ο.κ. Οι αριθμοί που παραμένουν τελικά είναι οι πρώτοι αριθμοί. Ένας κατάλογος των πρώτων αριθμών από 1 μέχρι 10.006.721 δημοσιεύτηκε από τον Lehmer. Ένας πρώτος αριθμός με 39 ψηφία είναι ο

$$2^{127} - 1 = 1701.41183.46046.92317.31687.30371.58841.05727$$

Ο μεγαλύτερος γνωστός πρώτος μέχρι την προηγούμενη δεκαετία είναι ο αριθμός με 13395 ψηφία $2^{44497} - 1$. Ο αριθμός $2^{257} - 1$ δεν είναι πρώτος, αλλά δεν γνωρίζουμε τους πρώτους διαιρέτες του. Ένα θεώρημα, γνωστό σαν **θεώρημα των πρώτων αριθμών**, είναι το εξής: Για $x \geq 1$, έστω $\pi(x)$ το πλήθος των πρώτων αριθμών $\leq x$. Τότε

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1 \quad (1)$$

Ο Legendre διατύπωσε το 1798 την εικασία ότι κατά προσέγγιση

$$\pi(x) = \frac{x}{A \ln x + B}$$

όπου A, B σταθερές. Μια πρώτη προσπάθεια για την απόδειξη της σχέσης (1) έγινε από τον Tchebycheff το 1852. Απέδειξε ότι για αρκετά μεγάλο x ,

$$0.92 \leq \frac{\pi(x)}{x / \ln x} \leq 1.106$$

Το 1860 ο Riemann δημοσίευσε μια εργασία στην οποία συνέδεσε τη συνάρτηση $\pi(x)$ με τη μιγαδική συνάρτηση "ζήτα του Riemann"

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Η πρώτη απόδειξη του θεωρήματος των πρώτων αριθμών (1) έγινε ανεξάρτητα από τον Hadamard και τον De la Vallee Poussin το 1896.

Συνεχίζουμε με ιδιότητες πρώτων αριθμών.

Πρόταση 2. Κάθε ακέραιος $\beta > 1$ έχει ένα τουλάχιστο πρώτο διαιρέτη.

Απόδειξη. Έστω $A = \{a : a/\beta, a > 1\}$. Επειδή $\beta \in A, A \neq \emptyset$. Το A περιέχει ένα ελάχιστο ακέραιο, έστω τον p . Θ' αποδείξουμε ότι ο p είναι πρώτος. Έστω q ένας θετικός διαιρέτης του p μη τετριμμένος ($\pm p, \pm 1$). Τότε $1 < q < p$. Επειδή q/p και p/β , έχουμε q/β , δηλαδή $q \in A$, πράγμα αντίθετο στην επιλογή του p . $\square$

Θεώρημα 2. Υπάρχουν άπειροι πρώτοι ακέραιοι.

Απόδειξη. (περιέχεται στα στοιχεία του Ευκλείδη, το 300 π.Χ.). Έστω ότι το πλήθος τους είναι πεπερασμένο και ότι $p_1, p_2, \dots, p_n$ είναι οι πρώτοι ακέραιοι. Θέτουμε $a = p_1 p_2 \dots p_n + 1$. Έστω p ένας πρώτος διαιρέτης του a .

Επειδή ο p_i δεν διαιρεί τον a , ενώ ο p/a , έχουμε $p \neq p_i$ (για $i = 1, 2, \dots, n$), πράγμα άτοπο. $\square$

Μέγιστος κοινός διαιρέτης

Έστω $a_1, a_2, \dots, a_n$ ακέραιοι, $n \geq 2$. Ένας ακέραιος a λέγεται κοινός διαιρέτης των $a_1, a_2, \dots, a_n$, αν a/a_i , $i = 1, 2, \dots, n$.

Ο ακέραιος d λέγεται μέγιστος κοινός διαιρέτης των $a_1, a_2, \dots, a_n$, αν

- i) $d > 0$
- ii) Είναι κοινός διαιρέτης των a_i ($i = 1, 2, \dots, n$)
- iii) Κάθε κοινός διαιρέτης d' των a_i είναι διαιρέτης του d :

$$d'/a_i \ (i = 1, 2, \dots, n) \Rightarrow d'/d.$$

Γράφουμε $d = \mu.χ.δ(a_1, a_2, \dots, a_n)$ ή απλούστερα $d = (a_1, a_2, \dots, a_n)$, όταν δεν υπάρχει κίνδυνος σύγχυσης.

Θεώρημα 3. Έστω a, β δύο ακέραιοι, όχι και οι δύο ίσοι με μηδέν. Υπάρχει ένας μόνο μέγιστος κοινός διαιρέτης των a, β και αυτός γράφεται υπό τη μορφή:

$$ax + \beta y$$

με x, y ακεραίους.

Απόδειξη. Έστω ότι ο d και ο d' είναι μέγιστος κοινός διαιρέτης των a, β . Τότε από την ιδιότητα (iii) έχουμε d'/d και d/d' . Συνεπώς $d = d'\lambda$ και $d' = d\mu$ με $\lambda, \mu \in \mathbb{Z}$. Τότε $d = d\mu\lambda$, $\mu\lambda = 1$, $\mu = \pm 1$, $d' = \pm d$ και επειδή $d, d' > 0$ είναι $d' = d$.

Αποδεικνύουμε τώρα την ύπαρξη του μέγιστου κοινού διαιρέτη των a, β : Θεωρούμε το σύνολο $A = \{ax + \beta y; x, y \in \mathbb{Z}\}$. Προφανώς, αν $z = ax + \beta y \in A$, ο ακέραιος $-z = a(-x) + \beta(-y) \in A$. Συνεπώς το A περιέχει ακεραίους > 0 . Έστω $S = \{z \in A; z > 0\}$. Αφού $\emptyset \neq S \subseteq \mathbb{N}$, το S έχει ελάχιστο στοιχείο. Έστω d το ελάχιστο στοιχείο του S . Έχουμε $d = ax_0 + \beta y_0$ με $x_0, y_0 \in \mathbb{Z}$.

Ότι ο $d/a, \beta$ προκύπτει ως εξής: Έχουμε $a = d\mu + v$ με $0 \leq v < d$. Είναι $v = a - d\mu = a - (ax_0 + \beta y_0)\mu = a(1 - x_0\mu) + \beta(-y_0\mu) \in A$. Επειδή $v < d$, έχουμε $v = 0$, δηλαδή d/a . Όμοια d/β .

Αν $d'/a, d'/\beta$, τότε d'/d (πρότ.1), άρα ο d είναι μέγιστος κοινός διαιρέτης των a, β . $\square$

Παρατήρηση 1. $\mu.χ.δ(a, 0) = |a|$.

Παρατήρηση 2. Κάθε στοιχείο του A είναι της μορφής $d\lambda$, με $\lambda \in \mathbb{Z}$. Πραγματικά, $d\lambda = a(x_0\lambda) + \beta(y_0\lambda) \in A$ για κάθε ακέραιο λ και η διαφορά δύο στοιχείων του A είναι στοιχείο του A , γιατί $(ax + \beta y) - (ax' + \beta y') = a(x - x') + \beta(y - y')$. Έστω τώρα $m \in A$ και q, v το πηλίκο και το υπόλοιπο του m με το d . Τότε $m = dq + v$ με $0 \leq v < d$ και $v = m - dq \in A$. Αφού d είναι ο μικρότερος θετικός στο σύνολο A , έχουμε $v = 0$, δηλαδή $m = dq$.

Πόρισμα 1. Αν $a_1, a_2, \dots, a_n$ είναι ακέραιοι όχι όλοι ίσοι με μηδέν, υπάρχει μέγιστος κοινός διαιρέτης αυτών, είναι μοναδικός και έχει τη μορφή

$$a_1x_1 + a_2x_2 + \dots + a_nx_n$$

με $x_i \in \mathbb{Z}$.

Οι ακέραιοι $a_1, a_2, \dots, a_n$ λέγονται **σχετικά πρώτοι**, αν

$$\mu.κ.δ(a_1, a_2, \dots, a_n) = 1$$

Σύμφωνα με το θεώρημα 1 οι ακέραιοι $a_1, a_2, \dots, a_n$ είναι σχετικά πρώτοι τότε και μόνο, όταν υπάρχουν ακέραιοι $\lambda_1, \lambda_2, \dots, \lambda_n$ τέτοιοι, ώστε

$$\lambda_1a_1 + \lambda_2a_2 + \dots + \lambda_na_n = 1.$$

Πρόταση 3. Έστω a, β δύο ακέραιοι σχετικά πρώτοι. Αν $a/\beta\gamma$, τότε a/γ .

Απόδειξη. Υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $ax + \beta y = 1$. Αφού $a/\beta\gamma$, έχουμε $\beta\gamma = \lambda a$ με $\lambda \in \mathbb{Z}$. Συνεπώς έχουμε

$$a\gamma x + \beta\gamma y = \gamma$$

$$a\gamma x + \lambda ay = \gamma, \quad (\gamma x + \lambda y)a = \gamma, \quad a/\gamma \quad \square$$

Πρόταση 4(Ευκλείδης). Αν ο p είναι πρώτος και $p/a\beta$, τότε p/a ή p/β .

Απόδειξη. Αν a ή β είναι μηδέν, το συμπέρασμα είναι προφανές. Έστω $a, \beta \neq 0$ και ότι $p \nmid a$. Τότε οι a, p είναι σχετικά πρώτοι. Κατά την προηγούμενη πρόταση p/β . $\square$

Πόρισμα. Αν ο p είναι πρώτος και $p/a_1a_2 \dots a_n$, τότε p/a_i για κάποιο $i \in \{1, 2, \dots, n\}$.

Παρατήρηση. Αν ο p δεν είναι πρώτος, είναι δυνατόν $p/a\beta$, $p \nmid a$, $p \nmid \beta$. Π.χ. $6/3 \cdot 4 = 12$ και $6 \nmid 3$, $6 \nmid 4$. Συνεπώς η πρόταση δίνει ισοδύναμο ορισμό του πρώτου αριθμού:

Ο p είναι πρώτος τότε και μόνο, όταν $p/a\beta \Rightarrow p/a$ ή p/β .

Το θεώρημα που ακολουθεί είναι γνωστό σαν **Θεμελιώδες** θεώρημα της αριθμητικής:

Θεώρημα 4. Κάθε ακέραιος $n > 1$ παρίσταται σαν γινόμενο πρώτων αριθμών $q_1, q_2, \dots, q_m > 1$

$$n = q_1 q_2 \cdots q_m$$

Οι πρώτοι αριθμοί q_i ορίζονται μονοσήμαντα όταν δεν λαμβάνουμε υπ' όψη τη σειρά τους. Αν δηλαδή $n = p_1 p_2 \cdots p_s$ είναι μια άλλη ανάλυση του n σε γινόμενο πρώτων, τότε $m = s$ και με κατάλληλη αρίθμηση $q_i = p_i$.

Απόδειξη. Αν ο n δεν είναι πρώτος, έχει διαιρέτη ένα πρώτο αριθμό q_1 . Έστω $n = q_1 \cdot p_1$. Ο p_1 έχει επίσης ένα πρώτο διαιρέτη q_2 , οπότε $p_1 = q_2 \cdot p_2$ και $n = q_1 q_2 p_2$. Συνεχίζοντας, αφού $n > p_1 > p_2 > \dots$, βλέπουμε ότι ο n γράφεται γινόμενο πρώτων αριθμών.

Έστω δύο αναλύσεις του n σε γινόμενο πρώτων

$$n = q_1 q_2 \cdots q_m = p_1 p_2 \cdots p_s$$

Θ' αποδείξουμε ότι $m = s$ και ότι $\{q_1, q_2, \dots, q_m\} = \{p_1, p_2, \dots, p_s\}$. Κάνουμε επαγωγή ως προς m . Αν $m = 1$, ό n είναι πρώτος και συνεπώς $n = q_1 = p_1$, δηλαδή το θεώρημα ισχύει. Θα υποθέσουμε ότι σ' ένα γινόμενο πρώτων αριθμών με πλήθος παραγόντων $< m$, το σύνολο των πρώτων παραγόντων ορίζεται μονοσήμαντα. Αν

$$q_1 q_2 \cdots q_m = p_1 p_2 \cdots p_s$$

το δεύτερο μέλος διαιρείται με q_1 . Συνεπώς q_1/p_i για κάποιο p_i . Αφού ο p_i είναι πρώτος, πρέπει $q_1 = p_i$. Μπορούμε να υποθέσουμε ότι $i = 1$, διαφορετικά αλλάζουμε την αρίθμηση. Τότε $q_1 = p_1$ και επομένως

$$q_2 \cdots q_m = p_2 \cdots p_s$$

Το πλήθος των πρώτων παραγόντων είναι $< m$. Κατά την υπόθεση της επαγωγής $m - 1 = s - 1$ και $\{q_2, \dots, q_m\} = \{p_2, \dots, p_s\}$. Άρα $m = s$ και $\{q_1, q_2, \dots, q_m\} = \{p_1, p_2, \dots, p_s\}$. $\square$

Πόρισμα 1. Αν $p_1, p_2, \dots, p_m$ είναι το σύνολο των διάφορων πρώτων διαιρετών του ακεραίου $n > 1$, τότε

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

με a_i ακεραίους ≥ 1 .

Πόρισμα 2. Αν οι θετικοί ακέραιοι a, β δέχονται την ανάλυση σε γινόμενο πρώτων

$$a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}, \quad \beta = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

όπου $a_i \geq 0, \beta_i \geq 0$ και a_i, β_i ακέραιοι, τότε

$$(a, \beta) = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_m^{\lambda_m} \quad \text{με } \lambda_i = \min(a_i, \beta_i)$$

Ελάχιστο κοινό πολλαπλάσιο (ε.κ.π)

Έστω οι ακέραιοι $a_1, a_2, \dots, a_n$. Ένας ακέραιος m λέγεται **κοινό πολλαπλάσιο** αυτών, αν

$$a_i/m \quad (i = 1, 2, \dots, n).$$

Ένας ακέραιος m λέγεται **ελάχιστο κοινό πολλαπλάσιο** των $a_1, a_2, \dots, a_n$, αν

- i) $m > 0$
- ii) m κοινό πολλαπλάσιο των a_i
- iii) m' κοινό πολ/σιο των $a_i \Rightarrow m/m'$. Γράφουμε τότε $[a_1, a_2, \dots, a_n] = m$.

Παράδειγμα. $[2, 3] = 6, [4, 6] = 12, [15, 20, 30] = 60$.

Θεώρημα 4. $(a, \beta)[a, \beta] = a\beta$.

Απόδειξη. Έστω $(a, \beta) = d, [a, \beta] = m$. Προφανώς $m/a\beta$. Θ' αποδείξουμε ότι $\frac{a\beta}{m} = d$. Έστω $\frac{a\beta}{m} = q$. Έχουμε $\beta/m, a\beta/am, a\beta = qm/am, q/a$. Όμοια q/β . Συνεπώς q είναι κοινός διαιρέτης των a, β . Αν p είναι ένας κοινός διαιρέτης των a, β και $a = px, \beta = py$ με $x, y \in \mathbb{Z}$, τότε $a/pxy, \beta/pxy$, συνεπώς m/pxy και

$$p \left(\frac{pxy}{m} \right) = \frac{pxpy}{m} = \frac{a\beta}{m} = q$$

δηλαδή p/q , άρα $q = d$. □

Θεώρημα 5. Αν

$$a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} \quad \text{και} \quad \beta = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

p_i διάφοροι πρώτοι και a_i, β_i ακέραιοι ≥ 0 , τότε $[a, \beta] = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ με $m_i = \max(a_i, \beta_i)$.

Απόδειξη. Προφανώς $a/m = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ και β/m . Αν m' είναι κοινό πολλαπλάσιο των a, β , τότε $p_j^{m_j}/m' (j=1, 2, \dots, n)$, συνεπώς $m' = p_1^{m_1} \cdots p_n^{m_n} q = mq$, m/m' και άρα $[a, \beta] = m$. $\square$

Θεώρημα (Γενίκευση του 4) **6.** Ισχύει

$$[a_1, a_2, \dots, a_n] = \frac{a_1 a_2 \cdots a_n}{(\beta_1, \beta_2, \dots, \beta_n)}$$

$$\text{όπου } \beta_k = a_1 a_2 \cdots a_k \cdots a_n = \frac{a_1 a_2 \cdots a_n}{a_k}.$$

Απόδειξη. (άσκηση)

2. ΑΚΕΡΑΙΟΙ ΩΣ ΠΡΟΣ ΜΕΤΡΟ m

Έστω m ένας ακέραιος θετικός. Στην § 7 του προηγούμενου κεφαλαίου ορίσαμε τους ακεραίους ως προς μέτρο m : Είναι τα σύνολα των ακεραίων

$$\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1} \quad (1)$$

όπου $\bar{a} = \{x \in \mathbb{Z}; x = qm + a \text{ με } q \in \mathbb{Z}\}$. Έτσι $x, y \in \bar{a}$ τότε και μόνο, όταν $m/x - y$. Αν $m/x - y$, γράφουμε $x \equiv y \pmod{m}$ και στην αντίθετη περίπτωση $x \not\equiv y \pmod{m}$.

Προφανώς

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \cdots \cup \overline{m-1}$$

$$a \not\equiv \beta \pmod{m} \Rightarrow \bar{a} \cap \bar{\beta} = \emptyset$$

Είδαμε ότι το σύνολο $\mathbb{Z}_m$ των ακεραίων $\pmod{m}$ γίνεται μοναδιαίος και αντι-μεταθετικός δαχτύλιος ως προς τις πράξεις

$$\bar{a} + \bar{\beta} = \overline{a + \beta}$$

$$\bar{a} \cdot \bar{\beta} = \overline{a \cdot \beta}$$

Οι πράξεις αυτές είναι καλά ορισμένες, γιατί παρατηρήσαμε ότι, όταν

$$x \equiv a \pmod{m}, y \equiv \beta \pmod{m}$$

τότε

$$x + y \equiv a + \beta \pmod{m}$$

$$x \cdot y \equiv a \cdot \beta \pmod{m}$$

Η παρακάτω πρόταση μας πληροφορεί ποιά στοιχεία του δακτυλίου $(\mathbb{Z}_m, +, \cdot)$ αντιστρέφονται.

Πρόταση 1. Έστω $\bar{a} \in \mathbb{Z}_m$. Το στοιχείο $\bar{a}$ αντιστρέφεται τότε και μόνο, όταν οι a, m είναι σχετικά πρώτοι.

Απόδειξη. Έστω ότι $(a, m) = 1$. Τότε υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $ax + my = 1$. Προφανώς $\overline{ax + my} = \bar{1}$ ή $\bar{a} \cdot \bar{x} + \bar{m} \cdot \bar{y} = \bar{1}$ ή $\bar{a} \cdot \bar{x} = \bar{1}$. Αντίστροφα, αν το $\bar{a}$ αντιστρέφεται, τότε υπάρχει $\bar{x} \in \mathbb{Z}_m$ με $\bar{a} \cdot \bar{x} = \bar{1}$. Αυτό σημαίνει ότι $m/ax - 1$ ή $ax - 1 = my$, δηλαδή $ax + m(-y) = 1$, άρα $(a, m) = 1$. $\square$

Πόρισμα. Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}_m$ αποτελούν ομάδα ως προς τον πολλαπλασιασμό.

Γιατί, αν τα $\bar{a}, \bar{\beta} \in \mathbb{Z}_m$ αντιστρέφονται, το γινόμενο $\bar{a} \cdot \bar{\beta}$ αντιστρέφεται και μάλιστα $(\bar{a} \cdot \bar{\beta})^{-1} = \bar{\beta}^{-1} \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot \bar{\beta}^{-1}$.

Θεώρημα 1. Ο δακτύλιος $(\mathbb{Z}_m, +, \cdot)$ είναι σώμα τότε και μόνο, όταν ο m είναι πρώτος.

Απόδειξη. Αν ο m είναι πρώτος, τότε κάθε στοιχείο $\bar{a} \neq \bar{0}$ του $\mathbb{Z}_m$ αντιστρέφεται, γιατί $(a, m) = 1$, συνεπώς το $\mathbb{Z}_m$ είναι σώμα. Αντίστροφα, αν το $\mathbb{Z}_m$ είναι σώμα, τα στοιχεία $\bar{2}, \bar{3}, \dots, \overline{m-1}$ αντιστρέφονται, συνεπώς οι ακέραιοι $2, 3, \dots, m-1$ δεν διαιρούν τον m , άρα ο m είναι πρώτος. $\square$

Θεώρημα 2. Η εξίσωση

$$\bar{a} \cdot \bar{x} = \bar{\beta} \quad (1)$$

έχει λύση στο $\mathbb{Z}_m$ τότε και μόνο, όταν ο $d = (a, m)/\beta$. Το σύνολο των λύσεων της (1) είναι

$$\bar{x}_k = \bar{x}_1 + \overline{k \frac{m}{d}} \quad k = 0, 1, 2, \dots, d-1 \quad (2)$$

όπου $\bar{x}_1$ μια λύση της (1). Το πλήθος τους είναι (a, m) .

Απόδειξη. Έστω $d = (a, m)$. Τότε υπάρχουν ακέραιοι λ, μ τέτοιοι, ώστε $\lambda a + \mu m = d$ (3). Αν η εξίσωση (1) έχει μια λύση, $\bar{x} \in \mathbb{Z}_m$, τότε $m/ax - \beta$, δηλαδή $ax - \beta = my$ με $y \in \mathbb{Z}$ ή $ax + m(-y) = \beta$. Αφού $d/a, d/m$ έπεται ότι d/β .

Αντίστροφα, έστω ότι d/β , $\beta = dq$ με $q \in \mathbb{Z}$. Από την (3) παίρνουμε $\lambda aq + \mu m q = \beta$, οπότε $m/a(\lambda q) - \beta$, δηλαδή $\overline{a(\lambda q)} = \bar{\beta}$ ή $\bar{a} \cdot \overline{\lambda q} = \bar{\beta}$. Άρα $\overline{\lambda q}$ είναι λύση της (1).

Αν $\bar{x}_1$ είναι μια λύση της (1), για κάθε $k = 0, 1, \dots, d-1$ η $\bar{x}_k$ που δίνεται από την (2) είναι επίσης λύση, γιατί

$$\bar{a}\bar{x}_k = \bar{a}\bar{x}_1 + \bar{a}k\frac{\bar{m}}{d} = \bar{\beta} + k\frac{\bar{a}}{d}\bar{m} = \bar{\beta} + \bar{0} = \bar{\beta}$$

αφού d/a . Για $0 \leq \mu < k$, έχουμε $0 < (k - \mu)\frac{m}{d} < m$ άρα στο $\mathbb{Z}_m$

$$\bar{x}_k - \bar{x}_\mu = (k - \mu)\frac{\bar{m}}{d} \neq \bar{0}$$

δηλαδή οι λύσεις (2) είναι διάφορες μεταξύ τους. Για κάθε λύση $\bar{x}$ της (1) έχουμε

$$\bar{a} \cdot \bar{x} = \bar{\beta} = \bar{a} \cdot \bar{x}_1, \text{ συνεπώς } ax - ax_1 = mq:$$

Αν $m = m_1d$, $a = a_1d$, παίρνουμε $a_1(x - x_1) = m_1q$ ή $m_1/a_1(x - x_1)$. Επειδή $(m_1, a_1) = 1$, $m_1/x - x_1$, δηλαδή

$$\eta \quad x \equiv x_1 \left(\text{mod } \frac{m}{d} \right)$$

$$\eta \quad x - x_1 = 0, \frac{m}{d}, 2\frac{m}{d}, \dots, (d-1)\frac{m}{d}$$

άρα στο $\mathbb{Z}_m$ έχουμε τις λύσεις

$$\bar{x}_1, \overline{x_1 + \frac{m}{d}}, \dots, \overline{x_1 + (d-1)\frac{m}{d}} \quad \square$$

Παράδειγμα 1. Βρείτε το πλήθος των λύσεων και τις λύσεις των εξισώσεων

- i) $\bar{3}\bar{x} = \bar{2}$ στο $\mathbb{Z}_7$ ή $3x \equiv 2 \pmod{7}$
- ii) $\bar{4}\bar{x} = \bar{5}$ στο $\mathbb{Z}_6$ ή $4x \equiv 5 \pmod{6}$
- iii) $\bar{3}\bar{x} = \bar{11}$ στο $\mathbb{Z}_{14}$ ή $3x \equiv 11 \pmod{14}$
- iv) $\bar{6}\bar{x} = \bar{12}$ στο $\mathbb{Z}_9$ ή $6x \equiv 12 \pmod{9}$

Λύση. i) Το $\mathbb{Z}_7$ είναι σώμα. Συνεπώς το $\bar{3}$ αντιστρέφεται. 'Αρα η εξίσωση δέχεται μια μόνο λύση $\bar{x} \in \mathbb{Z}_7$, την $\bar{x} = \bar{3}^{-1} \cdot \bar{2} = \bar{5} \cdot \bar{2} = \bar{10} = \bar{3}$

ii) Επειδή $(4, 6) = 2$ και ο 2 δεν διαιρεί τον 5, η εξίσωση δεν δέχεται λύση.

iii) 'Εχουμε $(3, 14) = 1/11$, συνεπώς η εξίσωση έχει μια μόνο λύση. Επειδή $\bar{3} \cdot \bar{5} = \bar{1}$ στο $\mathbb{Z}_{14}$, έχουμε $\bar{5} \cdot \bar{3} \cdot \bar{x} = \bar{5} \cdot \bar{11}$ ή $\bar{x} = \bar{55} = \bar{13}$.

iv) Επειδή $(6, 9) = 3/12$, υπάρχουν 3 λύσεις στο $\mathbb{Z}_9$. Μια λύση είναι η $\bar{x} = \bar{2}$. 'Αρα οι λύσεις είναι $\bar{2}, \bar{2} + 1 \cdot \bar{3} = \bar{5}, \bar{2} + 2 \cdot \bar{3} = \bar{8}$.

Πρόταση 2. Έστω a, β, γ ακέραιοι. Η εξίσωση

$$ax + \beta y = \gamma \quad (1)$$

έχει λύση $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ τότε και μόνο, όταν $(a, \beta)/\gamma$. Αν $(a, \beta) = 1$ και (x_0, y_0) είναι μια λύση της (1), το σύνολο των λύσεων (x, y) της (1) είναι

$$(x_0 + \beta\lambda, y_0 - a\lambda), \quad \lambda \in \mathbb{Z}$$

Απόδειξη. Έστω ότι $d = (a, \beta)/\gamma$. Υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $ax + \beta y = d$. Αν $\gamma = dm$, έχουμε $a(xm) + \beta(y m) = \gamma$, συνεπώς (xm, ym) είναι λύση της (1). Αν η (1) έχει λύση, τότε $d/ax + \beta y = \gamma$. Έστω ότι $(a, \beta) = 1$. Αν $(x_0, y_0), (x, y)$ είναι δύο λύσεις της (1), έχουμε

$$ax + \beta y = \gamma = ax_0 + \beta y_0, \quad a(x - x_0) = \beta(y_0 - y)$$

Επειδή $(a, \beta) = 1$, έπεται ότι $\beta/x - x_0$. Αν θέσουμε $x - x_0 = \beta\lambda$, έχουμε $x = x_0 + \beta\lambda, y = y_0 - a\lambda$ με $\lambda \in \mathbb{Z}$. Αντίστροφα, κάθε ζεύγος ακεραίων $(x_0 + \beta\lambda, y_0 - a\lambda)$ είναι λύση της (1). $\square$

Παράδειγμα 2. Να λυθεί στο $\mathbb{Z}$ η εξίσωση

$$2x + 3y = 7 \quad (1)$$

Επειδή $(2, 3) = 1$, η εξίσωση δέχεται λύση. Αναζητούμε μια μερική λύση (x_0, y_0) . Έχουμε $x = \frac{7-3y}{2} = 3 - y + \frac{1-y}{2}$. Αρχεί $y_0 = 1$, οπότε $x_0 = 2$. Η γενική λύση της εξίσωσης είναι $x = 2 + 3\lambda, y = 1 - 2\lambda$.

Παρατήρησῃ. Είδαμε στο προηγούμενο κεφάλαιο ένα δεύτερο τρόπο λύσης: Η εξίσωση (1) στο $\mathbb{Z}_2$ γράφεται $\bar{y} = \bar{1}$, οπότε $y = 1 + 2a$. Από την (1) παίρνουμε με αντικατάσταση $x = 2 - 3a, a \in \mathbb{Z}$.

Παράδειγμα 3. Να λυθεί στο $\mathbb{Z}$ η εξίσωση $65x + 58y = 427$.

Η εξίσωση έχει λύση, γιατί $(65, 58) = (5 \cdot 13, 2 \cdot 29) = 1$. Θ' αναζητήσουμε μια μερική λύση (x_0, y_0) . Έχουμε $x = \frac{427 - 58y}{65} = \frac{65 \cdot 6 + 37 - 65y + 7y}{65} = 6 - y + \frac{37 + 7y}{65}$. Για $y = 0, 1, 2, 3, 4, \dots$ βρίσκουμε ότι $\frac{37 + 7y}{65} = \frac{37}{65}, \frac{44}{65}, \frac{51}{65}, \frac{65}{65} = 1$. Άρα $y_0 = 4$ και $x_0 = 3$. Η γενική λύση της εξίσωσης είναι $x = 3 + 58\lambda, y = 4 - 65\lambda$.

Με το δεύτερο τρόπο η εξίσωση λύνεται ως εξής: Στο $\mathbb{Z}_{58}$ γράφεται $\overline{7x} + \bar{0} = \overline{21}$ ή $\overline{7x} = \overline{21}$ ή $7x = 21 + 58z$. Η εξίσωση αυτή στο $\mathbb{Z}_7$ γράφεται $\bar{0} = \bar{0} + \bar{2z}$

ή $2\bar{z} = \bar{0}$, οπότε $\bar{z} = \bar{0}$ (αφού $\mathbb{Z}_7$ είναι σώμα). Άρα $z = 7\mu$, $7x = 21 + 58 \cdot 7\mu$, $x = 3 + 58\mu$. Από την εξίσωση με αντικατάσταση παίρνουμε $y = 4 - 65\mu$.

Ορισμός. Μια εξίσωση της οποίας ζητούμε ακέραιες τιμές των αγνώστων λέγεται **Διοφαντική εξίσωση**.

Με τις ακέραιες λύσεις συγκεκριμένων εξισώσεων ασχολείται ο Διόφαντος (250 π.Χ.) στο κλασσικό έργο του τα "Αριθμητικά". Γενική μεθοδολογία αναπτύσσεται για πρώτη φορά από τους Ινδούς κατά τον μεσαίωνα. Οι Διοφαντικές εξισώσεις αποτελούν μάλλον αιώνιο πρόβλημα της θεωρίας των αριθμών. Η διοφαντική εξίσωση του Fermat

$$x^n + y^n = z^n$$

απασχόλησε τους μεγαλύτερους μαθηματικούς και η εικασία ότι για $n \geq 3$ δεν έχει ακέραιες λύσεις αποδείχτηκε μόλις πριν δύο χρόνια. Οι προσπάθειες όμως που έγιναν για την απόδειξη αυτή συνέβαλαν στην εισαγωγή νέων εννοιών και ανακαλύψεων.

Η εξίσωση του Fermat για $n = 2$ έχει λύση (άσκ.50). Γενικά η λύση διοφαντικών εξισώσεων είναι πρόβλημα δύσκολο και πολύπλοκο.

Παράδειγμα 4. Η εξίσωση $x^2 + 3xy - 2y^2 = 122$ δεν έχει λύση (x, y) με $x, y \in \mathbb{Z}$.

Έστω ότι η εξίσωση έχει λύση στο $\mathbb{Z}^2$. Γράφεται $\left(x + \frac{3}{2}y\right)^2 - \frac{9}{4}y^2 - 2y^2 = 122$ ή $(2x + 3y)^2 - 17y^2 = 488$. Στο σώμα $\mathbb{Z}_{17}$ γράφεται $\overline{2x + 3y^2} = \overline{12}$. Αλλά για $\bar{z} \in \mathbb{Z}_{17}$, έχουμε $\bar{z}^2 \in \{\bar{0}, \bar{1}, \bar{4}, \bar{8}, \bar{9}, \bar{13}, \bar{15}, \bar{16}\}$ και άρα $\bar{z}^2 \neq \bar{12} \pmod{17}$.

Θεώρημα (Κινέζικο) 3. Αν οι ακέραιοι $m_1, m_2, \dots, m_k$ είναι σχετικά πρώτοι ανά δύο, οι εξισώσεις

$$\begin{aligned}\bar{x} &= \bar{a}_1 \pmod{m_1} \\ \bar{x} &= \bar{a}_2 \pmod{m_2} \\ &\dots\dots\dots \\ \bar{x} &= \bar{a}_k \pmod{m_k}\end{aligned}\tag{1}$$

έχουν κοινή λύση ως προς x . Για δύο οποιεσδήποτε λύσεις x_0, x των εξισώσεων (1), ισχύει

$$\bar{x} = \bar{x}_0 \pmod{m = m_1 m_2 \dots m_k}$$

Απόδειξη. Επειδή $(m_1, m_i) = 1$, υπάρχουν ακέραιοι β_i, a_i τέτοιοι, ώστε $m_1\beta_i + m_i a_i = 1$. Τότε

$$(m_1\beta_2 + m_2 a_2)(m_1\beta_3 + m_3 a_3) \dots (m_1\beta_k + m_k a_k) = 1$$

ή $m_1\beta + m_2m_3\cdots m_k a = 1$ με $a, \beta \in \mathbb{Z}$. Θέτοντας $y_1 = m_2m_3\cdots m_k a$, έχουμε $m_1\beta + y_1 = 1$ ή

$$\bar{y}_1 = \bar{1} \pmod{m_1}, \quad \bar{y}_1 = \bar{0} \pmod{m_2\cdots m_k}$$

Προφανώς $\bar{y}_1 = \bar{0} \pmod{m_i}$ για $i \neq 1$. Έστω m_j το γινόμενο $m_1m_2\cdots m_j$, $\cdots m_k = \frac{m}{m_j}$ (παραλείπεται ο παράγοντας m_j). Για κάθε j υπάρχει συνεπώς ακέραιος y_j τέτοιος, ώστε

$$\bar{y}_j = \bar{1} \pmod{m_j}, \quad \bar{y}_j = \bar{0} \pmod{m_i} \text{ για } i \neq j$$

και $\bar{y}_j = \bar{0} \pmod{m_i}$ για $i \neq j$. Ο ακέραιος

$$x = a_1y_1 + a_2y_2 + \cdots + a_ky_k$$

πληρεί τις εξισώσεις (1), γιατί $\pmod{m_j}$ έχουμε

$$\bar{x} = \bar{a}_1 \cdot \bar{0} + \cdots + \bar{a}_j \cdot \bar{1} + \cdots + \bar{a}_k \cdot \bar{0} = \bar{a}_j$$

Η μοναδικότητα της λύσης του συστήματος (1) $\pmod{m}$ προκύπτει ως εξής: Έστω x, x_0 δύο λύσεις. Τότε $\bar{x} = \bar{x}_0 \pmod{m_i}$ για κάθε $i = 1, 2, \dots, k$, συνεπώς $m_i/x - x_0$ ($i = 1, 2, \dots, k$) και αφού $(m_i, m_j) = 1$ για $i \neq j$, $m_1m_2\cdots m_k = m/x - x_0$, δηλαδή $\bar{x} = \bar{x}_0 \pmod{m}$. $\square$

Παράδειγμα 5. Βρείτε τις κοινές λύσεις των εξισώσεων

$$\bar{x} = \bar{3} \pmod{4}, \quad \bar{x} = \bar{4} \pmod{5}, \quad \bar{x} = \bar{1} \pmod{3}$$

Λύση. Βρίσκουμε τις λύσεις $\bar{y}_i$ των συστημάτων

$$\begin{array}{lll} \bar{y}_1 = \bar{1} \pmod{4} & \bar{y}_2 = \bar{1} \pmod{5} & \bar{y}_3 = \bar{1} \pmod{3} \\ \bar{y}_1 = \bar{0} \pmod{15} & \bar{y}_2 = \bar{0} \pmod{12} & \bar{y}_3 = \bar{0} \pmod{20} \end{array}$$

Προφανώς $y_1 = 45, y_2 = 36, y_3 = 40$. Άρα $x = 3 \cdot 45 + 4 \cdot 36 + 1 \cdot 40 = 319$.

Παράδειγμα 6. Έστω $p_1, p_2, \dots, p_{1.000.000}$ οι 1.000.000 πρώτοι ακέραιοι κατά σειρά μεγέθους (2, 3, ...). Δείξτε ότι υπάρχουν 1.000.000 διαδοχικοί ακέραιοι $x, x+1, \dots, x+999999$ που ο καθένας διαιρείται με τον κύβο του αντίστοιχου πρώτου.

Λύση. Θεωρούμε το σύστημα

$$\bar{x} = \bar{0} \pmod{2^3}, \bar{x} = -\bar{1} \pmod{3^3}, \dots, \bar{x} = -\overline{999999} \pmod{p_{10^6}^3}$$

Επειδή $(p^3, q^3) = 1$ για διάφορους πρώτους p, q , το σύστημα δέχεται λύση. Μια γενίκευση του Κινέζικου Θεωρήματος είναι το εξής

Θεώρημα 4. Έστω $m_1, m_2, \dots, m_k$ ακέραιοι αριθμοί, $d = (m_1, m_2, \dots, m_k)$ και $m = [m_1, m_2, \dots, m_k]$. Το σύστημα

$$\bar{x} = \bar{a}_1 \pmod{m_1}, \quad \bar{x} = \bar{a}_2 \pmod{m_2}, \quad \dots, \quad \bar{x} = \bar{a}_k \pmod{m_k}$$

έχει λύση τότε και μόνο, όταν

$$(m_i, m_j) \mid a_i - a_j \quad \text{για } i \neq j$$

Αν ισχύει η συνθήκη αυτή, υπάρχει μια μόνο λύση x με $0 \leq x < m$.

Απόδειξη. Περιοριζόμαστε στην απόδειξη για $k = 2$. Έστω το σύστημα

$$\bar{x} = \bar{a} \pmod{m_1}, \quad \bar{x} = \bar{\beta} \pmod{m_2} \quad (1)$$

και $d = (m_1, m_2)$, $m = [m_1, m_2]$. Αν ο ακέραιος x πληρεί και τις δύο εξισώσεις (1), έχουμε

$$x = a + \lambda_1 m_1 = \beta + \lambda_2 m_2$$

με $\lambda_1, \lambda_2 \in \mathbb{Z}$, συνεπώς $a - \beta = \lambda_2 m_2 + (-\lambda_1) m_1$ ή

$$\overline{a - \beta} = \bar{\lambda}_2 \bar{m}_2 \pmod{m_1} \quad (2)$$

Αντίστροφα, η (2) έχει λύση ως προς $\bar{\lambda}_2$ τότε και μόνο, όταν $d = (m_1, m_2) \mid a - \beta$ (θεώρ. 1). Στην περίπτωση αυτή, υπάρχει ένα μόνο $\lambda_2 \pmod{\frac{m_1}{d}}$ και άρα μία μόνο λύση x με $0 \leq x < \frac{m_1 m_2}{d} = m$. $\square$

3. ΑΡΙΘΜΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

Μια συνάρτηση $f : \mathbb{N} \rightarrow \mathbb{C}$ λέγεται **αριθμητική συνάρτηση**. Αν για οποιουσδήποτε σχετικά πρώτους αριθμούς m, n , ισχύει $f(mn) = f(m)f(n)$, η αριθμητική συνάρτηση f λέγεται **πολλαπλασιαστική**. Για τη μελέτη προβλημάτων της Θεωρίας αριθμών χρησιμοποιούνται διάφορες αριθμητικές συναρτήσεις. Οι βασικότερες από αυτές είναι:

1. $\varphi(n)$ = ο αριθμός των θετικών ακεραίων $\leq n$, οι οποίοι είναι σχετικά πρώτοι με τον n . Η συνάρτηση φ λέγεται συνάρτηση “φί” του Euler.

2. $d(n)$ = αριθμός των θετικών διαιρετών του n .
3. $\sigma(n)$ = το άθροισμα των θετικών διαιρετών του n .
4. $\nu(n)$ = ο αριθμός των διαφόρων πρώτων παραγόντων του n .
5. $\Omega(n)$ = ο αριθμός των πρώτων παραγόντων του n .
Ένας θετικός ακέραιος n λέγεται **τετραγωνικά ελεύθερος**, αν ο 1^2 είναι ο μόνος αριθμός a^2 που διαιρεί τον n .
6. $\mu(n) = \begin{cases} 0; & n \text{ τετραγωνικά ελεύθερος} \\ (-1)^{\nu(n)}; & n \text{ όχι τετραγωνικά ελεύθερος} \end{cases}$
 $\mu(1) = 1$.

Παραδείγματα. Στον παρακάτω πίνακα δίνονται οι τιμές των συναρτήσεων $\varphi, d, \dots, \mu$ στους αριθμούς $1, 2, \dots, 6$.

v	1	2	3	4	5	6
φ	1	1	2	2	4	2
d	1	2	2	3	2	4
σ	1	3	4	7	6	12
ν	0	1	1	1	1	2
Ω	0	1	1	2	1	2
μ	1	-1	-1	0	-1	1

Θεώρημα 1. Αν m, n σχετικά πρώτοι ακέραιοι και φ η συνάρτηση Euler, ισχύει $\varphi(mn) = \varphi(m)\varphi(n)$.

Απόδειξη. Έστω $U(m) = \{x; 0 \leq x < m, (x, m) = 1\}$. Αν $x \in U(m)$, $y \in U(n)$, τότε $xn + ym \in U(mn)$. Πραγματικά, έστω d πρώτος που διαιρεί τους mn και $xn + ym$. Επειδή $(m, n) = 1$, ο d διαιρεί ένα μόνο από τους m, n , έστω d/m και $d \neq n$. Τότε d/ym και $d/(xn + ym) - ym = xn$, δηλαδή d/x , πράγμα άτοπο.

Έστω τώρα $x \in \{0, 1, 2, \dots, m-1\}$, $y \in \{0, 1, 2, \dots, n-1\}$. Οι ακέραιοι $xn + ym$, πλήθους mn , έχουν διάφορες κλάσεις mod (mn) , γιατί

$$\overline{xn + ym} = \overline{x'n + y'm} \pmod{mn}$$

συνεπάγεται $(x - x')n + (y - y')m = amn$ ή $m/(x - x')n$ και $n/(y - y')m$, οπότε $m/x - x'$ και $n/y - y'$, δηλαδή $x = x'$ και $y = y'$.

Έτσι κάθε κλάση $\bar{\beta} \in \mathbb{Z}_{mn}$ έχει αντιπρόσωπο β της μορφής $xn + ym$ με $0 \leq x < m$, $0 \leq y < n$. Αν όμως $(\beta, mn) = 1$, έχουμε $(x, m) = 1 = (y, n)$. Πραγματικά, έστω $(x, m) = d \neq 1$. Τότε

$$(\beta, m) = (xn + ym, m) = (xn, m) = (x, m) = d \neq 1$$

και άρα d/β , d/mn αντίθετα με την υπόθεση μας. Όμοια $(y, n) = 1$. Έστω $\mathbb{Z}_m^*$ το σύνολο των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_m$. Η συνάρτηση $f: \mathbb{Z}_m^* \rightarrow \mathbb{Z}_{mn}^*$ με τιμή $f(\bar{x}, \bar{y}) = \overline{xn + ym}$ είναι αμφιμονοσήμαντη και επί. Άρα τα σύνολα $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$, $\mathbb{Z}_{mn}^*$ έχουν το ίδιο πλήθος στοιχείων, δηλαδή $\varphi(m)\varphi(n) = \varphi(mn)$. $\square$

Θεώρημα 2. i) Αν p είναι πρώτος αριθμός,

$$\varphi(p^m) = p^m \left(1 - \frac{1}{p}\right)$$

ii) Αν $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ η ανάλυση του n σε γινόμενο διαφόρων πρώτων παραγόντων $p_1, p_2, \dots, p_k$

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Απόδειξη. i) Οι διαιρέτες του p^m είναι $1, p, p^2, \dots, p^{m-1}$. Κάθε αριθμός $a < p^m$ διάφορος των p^i με $i \leq m-1$ είναι σχετικά πρώτος με τον p^m . Άρα

$$\varphi(p^m) = p^m - p^{m-1} = p^m \left(1 - \frac{1}{p}\right)$$

ii) Σύμφωνα με το θεώρημα 1 έχουμε

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{a_1}) \varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k}) \\ &= p_1^{a_1} \left(1 - \frac{1}{p_1}\right) p_2^{a_2} \left(1 - \frac{1}{p_2}\right) \cdots p_k^{a_k} \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned} \quad \square$$

Παράδειγμα. 1) $\varphi(28) = \varphi(2^2 \cdot 7) = 28 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{7}\right) = 12$.

2) $\varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$.

Θεώρημα 3. Αν $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ είναι η ανάλυση του n σε γινόμενο πρώτων παραγόντων $p_i (p_i \neq p_j)$, τότε

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_m^{a_m+1} - 1}{p_m - 1} \quad (1)$$

Απόδειξη. Θεωρούμε το γινόμενο

$$(1 + p_1 + \cdots + p_1^{a_1})(1 + p_2 + \cdots + p_2^{a_2}) \cdots (1 + p_m + \cdots + p_m^{a_m}) \quad)$$

Κάνοντας τις πράξεις βρίσκουμε ότι ισούται με το άθροισμα όλων των γινόμενων

$$p_1^{s_1} p_2^{s_2} \cdots p_m^{s_m} \quad (3)$$

με $0 \leq s_i \leq a_i$ ($i = 1, 2, \dots, m$). Κάθε γινόμενο εμφανίζεται ως όρος μια φορά. Αλλά οι διαιρέτες του n είναι οι όροι (2). Άρα το γινόμενο (2) είναι το άθροισμα των θετικών διαιρετών του n και ισούται με το δεύτερο μέλος της (1), γιατί

$$1 + p_i + \cdots + p_i^{a_i} = \frac{p_i^{a_i+1} - 1}{p_i - 1} \quad \square$$

Θεώρημα 4. Αν $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ είναι η ανάλυση του n σε γινόμενο πρώτων παραγόντων p_i ($p_i \neq p_j$), τότε

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_m + 1)$$

Απόδειξη. Αν στο γινόμενο (2) που χρησιμοποιήσαμε στην απόδειξη του προηγούμενου θεωρήματος κάθε όρος (3) αντικατασταθεί με 1, αν δηλαδή $p_i = 1$, το άθροισμα των διαιρετών μας δίνει το πλήθος των θετικών διαιρετών του n . Αφού $1 + p_i + \cdots + p_i^{a_i} = a_i + 1$ για $p_i = 1$, το συμπέρασμα αποδείχτηκε. $\square$

4. ΙΣΟΔΥΝΑΜΙΕΣ ΑΝΩΤΕΡΟΥ ΒΑΘΜΟΥ

Έστω $f(x) = a_n x^n + \cdots + a_0$ ένα πολυώνυμο με συντελεστές a_i ακεραίους και m ένας αχέραιος. Ένα ενδιαφέρον πρόβλημα της θεωρίας αριθμών, που παραμένει ανοικτό μέχρι σήμερα, είναι η λύση των πολυωνυμικών ισοδυναμιών

$$f(x) \equiv 0 \pmod{m}. \quad (1)$$

Το πρόβλημα αυτό συνδέεται με τη θεωρία πολυωνύμων και γι' αυτό θα επανέλθουμε αργότερα.

Αν x_0 είναι μια λύση της (1), για κάθε $\lambda \in \mathbb{Z}$ ο αριθμός $x_0 + \lambda m$ είναι λύση, γιατί $\text{mod } m$ έχουμε

$$\overline{(x_0 + \lambda m)^k} = \overline{x_0 + \lambda m}^k = \overline{x_0^k}$$

και συνεπώς $\overline{f(x_0 + \lambda m)} = \overline{f(x_0)} = \bar{0} \pmod{m}$. Έτσι δύο λύσεις της (1) είναι διάφορες, αν οι κλάσεις τους $\text{mod } m$ είναι διάφορες.

Οι ισοδυναμίες

$$x^2 \equiv 1, \quad x^2 \equiv 4 \pmod{5}$$

έχουν λύσεις $x = 1, 4$ αντίστοιχα $x = 2, 3$. Οι ισοδυναμίες

$$x^2 \equiv 2, \quad x^2 \equiv 3 \pmod{5}$$

δεν έχουν λύση.

Ορισμός 1. Αν ο p είναι πρώτος και η ισοδυναμία

$$x^2 \equiv a \pmod{p} \quad (2)$$

έχει λύση, ο ακέραιος a λέγεται **τετραγωνικό υπόλοιπο** ως προς μέτρο p . Έτσι οι αριθμοί $1, 4$ είναι τετραγωνικά υπόλοιπα ως προς μέτρο 5 , ενώ οι αριθμοί $2, 3$ δεν είναι. Παρατηρούμε ότι οι μισοί από τους αριθμούς $1, 2, 3, 4$ είναι τετραγωνικά υπόλοιπα ως προς μέτρο 5 και οι άλλοι μισοί δεν είναι. Γενικά ισχύει το

Θεώρημα 1. Έστω p πρώτος $\neq 2$. Υπάρχουν $\frac{1}{2}(p-1)$ τετραγωνικά υπόλοιπα ως προς μέτρο p και $\frac{1}{2}(p-1)$ μη τετραγωνικά υπόλοιπα ως προς μέτρο p . Ένα σύνολο αριθμών που είναι τετραγωνικά υπόλοιπα ως προς μέτρο p είναι οι αριθμοί $1^2, 2^2, \dots, \left(\frac{1}{2}(p-1)\right)^2$, οι οποίοι ανά δύο δεν είναι ισοδύναμοι $\pmod{p}$.

Απόδειξη. Η ισοδυναμία $x^2 \equiv a \pmod{p}$ για κάθε $a = k^2 \in \{1^2, 2^2, \dots, \left(\frac{1}{2}(p-1)\right)^2\}$ έχει λύση, την $x = k$. Αν $0 \leq k < \frac{1}{2}(p-1)$, έχουμε $m^2 - k^2 = (m-k)(m+k)$ και $0 < m-k < m+k < p$, συνεπώς $m^2 \not\equiv k^2 \pmod{p}$, δηλαδή οι $\frac{1}{2}(p-1)$ αριθμοί $1^2, 2^2, \dots, \left(\frac{1}{2}(p-1)\right)^2$ είναι τετραγωνικά υπόλοιπα $\pmod{p}$ και ανά δύο μη ισοδύναμοι $\pmod{p}$. $\square$

Αν η ισοδυναμία $x^2 \equiv a \pmod{p}$ δέχεται μια λύση x , δέχεται και τη λύση $p-x$, γιατί $(p-x)^2 = p-x^2 = (-x)^2 = x^2 \equiv a \pmod{p}$. Άρα δέχεται μια λύση x με $0 < x \leq \frac{1}{2}(p-1)$.

Μια ισοδυναμία της μορφής

$$ax^2 + \beta x + \gamma \equiv 0 \pmod{p}, \quad a \not\equiv 0 \pmod{p} \quad (3)$$

με $p > 2$ ανάγεται σε ισοδυναμία της μορφής (2), γιατί, αφού $\bar{a} \not\equiv 0$ στο σώμα $\mathbb{Z}_p$, υπάρχει $\bar{b}$ με $\bar{a}\bar{b} = \bar{1}$ και η (3) είναι ισοδύναμη της $b(ax^2 + \beta x + \gamma) \equiv 0 \pmod{p}$ ή της $x^2 + b\beta x + \gamma \equiv 0 \pmod{p}$ που γράφεται

$$\left(x + \frac{b\beta}{2}\right)^2 + \gamma - \frac{b^2\beta^2}{4} \equiv 0 \pmod{p}$$

$$\text{ή} \quad y^2 \equiv a \pmod{p} \quad (4)$$

όπου $y = x + \frac{b\beta}{2}$, $a = \frac{b^2\beta^2 - 4\gamma}{4}$. Σύμφωνα με το θεώρημα 1 η (4) έχει λύση τότε και μόνο, όταν το a είναι τετραγωνικό υπόλοιπο ως προς μέτρο p .

Θεώρημα 2. Έστω $(m_1, m_2) = 1$. Το πλήθος των λύσεων της ισοδυναμίας

$$f(x) \equiv 0 \pmod{m_1 m_2} \quad (1)$$

είναι το γινόμενο του αριθμού των λύσεων των ισοδυναμιών

$$f(x) \equiv 0 \pmod{m_1} \quad (2)$$

$$f(x) \equiv 0 \pmod{m_2} \quad (3)$$

Αν $m = m_1 m_2 = p_1^{k_1} p_2^{k_2} \cdots p_\lambda^{k_\lambda}$ ($p_1 < p_2 < \cdots < p_\lambda$) η ανάλυση του m σε γινόμενο πρώτων παραγόντων, ο αριθμός των λύσεων της (1) είναι το γινόμενο του αριθμού των λύσεων των λ ισοδυναμιών

$$f(x) \equiv 0 \pmod{p_i^{k_i}} \quad 1 \leq i \leq \lambda \quad (4)$$

Απόδειξη. Προφανώς κάθε λύση της (1) είναι και λύση των (2) και (3). Αντίστροφα, αν x_1, x_2 λύσεις των (2), (3) αντίστοιχα, και x μια λύση των $x \equiv x_1 \pmod{m_1}$, $x \equiv x_2 \pmod{m_2}$, η οποία υπάρχει και είναι μοναδική $\pmod{m_1 m_2}$ κατά το Κινέζικο θεώρημα, τότε $m_1/f(x)$, $m_2/f(x)$, συνεπώς $m_1 m_2/f(x)$. $\square$

ΑΣΚΗΣΕΙΣ

1. Ν' αποδειχτεί ότι για κάθε ακέραιο n υπάρχουν μοναδικοί ακέραιοι q, v τέτοιοι, ώστε $n = 15q + v$ με $|v| \leq 7$.
2. Έστω a, β, γ τρεις φυσικοί αριθμοί. Δείξτε ότι $(a, \beta, \gamma) = 1 \Leftrightarrow (a, \beta) = 1 = (a, \gamma)$.
3. Έστω a, β δύο ακέραιοι τέτοιοι, ώστε $23/a\beta$. Δείξτε ότι $23^2/a^2$ ή $23^2/\beta^2$.
4. Έστω $n = 2^a \cdot 3^b$ με $a, b \geq 0, a, b \in \mathbb{Z}$.
 - (i) Βρείτε τους διαιρέτες του n .
 - (ii) Δείξτε ότι είναι πλήθους $(a+1)(b+1)$.
5. Δείξτε ότι για κάθε φυσικό n οι ακέραιοι $3n+4, 5n+7$ είναι σχετικά πρώτοι.
6. Δείξτε ότι για κάθε $n \in \mathbb{Z}$
 - i) $(n, n+4)/4$
 - ii) $(n+1, n^2-n+1)/3$
7. Δείξτε ότι, αν $(a, \beta) = 1$, τότε $(a^2 + \beta^2, a + \beta) \in \{1, 2\}$.
8. Βρείτε το μ.κ.δ των αριθμών
 - a) 22471, 3266
 - β) 20384, 10725
9. Γράψτε το μ.κ.δ των αριθμών $a, \beta, \dots$ σαν γραμμικό συνδυασμό αυτών, αν
 - i) $a = 49349, \beta = 15555$
 - ii) $a = 15, \beta = 4, \gamma = 35$
10. Δείξτε ότι για $m \neq n$ οι αριθμοί $2^{2^m} + 1, 2^{2^n} + 1$ είναι σχετικά πρώτοι.
11. Δείξτε ότι
 - i) $3/n(n+1)(2n+1)$
 - ii) $5/n^5 + 4n$
 - iii) $10/n(n^2+1)(n^2+4)$
 - iv) $35/6^{2^n} - 6^{2^{(n-1)}}$
 - v) $70/101^{64} - 1$
12. Να λύσετε στο σώμα $\mathbb{Z}_7$ τις εξισώσεις $5\bar{x} = \bar{4}, \bar{y}^2 - \bar{y} + \bar{1} = 0$.
13. Βρείτε τα αντίστροφα των στοιχείων $\bar{4} \in \mathbb{Z}_7, \bar{11} \in \mathbb{Z}_{31}$.
14. Σε ποιο σώμα $\mathbb{Z}_p$ το σύστημα $3x + y = 1, 5x + 4y = 2$ δεν έχει λύση;
15. Να λυθεί στο δακτύλιο $\mathbb{Z}_9$ το σύστημα $2x + y - z = 5, 3x - 2y + z = 4, x + 2y - 3z = 6$.
16. Βρείτε τα αντιστρέψιμα στοιχεία των δακτυλίων $\mathbb{Z}_6, \mathbb{Z}_9$ και τα αντίστροφά τους.

17. Βρείτε το μικρότερο θετικό ακέραιο x , αν $9/x - 7$, $7/x - 6$, $5/x - 2$.

18. Έστω x, y δύο ακέραιοι. Δείξτε ότι

$$19/3x + 5y \Leftrightarrow 19/13x + 9y$$

19. Δείξτε ότι η εξίσωση $\bar{x}^2 = \bar{3} \pmod{4}$ δεν έχει λύση και βάσει αυτού ότι δεν έχουν λύσεις οι εξισώσεις $y^2 = \bar{12}$ στο $\mathbb{Z}_{16}$ και $z^2 = \bar{4444}$ στο $\mathbb{Z}_{10^4}$.

20. Ποιο το υπόλοιπο της διαίρεσης του αριθμού $1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ με 30.

21. Αν a, β, γ ακέραιοι τέτοιοι, ώστε $\beta\gamma \equiv 1 \pmod{a}$, $\gamma a \equiv 1 \pmod{\beta}$, $a\beta \equiv 1 \pmod{\gamma}$, δείξτε ότι $\beta\gamma + \gamma a + a\beta \equiv 1 \pmod{a\beta\gamma}$.

22. Δείξτε ότι οι όροι της αριθμητικής προόδου $2, 5, 8, 11, \dots$ δεν είναι τετράγωνα ακεραίων αριθμών.

23. Η εξίσωση $x^2 - 3y^2 = 992$ έχει λύση (x, y) με $x, y \in \mathbb{Z}$;

24. Γιατί στο δακτύλιο $\mathbb{Z}_{2n+1}$ υπάρχουν το πολύ $n + 1$ διάφορα τετράγωνα;

25. Έστω $A(n)$ το σύνολο των πρώτων διαιρετών του n .

- i) Βρείτε τα σύνολα $A(1), A(2), A(6), A(12), A(p)$, όπου p πρώτος.
- ii) Αν $q/n, A(q) \subseteq A(n)$.
- iii) Αν q είναι κοινός παράγοντας και r κοινό πολλαπλάσιο των m, n δείξτε ότι $A(q) \subseteq A(m) \cap A(n)$, $A(m) \cup A(n) \subseteq A(r)$.
- iv) $A((m, n)) = A(m) \cap A(n)$.
- v) $A([m, n]) = A(m) \cup A(n)$.

26. Έστω $B(n)$ το σύνολο των πρώτων δυνάμεων που διαιρούν τον n . Δείξτε ότι

- i) $B(1) = 1, B(2) = \{1, 2\}, B(12) = \{1, 2, 2^2, 3\}$.
- ii) $B((m, n)) = B(m) \cap B(n), B([m, n]) = B(m) \cup B(n)$.

27. Έστω η ακολουθία (a_n) με $a_1 = 2$ και $a_{n+1} = a_n^2 - a_n + 1$. Δείξτε ότι

- i) $(a_k, a_\lambda) = 1$ για $k \neq \lambda$.
- ii) Ο 19 δεν διαιρεί τον a_n για $n = 1, 2, \dots$

28. Οι αριθμοί Fibonacci $1, 1, 2, 3, 5, 8, \dots$ ορίζονται επαγωγικά από την ισότητα

$$a_{n+1} = a_n + a_{n-1} \quad , \text{ με } a_1 = 1, a_2 = 1$$

N' αποδειχτεί ότι

- 1) $(a_n, a_{n+1}) = 1$.
- 2) $a_n^2 - a_{n-1}a_{n+1} = (-1)^{n-1}$ για $n \geq 1$.
- 3) $m/n \Rightarrow a_m/a_n$.
- 4) $(m, n) = d \Rightarrow (a_m, a_n) = a_d$.
- 5) $(m, n) = 1 \Rightarrow a_m a_n / a_{mn}$.

29. Έστω ο ακέραιος $n = a_k a_{k-1} \cdots a_0$, όπου a_i τα ψηφία του στο δεκαδικό σύστημα αρίθμησης. Έστω $m = \beta_{k-1} \cdots \beta_0$ ο ακέραιος με

$$\begin{aligned}\beta_i &= a_{i+1}, i > 0 \\ \beta_0 &\equiv a_1 - 2a_0 \pmod{7}\end{aligned}$$

Δείξτε ότι $m \equiv 0 \pmod{7} \Leftrightarrow n \equiv 0 \pmod{7}$.

30. Για ποιές τιμές του φυσικού n απλοποιείται το κλάσμα $\frac{2n^7 + 1}{3n^3 + 2}$ (δίνεται ότι ο αριθμός 1163 είναι πρώτος).

31. Αν ο αριθμός $2^n + 1$ είναι πρώτος, δείξτε ότι $n = 2^k$.

32. Αν ο αριθμός $2^p - 1$ είναι πρώτος, τότε και ο p είναι πρώτος.

33. Δείξτε ότι $(m, n)^2 = (m^2, n^2)$.

34. Αν οι ακέραιοι a, β, γ είναι περιττοί, τότε $(a, \beta, \gamma) = \left(\frac{a+\beta}{2}, \frac{\beta+\gamma}{2}, \frac{\gamma+a}{2}\right)$.

35. Να λύσετε στο $\mathbb{Z}$ την εξίσωση $6x + 15y + 20z = 17$.

36. Αν φ είναι η συνάρτηση Euler, βρείτε τις τιμές $\varphi(60)$, $\varphi(360)$.

37. Αν $d_1, d_2, \dots$, οι θετικοί διαιρέτες του 12, δείξτε ότι $\varphi(d_1) + \varphi(d_2) + \dots = 12$.

38. Να λύσετε την εξίσωση $\varphi(n) = 4$.

39. Να λύσετε το σύστημα

$$x \equiv 0 \pmod{2}, \quad x \equiv 1 \pmod{3}, \quad x \equiv 2 \pmod{5}$$

40. Να λυθεί το σύστημα

$$26x - 141y = -697, \quad 55x - 112y = 202$$

στα σώματα $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ και μετά στον δακτύλιο $\mathbb{Z}$.

41. Να λυθεί το σύστημα

$$x \equiv 36 \pmod{41}, \quad x \equiv 5 \pmod{17}$$

42. Δείξτε ότι ο μ.κ.δ των

$$\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}$$

είναι p , αν $n = p^a$ ($a > 0$) και 1 στην αντίθετη περίπτωση.

43. Δείξτε ότι $\varphi(n) \neq 14$ για κάθε $n \in \mathbb{N}$.

44. Αν p είναι πρώτος και $a^{p-1} \equiv 1 \pmod{p^2}$, ο a λέγεται μια λύση του Fermat ως προς p . Ν' αποδειχτεί ότι ο 2 είναι μια λύση του Fermat ως προς 1093, ότι δηλαδή $2^{1092} \equiv 1 \pmod{1093}$.

45. Αν $\varphi(n) \equiv 2 \pmod{4}$, δείξτε ότι $n = p^a$ ή $n = 2p^a$, όπου p πρώτος με $p \equiv 3 \pmod{4}$.

46. Αν $a, \beta \in \mathbb{N}$ και $d = (a, \beta)$, δείξτε ότι $\varphi(ab) = \frac{d\varphi(a)\varphi(\beta)}{\varphi(d)}$.

47. Έστω G_p το σύνολο των συναρτήσεων $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ με τιμή $f(x) = ax + \beta$, όπου $a \not\equiv 0 \pmod{p}$. Δείξτε ότι $(G_p, \circ)$ είναι ομάδα τάξης $p(p-1)$.

48. Έστω $(a, \beta) = 1$, $a, \beta > 0$. Δείξτε ότι κάθε ακέραιος $> a\beta - a - \beta$ γράφεται υπό τη μορφή $ax + \beta y$ με $a \geq 0, \beta \geq 0$, ενώ ο αριθμός $a\beta - a - \beta$ δεν γράφεται υπό τη μορφή αυτή.

Σημείωση. Το πρόβλημα γενικεύεται ως εξής: Αν a, β, γ τρεις θετικοί ακέραιοι και $(a, \beta, \gamma) = 1$, βρείτε το μεγαλύτερο ακέραιο που δεν γράφεται υπό τη μορφή $ax + \beta y + \gamma z$ με $x \geq 0, y \geq 0, z \geq 0$. Αλλά είναι ένα άλυτο πρόβλημα.

49. Έστω $f(x)$ ένα πολυώνυμο με συντελεστές ακραίους. Η ακολουθία

$$f(1), f(2), \dots, f(n), \dots \quad (1)$$

περιέχει άπειρους πρώτους αριθμούς.

Υπόδειξη: Στην περίπτωση που ο σταθερός όρος του f είναι $\neq 0$ και το πλήθος των πρώτων αριθμών στην (1) $p_1, p_2, \dots, p_k$, θεωρήστε το πολυώνυμο $f(p_1 p_2 \cdots p_k y)$.

50. Να υπολογιστούν οι ακέραιοι x, y, z που αποτελούν λύση της εξίσωσης

$$x^2 + y^2 = z^2 \quad (1)$$

Προς τούτο:

1. Αν (x, y, z) είναι μια λύση της (1) και οι x, y, z είναι σχετικά πρώτοι ανά δύο, δείξτε ότι για κάθε λύση (x', y', z') της (1) υπάρχει ακέραιος d τέτοιος, ώστε $x' = dx, y' = dy, z' = dz$.
2. Αν (x, y, z) είναι μια λύση της (1) και οι x, y, z είναι σχετικά πρώτοι ανά δύο, δείξτε ότι $x \not\equiv y \pmod{2}$.
3. Έστω x άρτιος και y περιττός. Δείξτε ότι υπάρχουν ακέραιοι u, v τέτοιοι, ώστε $y = u - v, z = u + v$ με $(u, v) = 1$.
4. Δείξτε ότι οι u, v είναι τετράγωνα ακεραίων σχετικά πρώτων.
5. Βρείτε όλες τις λύσεις της (1).

2 | Αλγεβρικές δομές εσωτερικών νόμων

1. ΗΜΙΟΜΑΔΑ, ΜΟΝΟΕΙΔΕΣ, ΟΜΑΔΑ

Έστω A ένα σύνολο $\neq \emptyset$ και ένας εσωτερικός νόμος " $\cdot$ ", επί του A . Η δομή $(A, \cdot)$ λέγεται:

ημιομάδα, αν ο νόμος " $\cdot$ ", είναι προσεταιριστικός, δηλαδή

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \text{για όλα τα } x, y, z \in A$$

μονοειδές, αν είναι ημιομάδα και ο νόμος έχει ουδέτερο στοιχείο, αν δηλαδή

i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

ii) υπάρχει $e \in A$ τέτοιο, ώστε για κάθε $x \in A$, $x \cdot e = e \cdot x = x$.

ομάδα, αν είναι μονοειδές και κάθε στοιχείο $x \in A$ έχει αντίστροφο.

Άρα $(A, \cdot)$ είναι ομάδα, αν για όλα τα $x, y, z \in A$ ισχύουν τα εξής:

1. $x \cdot y \in A$.

2. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.

3. Υπάρχει $e \in A$ και για κάθε $x \in A$, $x \cdot e = e \cdot x = x$.

4. Για κάθε $x \in A$, υπάρχει $x' \in A$ τέτοιο, ώστε $x \cdot x' = x' \cdot x = e$. Το x' είναι μοναδικό, συμβολίζεται με x^{-1} και λέγεται **αντίστροφο** του x .

Η προσεταιριστική ιδιότητα ενός εσωτερικού νόμου μας επιτρέπει να γράφουμε το "γινόμενο" τριών στοιχείων x, y, z χωρίς παρανθέσεις $x \cdot y \cdot z$, γιατί όποιο από τα δύο γινόμενα $x \cdot y$ ή $y \cdot z$ κι αν υπολογιστεί πρώτο, το αποτέλεσμα είναι το ίδιο:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

Αν ο νόμος μιας ομάδας συμβολίζεται με $+$, το ουδέτερο συμβολίζεται με 0 και το αντίστροφο του x με $-x$, λέγεται δε **αντίθετο** του x . Οι ιδιότητες της ομάδας γράφονται τότε

$$\begin{aligned} x + y &\in A, & x + (y + z) &= (x + y) + z, \\ 0 + x &= x + 0 = x, & x + (-x) &= (-x) + x = 0. \end{aligned}$$

Αν σ' ένα μονοειδές, τα στοιχεία x, y έχουν αντίστροφα, το στοιχείο $x \cdot y$ έχει αντίστροφο και μάλιστα $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$, γιατί

$$\begin{aligned} (y^{-1} \cdot x^{-1}) \cdot (x \cdot y) &= y^{-1} \cdot (x^{-1} \cdot (x \cdot y)) = y^{-1} \cdot ((x^{-1} \cdot x) \cdot y) = \\ &= y^{-1} \cdot (e \cdot y) = y^{-1} \cdot y = e \end{aligned}$$

και όμοια $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e$.

Ορισμός 1. Μια δομή $(A, \cdot)$ λέγεται **αντιμεταθετική**, αν $x \cdot y = y \cdot x$ για όλα τα $x, y \in A$.

Παραδείγματα

1. Έστω A^A το σύνολο των συναρτήσεων $f: A \rightarrow A$. Η σύνθεση $f \circ g$ είναι εσωτερικός νόμος του A^A .

Επειδή είναι προσεταιριστικός, το ζεύγος $(A^A, \circ)$ είναι ημιομάδα. Είναι μονοειδές, γιατί η ταυτοτική συνάρτηση 1_A του A είναι ουδέτερο, αφού $f \circ 1_A = 1_A \circ f = f$ για κάθε συνάρτηση $f: A \rightarrow A$.

Επειδή υπάρχουν συναρτήσεις $g: A \rightarrow A$ που δεν αντιστρέφονται, π.χ. οι σταθερές συναρτήσεις, αφού για τη συνάρτηση $g: A \rightarrow A$ με $g(x) = \alpha$ έχουμε $g \circ f(x) = g(f(x)) = \alpha$ ή $g \circ f \neq 1_A$, έπεται ότι $(A^A, \circ)$ δεν είναι ομάδα.

2. Το σύνολο των αμφιμονοσήμαντων συναρτήσεων $f: E \rightarrow E$ είναι ως προς τη σύνθεση " $\circ$ ", μια ομάδα, η οποία λέγεται **ομάδα μεταθέσεων** του E .

3. $(\mathbb{N}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ είναι μονοειδή.
4. $(\mathbb{N}, +)$ είναι ημιομάδα, δεν είναι μονοειδές, αφού $0 \notin \mathbb{N}$.
5. $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ είναι ομάδες.
6. $(\mathbb{Z}, \cdot)$ δεν είναι ομάδα, γιατί μόνο τα στοιχεία 1, -1 έχουν αντίστροφο στο $\mathbb{Z}$.
7. Έστω G το σύνολο των πινάκων $\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix}$ με $\alpha, \beta \in \mathbb{R}$, και $G' = \left\{ \begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix}; \alpha \in \mathbb{R} \right\}$. Είναι μονοειδή ως προς τον πολλαπλασιασμό των πινάκων 2×2 ;

Έχουμε

$$\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} \alpha x & 0 \\ \beta x & 0 \end{pmatrix} \in G$$

Έτσι ο πολλαπλασιασμός των πινάκων του συνόλου G είναι εσωτερικός νόμος στο G . Επειδή ο πολλαπλασιασμός είναι προσεταιριστικός στο σύνολο των πινάκων $n \times n$, το $(G, \cdot)$ είναι ημιομάδα.

Θα εξετάσουμε αν υπάρχει ουδέτερο του πολλαπλασιασμού στο G .

Έστω ότι το $\begin{pmatrix} e & 0 \\ e' & 0 \end{pmatrix}$ είναι ουδέτερο. Τότε

$$\begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} \begin{pmatrix} e & 0 \\ e' & 0 \end{pmatrix} = \begin{pmatrix} \alpha e & 0 \\ \beta e & 0 \end{pmatrix} \quad \text{ή} \quad \begin{pmatrix} \alpha e & 0 \\ \beta e & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix}$$

για όλα τα $\alpha, \beta \in \mathbb{R}$. Συνεπώς $\alpha e = \alpha$, $\beta e' = \beta$ και $e = e' = 1$. Αλλά

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix} \neq \begin{pmatrix} \alpha & 0 \\ \beta & 0 \end{pmatrix} \quad \text{για } \alpha \neq \beta.$$

Άρα το G δεν είναι μονοειδές.

Προφανώς

$$\begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix} \begin{pmatrix} \beta & 0 \\ \beta & 0 \end{pmatrix} = \begin{pmatrix} \alpha\beta & 0 \\ \alpha\beta & 0 \end{pmatrix} \in G'$$

$$\begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ \alpha & 0 \end{pmatrix}$$

Άρα το G' είναι μονοειδές.

8. Το σύνολο G_n των ριζών της εξίσωσης $z^n = 1$ στο σύνολο των μιγαδικών αριθμών είναι ομάδα ως προς τον πολλαπλασιασμό των μιγαδικών.

Πραγματικά, αν z_1, z_2 είναι δύο ρίζες, έχουμε $(z_1 z_2)^n = z_1^n z_2^n = 1$, δηλαδή $z_1 z_2 \in G$. Ο πολλαπλασιασμός είναι προσεταιριστικός και το ουδέτερο $1 \in G$. Συνεπώς το $(G, \cdot)$ είναι μονοειδές. Αν $z_1 \in G$, τότε $(z_1^{-1})^n = (z_1^n)^{-1} = 1^{-1} = 1$, δηλαδή $z_1^{-1} \in G$. Άρα το G είναι ομάδα.

9. Έστω G_n οι n -ρίζες της μονάδας στο σύνολο των μιγαδικών. Το σύνολο

$$G = \bigcup_1^\infty G_n$$

είναι ομάδα ως προς τον πολλαπλασιασμό του $\mathbb{C}$.

Πραγματικά, έστω $z_1, z_2 \in G$. Τότε $z_1 \in G_{n_1}, z_2 \in G_{n_2}$, οπότε $z_i^{n_i} = 1$ και $(z_1 z_2)^{n_1 n_2} = z_1^{n_1 n_2} \cdot z_2^{n_1 n_2} = (z_1^{n_1})^{n_2} \cdot (z_2^{n_2})^{n_1} = 1$, δηλαδή $z_1 z_2 \in G_{n_1 n_2}$ και $z_1 z_2 \in G$. Αν $z \in G$, τότε $z \in G_n$ για κάποιο n , $z^{-1} \in G_n$, συνεπώς $z^{-1} \in G$. Τέλος $1 \in G$. Άρα $(G, \cdot)$ είναι ομάδα.

10. Έστω $\mathcal{P}(E)$ το σύνολο των υποσυνόλων ενός συνόλου $E \neq \emptyset$. Αν $A, B \subseteq E$, ορίζουμε

$$A \oplus B = (A - B) \cup (B - A)$$

Το $(\mathcal{P}(E), \oplus)$ είναι ομάδα με ουδέτερο το κενό $\emptyset$ υποσύνολο του E και αντίστροφο του A το συμπληρωματικό υποσύνολο A' αυτού στο E (βλ. §1, Κεφ. 0).

2. ΔΑΚΤΥΛΙΟΙ, ΣΩΜΑΤΑ

Οι δακτύλιοι και τα σώματα μοιάζουν με τα συστήματα των ακεραίων και πραγματικών αριθμών. Αποτελούν όμως τόσο μεγάλες γενικεύσεις, ώστε να περιλαμβάνουν ποικίλα και τελείως διάφορα συστήματα αντικειμένων της φύσης και της γνώσης.

Δακτύλιος είναι ένα σύνολο A με δύο εσωτερικούς νόμους $+$, $\cdot$, αυστηρότερα μια τριάδα $(A, +, \cdot)$, με τις παρακάτω ιδιότητες 1-3:

1. $(A, +)$ είναι ομάδα αντιμεταθετική.

Το ουδέτερο αυτής συμβολίζεται με θ_A ή απλά θ και λέγεται μηδέν του δακτυλίου.

2. $(A, \cdot)$ είναι ημιομάδα.

3. Ο δεύτερος νόμος είναι επιμεριστικός ως προς τον πρώτο $+$, δηλαδή

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma \quad \text{και} \quad (\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$$

για όλα τα $\alpha, \beta, \gamma \in A$.

Ο δακτύλιος λέγεται

μοναδιαίος, αν ο δεύτερος νόμος "ο", έχει ουδέτερο,

αντιμεταθετικός, αν ο νόμος $\cdot$ είναι αντιμεταθετικός,

ακέραια περιοχή, αν $\alpha\beta = 0 \Rightarrow \alpha = 0$ ή $\beta = 0$. Στην περίπτωση που $\alpha\beta = 0$ και $\alpha \neq 0 \neq \beta$, ο α λέγεται **αριστερός διαιρέτης** του μηδενός και ο β **δεξιός διαιρέτης** του μηδενός.

Σώμα λέγεται ένας δακτύλιος $(\mathbb{R}, +, \cdot)$, αν είναι μοναδιαίος και κάθε στοιχείο $x \in \mathbb{R}$ **διάφορο** του μηδενός έχει ως προς το δεύτερο νόμο **αντίστροφο**.

Ο λογισμός σε δακτύλιο

Έστω $(\mathbb{R}, +, \cdot)$ ένας δακτύλιος. Ισχύουν οι ιδιότητες:

1. $\alpha \cdot 0 = 0 = 0 \cdot \alpha$ για κάθε $\alpha \in \mathbb{R}$.
2. $\alpha \cdot (-\beta) = -\alpha \cdot \beta = (-\alpha) \cdot \beta$.
3. $\alpha \cdot (\beta - \gamma) = \alpha \cdot \beta - \alpha \cdot \gamma$, $(\alpha - \beta) \cdot \gamma = \alpha \cdot \gamma - \beta \cdot \gamma$.
4. $(-1)\alpha = -\alpha$.
5. $(-1)(-1) = 1$.

Απόδειξη. 1. Είναι για κάθε $\alpha \in \mathbb{R}$

$$\alpha \cdot 0 = \alpha \cdot (0 + 0) = \alpha \cdot 0 + \alpha \cdot 0, \text{ συνεπώς } \alpha \cdot 0 + \alpha \cdot 0 = \alpha \cdot 0 + 0.$$

Αφού $(\mathbb{R}, +)$ είναι ομάδα, κάθε στοιχείο της είναι ομαλό, άρα $\alpha \cdot 0 = 0$.

Όμοια $0 \cdot \alpha = 0$.

2. Επειδή $\alpha \cdot \beta + \alpha \cdot (-\beta) = \alpha [\beta + (-\beta)] = \alpha \cdot 0 = 0$, και κάθε στοιχείο της ομάδας $(\mathbb{R}, +)$ έχει ένα μόνο αντίστροφο (αντίθετο), έχουμε $-\alpha \cdot \beta = \alpha(-\beta)$. Όμοια $(-\alpha)\beta = -\alpha\beta$.

3. Είναι $\alpha \cdot (\beta - \gamma) = \alpha \cdot [\beta + (-\gamma)] = \alpha \cdot \beta + \alpha \cdot (-\gamma) = \alpha \cdot \beta + (-\alpha \cdot \gamma) = \alpha \cdot \beta - \alpha \cdot \gamma$ (κ.λ.π). $\square$

Πρόταση 1. Στο σώμα $(K, +, \cdot)$ δεν υπάρχουν διαιρέτες του μηδενός και το σύνολο $K^* = K - \{0\}$ είναι ομάδα ως προς τον πολλαπλασιασμό.

Απόδειξη. Έστω ότι $\alpha \cdot \beta = 0$. Αν $\alpha \neq 0$, υπάρχει το αντίστροφο α' του α . Συνεπώς

$$\alpha' \cdot (\alpha \cdot \beta) = \alpha' \cdot 0 \text{ ή } (\alpha' \cdot \alpha) \cdot \beta = 0 \text{ ή } 1 \cdot \beta = 0 \text{ ή } \beta = 0.$$

Αυτό σημαίνει ότι ο πολλαπλασιασμός είναι εσωτερικός νόμος στο K^* . Προφανώς $(K^*, \cdot)$ είναι ομάδα με ουδέτερο τη μονάδα του δακτυλίου $(K, +, \cdot)$. $\square$

Πόρισμα 1. Ο δακτύλιος $(K, +, \cdot)$ είναι σώμα τότε και μόνο, όταν $(K^*, \cdot)$ είναι ομάδα.

Παραδείγματα

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ είναι μοναδιαίοι δακτύλιοι χωρίς διαιρέτες του μηδενός. Ο πρώτος δεν είναι σώμα. Οι υπόλοιποι τρεις είναι σώματα αντιμεταθετικά.

2. Το σύνολο G των πινάκων $M(x, y) = \begin{pmatrix} x & -\bar{y} \\ y & \bar{x} \end{pmatrix}$, $x, y \in \mathbb{C}$, $\bar{x}$ ο συζυγής του x , είναι ως προς την πρόσθεση και τον πολλαπλασιασμό των πινάκων 2×2 ένα σώμα μη αντιμεταθετικό.

Πραγματικά,

$$M(x, y) + M(\alpha, \beta) = \begin{pmatrix} x & -\bar{y} \\ y & \bar{x} \end{pmatrix} + \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} x + \alpha & -\bar{y} - \bar{\beta} \\ y + \beta & \bar{x} + \bar{\alpha} \end{pmatrix},$$

$$M(x + \alpha, y + \beta) \in G, \quad -M(x, y) = M(-x, -y)$$

και συνεπώς $(G, +)$ είναι ομάδα και μάλιστα αντιμεταθετική. Προφανώς $\theta = M(0, 0)$. Ο πολλαπλασιασμός είναι εσωτερικός νόμος του G , γιατί

$$M(x, y) \cdot M(\alpha, \beta) = \begin{pmatrix} x\alpha - \bar{y}\beta & y\alpha + \bar{x}\beta \\ -x\bar{\beta} - \bar{y}\bar{\alpha} & -y\bar{\beta} + \bar{x}\bar{\alpha} \end{pmatrix} = M(x\alpha - \bar{y}\beta, -x\bar{\beta} - \bar{y}\bar{\alpha})$$

Ο μοναδιαίος πίνακας $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M(1, 0) \in G$. Επειδή $|M(x, y)| = x\bar{x} + y\bar{y} = |x|^2 + |y|^2 \neq 0$ για $M(x, y) \neq \theta$, ο πίνακας $M(x, y)$ αντιστρέφεται. Ο αντίστροφός του είναι

$$\frac{1}{|M(x, y)|} \cdot \begin{pmatrix} \bar{x} & \bar{y} \\ -y & x \end{pmatrix} = M\left(\frac{\bar{x}}{\Delta}, \frac{-y}{\Delta}\right), \quad \text{όπου } \Delta = |M(x, y)|$$

και ανήκει στο G .

3. Το σύνολο των μιγαδικών $\alpha + \beta i$ με $\alpha, \beta \in \mathbb{Z}$ είναι ως προς την πρόσθεση και τον πολλαπλασιασμό των μιγαδικών δακτύλιος. Συμβολίζεται με $\mathbb{Z}[i]$ και λέγεται δακτύλιος του Gauss.

4. Έστω $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2} ; \alpha, \beta \in \mathbb{Q}\}$. Το σύνολο $\mathbb{Q}(\sqrt{2})$ είναι ως προς την πρόσθεση και τον πολλαπλασιασμό των πραγματικών αριθμών σώμα αντιμεταθετικό.

Πραγματικά, $0 = 0 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $1 = 1 + 0 \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ και αν $\alpha + \beta\sqrt{2}$, $\alpha' + \beta'\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, τότε

$$(\alpha + \beta\sqrt{2}) + (\alpha' + \beta'\sqrt{2}) = (\alpha + \alpha') + (\beta + \beta')\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$$(\alpha + \beta\sqrt{2}) + (\alpha' + \beta'\sqrt{2}) = (\alpha\alpha' + 2\beta\beta') + (\alpha\beta' + \alpha'\beta)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

δηλαδή η πρόσθεση και ο πολλαπλασιασμός είναι εσωτερικοί νόμοι του $\mathbb{Q}(\sqrt{2})$. Ένα στοιχείο $\alpha + \beta\sqrt{2}$ του $\mathbb{Q}(\sqrt{2})$ είναι μηδέν τότε και μόνο, όταν $\alpha = \beta = 0$, γιατί διαφορετικά, αν $\alpha + \beta\sqrt{2} = 0$ και $\beta \neq 0$, θα είχαμε $\sqrt{2} = -\frac{\alpha}{\beta} \in \mathbb{Q}$, πράγμα άτοπο. Έτσι $\alpha + \beta\sqrt{2} \neq 0$ συνεπάγεται $\alpha^2 \neq 2\beta^2$

$$\text{και } \frac{1}{\alpha + \beta\sqrt{2}} = \frac{\alpha - \beta\sqrt{2}}{\alpha^2 - 2\beta^2} = \frac{\alpha}{\alpha^2 - 2\beta^2} + \frac{-\beta}{\alpha^2 - 2\beta^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

5. Έστω E ένα σύνολο $\neq \emptyset$ και $\mathcal{P}(E)$ το σύνολο των υποσυνόλων του. Το σύνολο αυτό είναι ένας μοναδιαίος δακτύλιος ως προς τους εσωτερικούς νόμους $\oplus$ και $\cdot$ που ορίζονται από τις ισότητες

$$A \oplus B = (A - B) \cup (B - A)$$

$$A \cdot B = A \cap B$$

Το μηδέν του δακτυλίου είναι το κενό υποσύνολο $\emptyset$ του E και η μονάδα το σύνολο E . Για την απόδειξη βλ. §1, Κεφ. 0.

Ο δακτύλιος αυτός έχει εφαρμογές στους υπολογιστές και στη θεωρία των κυκλωμάτων των διακοπών. Λέγεται δακτύλιος του Boole. Στο δακτύλιο αυτό έχουμε $x \cdot x = x$. Γενικά ένας δακτύλιος στον οποίο $x \cdot x = x$ για κάθε στοιχείο του x , θα λέγεται δακτύλιος του Boole.

3. Ο ΔΑΚΤΥΛΙΟΣ ΤΩΝ ΑΚΕΡΑΙΩΝ $\text{mod } m$

Για κάθε φυσικό m ορίσαμε στο $\mathbb{Z}$ μια σχέση ισοδυναμίας θέτοντας $x \sim y$ τότε και μόνο, όταν $m \mid x - y$ στο $\mathbb{Z}$. Η κλάση ενός ακεραίου α είναι το σύνολο των ακεραίων που διαιρούμενοι με τον m δίνουν το ίδιο υπόλοιπο v και συμβολίζεται με $\bar{v}$. Τα υπόλοιπα είναι $0, 1, 2, \dots, m-1$. Συνεπώς οι κλάσεις είναι $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}$ και λέγονται **ακέρατοι ως προς μέτρο m** (ή modulo m , σύντομα $\text{mod } m$). Το σύνολό τους συμβολίζεται με $\mathbb{Z}_m$. Έτσι

$$\bar{v} = \{m\alpha + v; \alpha \in \mathbb{Z}\} = m\mathbb{Z} + v$$

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\} \quad ,$$

Θεώρημα 1. Το σύνολο $\mathbb{Z}_m$ είναι ένας αντιμεταθετικός και μοναδιαίος δακτύλιος ως προς τους νόμους $\oplus, \odot$ που ορίζονται από τις ισότητες

$$\bar{\alpha} \oplus \bar{\beta} = \overline{\alpha + \beta} \quad , \quad \bar{\alpha} \odot \bar{\beta} = \overline{\alpha \beta}$$

Οι νόμοι αυτοί είναι οι επεκτάσεις των νόμων $+, \cdot$ του $\mathbb{Z}$ στο σύνολο των υποσυνόλων του $\mathcal{P}(\mathbb{Z})$. Το μηδέν είναι η κλάση $\bar{0}$ και η μονάδα η κλάση $\bar{1}$.

Απόδειξη. Προκύπτει από την πρότ.3,§7, Κεφ.0. $\square$

Όταν ο m δεν είναι πρώτος, ο $\mathbb{Z}_m$ έχει διαιρέτες του μηδενός. Π.χ. ο $\mathbb{Z}_4$ έχει διαιρέτη του μηδενός τον $\bar{2}$, γιατί $\bar{2} \cdot \bar{2} = \bar{4} = \bar{0}$ και $\bar{2} \neq \bar{0}$.

Θεώρημα 2. Ο δακτύλιος $(\mathbb{Z}_m, \oplus, \odot)$ είναι σώμα τότε και μόνο, όταν ο m είναι πρώτος αριθμός.

Απόδειξη. Αν ο m δεν είναι πρώτος, ο $\mathbb{Z}_m$ δεν είναι σώμα, γιατί έχει διαιρέτες του μηδενός. Πραγματικά, έστω ότι ο m δεν είναι πρώτος. Τότε $m = \alpha \cdot \beta$ με $1 < \alpha < m, 1 < \beta < m$, οπότε $\bar{\alpha} \cdot \bar{\beta} = \overline{\alpha \beta} = \bar{m} = \bar{0}$, ενώ $\bar{\alpha} \neq \bar{0}, \bar{\beta} \neq \bar{0}$, αφού $m \neq \alpha$ και $m \neq \beta$.

Έστω τώρα ότι ο m είναι πρώτος αριθμός και $\bar{\alpha} \in \mathbb{Z}_m$. Οι αριθμοί α, m είναι σχετικά πρώτοι, αφού ο m είναι πρώτος. Συνεπώς υπάρχουν ακέραιοι β, n τέτοιοι, ώστε $\alpha\beta + mn = 1$. Οπότε $\overline{\alpha\beta + mn} = \bar{1}$ ή $\bar{\alpha}\bar{\beta} + \bar{0} = \bar{1}$ ή $\bar{\alpha} \cdot \bar{\beta} = \bar{1}$, δηλαδή ο $\bar{\alpha}$ έχει αντίστροφο στο $\mathbb{Z}_m$. Άρα το $\mathbb{Z}_m$ είναι σώμα. $\square$

Εφαρμογές

1. *N' αποδειχτεί ότι δεν υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $x^2 - 3y^2 = 992$.*

Λύση. Ας υποθέσουμε ότι υπάρχουν τέτοιοι ακέραιοι. Τότε εργαζόμενοι στο $\mathbb{Z}_3$ θα πρέπει να έχουμε $\overline{x^2 - 3y^2} = \overline{992}$. Αλλά $\overline{x^2 - 3y^2} = \overline{x^2} - \overline{3y^2} = \bar{x}^2 - \bar{0} = \bar{x}^2$ και $\overline{992} = \bar{2}$. Συνεπώς πρέπει να έχουμε $\bar{x}^2 = \bar{2}$. Όμως $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ και $\bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1}, \bar{2}^2 = \bar{4} = \bar{1}$, δηλαδή $\bar{x}^2 \neq \bar{2}$ για όλα τα στοιχεία $\bar{x}$ του $\mathbb{Z}_3$. Άρα η εξίσωση μας δεν δέχεται λύση με x, y ακεραίους.

2. *N' αποδειχτεί ότι ο ακέραιος $a = a_n a_{n-1} \dots a_0$ (a_i είναι τα ψηφία του στο δεκαδικό-σύστημα αρίθμησης) διαιρείται με το 9 τότε και μόνο, όταν $9 \mid a_0 + a_1 + \dots + a_n$.*

Λύση. Ο αριθμός a γράφεται

$$a = a_0 + 10a_1 + 10^2a_2 + \dots + 10^n a_n$$

Στο $\mathbb{Z}_9$ έχουμε $\overline{10} = \bar{1}$ και $\overline{10^k} = \bar{1}^k = \bar{1}$. Συνεπώς

$$\begin{aligned}\bar{a} &= \bar{a}_0 + \overline{10} \cdot \bar{a}_1 + \dots + \overline{10^n} \bar{a}_n = \bar{a}_0 + \bar{a}_1 + \dots + \bar{a}_n = \\ &= \overline{a_1 + a_2 + \dots + a_n}\end{aligned}$$

Αλλά $9/a$ τότε και μόνο, όταν $\bar{a} = \bar{0}$ ή $\overline{a_1 + a_2 + \dots + a_n} = \bar{0}$ ή $9/a_1 + a_2 + \dots + a_n$.

3. Ν' αποδειχτεί ότι ένας ακέραιος αριθμός της μορφής $4K+3$ δεν γράφεται σαν άθροισμα δύο τετραγώνων ακεραίων αριθμών.

Λύση. Έστω ότι $4K+3 = a^2 + b^2$, όπου a, b ακέραιοι. Εργαζόμενοι στο δακτύλιο $\mathbb{Z}_4$ παίρνουμε $\bar{3} = \bar{a}^2 + \bar{b}^2$. Αλλά $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ και $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{0}$, $\bar{3}^2 = \bar{1}$. Έτσι για όλα τα $\bar{x}, \bar{y} \in \mathbb{Z}_4$ είναι $\bar{x}^2 + \bar{y}^2 = \bar{0}, \bar{1}, \bar{2}$, δηλαδή $\bar{x}^2 + \bar{y}^2 \neq \bar{3}$. Άρα το συμπέρασμα.

4. Να βρεθούν όλοι οι ακέραιοι x, y που επαληθεύουν την εξίσωση $8x+5y=42$.

Λύση. Εργαζόμαστε στο $\mathbb{Z}_5$. Έχουμε $\overline{8x+5y} = \overline{42}$ ή $\bar{3}\bar{x} = \bar{2}$. Το $\mathbb{Z}_5$ είναι σώμα. Ο αντίστροφος του $\bar{3}$ είναι $\bar{2}$, γιατί $\bar{3} \cdot \bar{2} = \bar{6} = \bar{1}$. Συνεπώς $\bar{2}(\bar{3}\bar{x}) = \bar{2} \cdot \bar{2}$ ή $\bar{1} \cdot \bar{x} = \bar{4}$ ή $\bar{x} = \bar{4}$, δηλαδή $x = 5\lambda + 4$ με $\lambda \in \mathbb{Z}$. Κάνοντας αντικατάσταση στην εξίσωσή μας παίρνουμε $8(5\lambda+4)+5y=42$ ή $40\lambda+5y=10$ ή $y=2-8\lambda$, $\lambda \in \mathbb{Z}$. Άρα οι λύσεις είναι $(x, y) = (5\lambda+4, -8\lambda+2)$.

Παρατήρηση. Στη λύση που κάναμε υπολογίσαμε το αντίστροφο του $\bar{3}$ στο $\mathbb{Z}_5$. Αυτό είναι σχετικά απλό, γιατί ο 5 είναι μικρός ακέραιος. Στην περίπτωση μεγάλων συντελεστών αναγόμεθα σε άλλη παρόμοια εξίσωση με μικρούς συντελεστές, όπως στο παρακάτω παράδειγμα.

5. Να βρεθούν οι ακέραιοι x, y ώστε

$$28x + 45y = 191.$$

Λύση. Στο δακτύλιο $\mathbb{Z}_{28}$ έχουμε $\overline{28x+45y} = \overline{191}$ ή $\overline{17y} = \overline{23}$ ή $17y = 23 + 28z$. Στο $\mathbb{Z}_{17}$ η εξίσωση αυτή γράφεται $\bar{0} = \bar{6} + \bar{11}z$ ή $6 + 11z = 17\omega$. Εργαζόμενοι στο $\mathbb{Z}_{11}$ παίρνουμε $\bar{6} = \bar{6}\omega$ ή $6 = 6\omega + 11\phi$. Η τελευταία εξίσωση στο $\mathbb{Z}_6$ γίνεται $\bar{0} = \bar{0} + \bar{5}\phi$ ή $5\phi = 6t$. Στο $\mathbb{Z}_5$ θα έχουμε $\bar{t} = \bar{0}$ ή $t = 5\lambda$. Οπότε $\phi = 6\lambda$, $\omega = 1 - 11\lambda$, $z = 1 - 17\lambda$, $y = 3 - 28\lambda$ και $x = 2 + 45\lambda$.

6. Να βρεθεί ο αντίστροφος του $\overline{49}$ στο σώμα $\mathbb{Z}_{53}$.

Λύση. Αν $\bar{x}$ ο αντίστροφος, έχουμε $\overline{49} \cdot \bar{x} = \bar{1}$ ή $49x = 1 + 53y$ με $x, y \in \mathbb{Z}$. Στο $\mathbb{Z}_{49}$ η σχέση αυτή γίνεται $\bar{0} = \bar{1} + \bar{4}\bar{y}$ ή $4y + 1 = 49z$. Στο

$\mathbb{Z}_4$ η σχέση γίνεται $\bar{1} = \bar{z}$, οπότε $z = 4a + 1$ με $a \in \mathbb{Z}$, $y = 49a + 12$, $49x = 1 + 53(49a + 12)$ ή $49x = 53 \cdot 49 \cdot a + 49 \cdot 13$ ή $x = 53 \cdot a + 13$. Άρα $\bar{x} = \bar{13}$.

4. ΙΣΟΔΥΝΑΜΟΙ ΟΡΙΣΜΟΙ ΟΜΑΔΑΣ

Για ν' αποδείξουμε ισοδυναμία δύο ορισμών μιας ομάδας θα χρησιμοποιήσουμε μερικές απλές ιδιότητες αυτής. Τις περιγράφουμε στις προτάσεις που ακολουθούν.

Πρόταση 1. Κάθε στοιχείο a μιας ομάδας $(G, \cdot)$, είναι ομαλό, δηλαδή $ax = ay$ συνεπάγεται $x = y$ και $xa = ya$ συνεπάγεται επίσης $x = y$.

Απόδειξη. Έστω $ax = ay$. Αν a^{-1} το αντίστροφο του a , έχουμε $a^{-1}(ax) = a^{-1}(ay)$ ή $(a^{-1}a)x = (a^{-1}a)y$ ή $ex = ey$ ή $x = y$. Όμοια αποδεικνύεται ότι $xa = ya$ συνεπάγεται $x = y$. $\square$

Πρόταση 2. Έστω $(G, \cdot)$ μια ομάδα και $a, \beta \in G$. Οι εξισώσεις $ax = \beta$, $ya = \beta$ έχουν μια μόνο λύση ως προς x αντίστοιχα y στη G .

Απόδειξη. Μια λύση της $ax = \beta$ είναι η $x_o = a^{-1}\beta$, γιατί $a(a^{-1}\beta) = (aa^{-1})\beta = e\beta = \beta$. Είναι μοναδική, γιατί $ax_o = \beta$ και $ax = \beta$ συνεπάγονται $ax_o = ax$ ή $x_o = x$ κατά την πρόταση 1. Όμοια η εξίσωση $xa = \beta$ έχει τη μοναδική λύση $y = \beta a^{-1}$. $\square$

Ορισμός 1. Αν $A, B \subseteq G$, το γινόμενο $A \cdot B$ ορίζεται από την ισότητα

$$A \cdot B = \{a \cdot \beta ; a \in A \text{ και } \beta \in B\}.$$

Το γινόμενο μονοσυνόλου $\{a\}$ με το υποσύνολο B του G γράφεται aB αντί $\{a\}B$ (γράφουμε επίσης Ba αντί $B\{a\}$). Έτσι ο εσωτερικός νόμος της ομάδας G ορίζεται στο σύνολο των υποσυνόλων της $\mathcal{P}(G)$.

Πρόταση 3. Αν $(G, \cdot)$ είναι μια ομάδα, τότε για κάθε $a \in G$,

$$a \cdot G = G \cdot a = G$$

Λέμε ότι το στοιχείο a αναπαράγει την ομάδα.

Απόδειξη. Προφανώς $aG \subseteq G$. Έστω $\beta \in G$. Τότε υπάρχει $x \in G$ με $ax = \beta$. Συνεπώς $\beta \in aG$ ή $G \subseteq aG$. Άρα $aG = G$. Όμοια $Ga = G$. $\square$

Πρόταση 4. Έστω $(G, \cdot)$ μια ημιομάδα. Αν υπάρχει δεξιό μοναδιαίο και κάθε $a \in G$ έχει δεξιό αντίστροφο, η ημιομάδα είναι ομάδα.

Απόδειξη. Έστω $e \in G$ τέτοιο, ώστε $ae = a$ για κάθε $a \in G$ και ότι για κάθε $a \in G$ υπάρχει $a' \in G$ τέτοιο, ώστε $a \cdot a' = e$. Υπάρχει τότε $a'' \in G$ με $a'a'' = e$, οπότε

$$\begin{aligned} a'a &= (a'a)e = (a'a)(a'a'') = [(a'a)a']a'' = [a'(aa')]a'' = \\ &= (a'e)a'' = a'a'' = e \end{aligned}$$

δηλαδή $a \cdot a' = a' \cdot a = e$ και επιπλέον

$$e \cdot a = (aa')a = a(a'a) = ae = a = a \cdot e$$

Έτσι το e είναι ουδέτερο του νόμου της ημιομάδας και το a' αντίστροφο του a . Έρα $(G, \cdot)$ είναι ομάδα. $\square$

Πρόταση 5. Αν σε μια ημιομάδα $(G, \cdot)$ υπάρχει αριστερό ουδέτερο και αριστερό αντίστροφο κάθε στοιχείου της, η ημιομάδα είναι ομάδα.

Απόδειξη. Όμοια με την απόδειξη της προηγούμενης πρότασης. $\square$

Πρόταση 6. Έστω $(G, \cdot)$ μια ημιομάδα. Αν για κάθε $a \in G$,

$$aG = Ga = G$$

η ημιομάδα $(G, \cdot)$ είναι ομάδα.

Απόδειξη. Θ' αποδείξουμε ότι υπάρχει δεξιό μοναδιαίο και δεξιό αντίστροφο κάθε στοιχείου της ημιομάδας. Επειδή $a \in G$, υπάρχει ένα στοιχείο $e_a \in G$ τέτοιο, ώστε $a \cdot e_a = a$. Έστω $x \in G$. Υπάρχει $y \in G$ τέτοιο, ώστε $x = ya$, γιατί $Gx = G$. Συνεπώς έχουμε

$$xe_a = (ya)e_a = y(ae_a) = ya = x$$

δηλαδή το e_a είναι δεξιό ουδέτερο. Για κάθε $a \in G$ υπάρχει δεξιό αντίστροφο, γιατί από τις σχέσεις $aG = G$ και $e_a \in G$ προκύπτει ότι υπάρχει $a' \in G$ τέτοιο, ώστε $aa' = e_a$. $\square$

Αποδείξαμε συνεπώς ότι $(G, \cdot)$ είναι ομάδα τότε και μόνο, όταν ισχύει μια από τις παρακάτω προτάσεις:

1. Ο νόμος $\cdot$ είναι προσεταιριστικός και για κάθε $a \in G$, $a \cdot G = G \cdot a = G$.
2. Ο νόμος $\cdot$ είναι προσεταιριστικός, έχει δεξιό ουδέτερο και κάθε στοιχείο έχει δεξιό αντίστροφο.
3. Ο νόμος $\cdot$ είναι προσεταιριστικός, έχει αριστερό ουδέτερο και κάθε στοιχείο έχει αριστερό αντίστροφο.

Οι πεπερασμένες ημιομάδες είναι ομάδες σύμφωνα με την

Πρόταση 7. Μια πεπερασμένη ημιομάδα $(G, \cdot)$ στην οποία ισχύει η ιδιότητα της διάγραφής είναι ομάδα.

Απόδειξη. Έστω $a \in G$. Η συνάρτηση $f_a : G \rightarrow G$ με τιμή $f_a(x) = ax$ είναι αμφιμονοσήμαντη, γιατί $f_a(x) = f_a(y)$ συνεπάγεται $ax = ay$ ή $x = y$ (πρότ.1). Αφού το G είναι πεπερασμένο, η f_a είναι επί του G , δηλαδή $f_a(G) = G$ ή $aG = G$. Όμοια $Ga = G$. Κατά την πρότ.6 η G είναι ομάδα. $\square$

5. ΟΜΑΔΑ ΑΝΤΙΣΤΡΕΨΙΜΩΝ ΣΤΟΙΧΕΙΩΝ ΔΑΚΤΥΛΙΟΥ

Έστω $(A, +, \cdot)$ είναι μοναδιαίος δακτύλιος με μονάδα 1. Λέμε ότι ένα στοιχείο a του A είναι **αντιστρέψιμο αριστερά**, αν υπάρχει $\beta \in A$ τέτοιο, ώστε $a\beta = 1$. Το β θα λέγεται **αντιστρέψιμο δεξιά**. Αν για το στοιχείο a υπάρχει β τέτοιο, ώστε $a\beta = \beta a = 1$, το a λέγεται **αντιστρέψιμο**. Το β είναι μοναδικό με την ιδιότητα αυτή και λέγεται **αντίστροφο** του a . Γράφουμε $\beta = a^{-1}$. Προφανώς αν τα a, β αντιστρέφονται, αντιστρέφεται και το $a\beta$, μάλιστα $(a\beta)^{-1} = \beta^{-1}a^{-1}$ (βλ. §1).

Θεώρημα 1. Έστω $(A, +, \cdot)$ ένας μοναδιαίος δακτύλιος και $U(A)$ το σύνολο των αντιστρέψιμων στοιχείων του. Το $U(A)$ ως προς τον πολλαπλασιασμό του δακτυλίου είναι ομάδα με μονάδα τό 1.

Απόδειξη. Έστω $u, v \in U(A)$. Έχουμε $uv \in U(A)$, γιατί $(uv)^{-1} = v^{-1}u^{-1}$. Επειδή $(u^{-1})^{-1} = u$, $u^{-1} \in U(A)$. Αφού $1 \cdot 1 = 1 \cdot 1 = 1$, $1 \in U(A)$. Άρα $(U(A), \cdot)$ είναι ομάδα. $\square$

Π.χ. $U(\mathbb{Z}_6) = \{\bar{1}, \bar{5}\}$, $U(\mathbb{Z}_{10}) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$ είναι πολλαπλασιαστικές ομάδες.

Θεώρημα (Euler) 2. Αν ο a είναι σχετικά πρώτος με τον m , τότε

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Απόδειξη. Έστω $U(\mathbb{Z}_m) = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\phi(m)}\}$. Αφού $\bar{a} \in U(\mathbb{Z}_m)$, έχουμε $\bar{a}U(\mathbb{Z}_m) = U(\mathbb{Z}_m)$. Συνεπώς

$$\overline{a_1 a_2 \dots a_{\phi(m)}} = \overline{a a_1 a a_2 \dots a a_{\phi(m)}} = \bar{a}^{\phi(m)} \overline{a_1 a_2 \dots a_{\phi(m)}}$$

δηλαδή $\bar{a}^{\phi(m)} = \bar{1}$ (πολλαπλασιάζουμε με το αντίστροφο του $\overline{a_1 a_2 \dots a_{\phi(m)}}$). $\square$

Πόρισμα (Fermat) Αν p είναι πρώτος αριθμός και a αχέραιος, τότε $p/a^p - a$.

Γιατί $\mathbb{Z}_p$ είναι σώμα, συνεπώς $U(\mathbb{Z}_p) = \mathbb{Z}_p^*$, $\phi(p) = p - 1$, οπότε $a^{p-1} \equiv 1 \pmod{p}$ ή $a^p \equiv a \pmod{p}$, δηλαδή $p/a^p - a$. $\square$

Θεώρημα (Wilson) 3. Αν ο αριθμός p είναι πρώτος, τότε

$$(p-1)! \equiv -1 \pmod{p} \quad (1)$$

και αντίστροφα.

Απόδειξη. Αν $p = 2$, είναι προφανές.

Έστω $p > 2$. Το $\mathbb{Z}_p$ είναι σώμα. Τα αντιστρέψιμα στοιχεία είναι τα στοιχεία του συνόλου $U(\mathbb{Z}_p) = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$. Προφανώς $\bar{1} \cdot \bar{1} = \bar{1}$ και $\overline{p-1} \cdot \overline{p-1} = (-\bar{1})(-\bar{1}) = \bar{1}$. Αν $1 < a < p-1$, το αντίστροφο του $\bar{a}$ είναι το $\bar{\beta}$ με $1 < \beta < p-1$. Συνεπώς στο γινόμενο τους $\bar{1} \cdot \bar{2} \cdots \overline{p-1} = \overline{(p-1)!}$ ανά δύο παράγοντες εκτός των $\bar{1}$, $\overline{p-1}$ είναι αντίστροφοι. Άρα το γινόμενό τους ισούται με $\bar{1} \cdot \overline{p-1} = \bar{1} \cdot (-\bar{1}) = -\bar{1}$, δηλαδή $\overline{(p-1)!} = -\bar{1}$, από όπου και το συμπέρασμα (1).

Έστω ότι ο p δεν είναι πρώτος. Τότε έχει ένα διαιρέτη a με $1 < a < p-1$. Αν υποθέσουμε ότι $\overline{(p-1)!} \equiv -1 \pmod{p}$, θα έχουμε $(p-1)! = -1 + pm$ ή $(p-1)! + p(-m) = -1$. Όμως ο a διαιρεί το πρώτο μέλος και δεν διαιρεί το δεύτερο. Καταλήξαμε έτσι σε άτοπο. Άρα ο p είναι πρώτος. $\square$

Σημείωση: Το θεώρημα Wilson είναι ένα κριτήριο για να είναι ένας αριθμός p πρώτος. Δεν είναι όμως στην πράξη χρήσιμο, γιατί ο υπολογισμός του $(p-1)!$ είναι ασύμφορος χρονικά να γίνει με υπολογιστή.

ΑΣΚΗΣΕΙΣ

1. Έστω $E = \{1, 2\}$ και οι συναρτήσεις $f_i : E \rightarrow E$ με τιμές $f_1(a) = a$, $f_2(a) = 1$, $f_3(a) = 2$, $f_4(a) \neq a$. Οι πίνακες

$$(a) \begin{array}{c|cc} \circ & f_1 & f_2 \\ \hline f_1 & f_1 & f_2 \\ \hline f_2 & f_2 & f_2 \end{array} \quad (\beta) \begin{array}{c|cc} \circ & f_1 & f_4 \\ \hline f_1 & f_1 & f_4 \\ \hline f_4 & f_4 & f_1 \end{array} \quad (\gamma) \begin{array}{c|cc} \circ & f_2 & f_3 \\ \hline f_2 & f_2 & f_2 \\ \hline f_3 & f_3 & f_3 \end{array}$$

ορίζουν το νόμο της σύνθεσης δύο συναρτήσεων στα σύνολα $A = \{f_1, f_2\}$, $B = \{f_1, f_4\}$, $\Gamma = \{f_2, f_3\}$. Δείξτε ότι A , B είναι ημιομάδες και Γ ομάδα ως προς την σύνθεση.

2. Να εξετάσετε, αν τα σύνολα των πινάκων

$$\text{i) } \begin{pmatrix} a & -\beta \\ \beta & a \end{pmatrix}, a^2 + \beta^2 \neq 0, a, \beta \in \mathbb{R}$$

$$\text{ii) } \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}, z \in \mathbb{C}$$

είναι ομάδες ως προς τον πολλαπλασιασμό.

3. Ποιές από τις παρακάτω δομές είναι μονοειδή; Ποιές είναι ομάδες;

- 1) $(\mathbb{Q}^+, *)$, $a * \beta = \frac{a\beta}{2}$
- 2) $(\mathbb{Z}, *)$, $x * y = x + y + xy$
- 3) $(\mathbb{Z}, *)$, $x * y = \max\{x, y\}$
- 4) $(\mathbb{R}, *)$, $x * y = \sqrt{x^v + y^v}$ ($v = 2$ ή 3)
- 5) $(S, *)$, $S = \{1, 2, 3, 4, 5, 6\}$, $a * \beta = \mu.κ.δ(a, \beta)$
- 6) $(S, *)$, $S = \{1, 2, 4, 5, 10, 20\}$, $a * \beta = \epsilon.κ.π(a, \beta)$
- 7) $(S, *)$, $S = \{1, 2, 5, 7, 10, 14, 35, 70\}$, $a * \beta = \epsilon.κ.π(a, \beta)$. Να παρατηρήσετε ότι το 2 δεν αντιστρέφεται.
- 8) $\{z \in \mathbb{C}; |z| = 1\}$, $a * \beta = \frac{a + \beta + a\beta - 1}{a + \beta - a\beta + 1}$.

4. Έστω p ένας πρώτος αριθμός. Δείξτε ότι το σύνολο $\{\frac{m}{p^n}; m \in \mathbb{Z}, n \in \mathbb{Z}, n \geq 0\}$ είναι ομάδα ως προς την πρόσθεση των πραγματικών αριθμών.

5. Η εξίσωση $x^2 = x$ έχει δύο λύσεις στο $\mathbb{R}$. Πόσες λύσεις έχει σε μια ομάδα $(G, \cdot)$;

6. Θεωρούμε τις συναρτήσεις με πεδίο ορισμού $\mathbb{R} - \{0, 1\}$ και τιμές στο x τις εξής:

$$x, \frac{1}{1-x}, \frac{x-1}{x}, \frac{1}{x}, 1-x, \frac{x}{x-1}$$

Δείξτε ότι ως προς την σύνθεση αποτελούν μια ομάδα G μη αντιμεταθετική. Λύστε την εξίσωση $x^2 = e$ στην ομάδα G , αν e το ουδέτερο αυτής.

7. Αν η τάξη μιας ομάδας είναι άρτιος αριθμός, δείξτε ότι το πλήθος των λύσεων της εξίσωσης $x^2 = e$ είναι περιττός αριθμός.

8. Αν $(G, \cdot)$ είναι ομάδα και για κάθε $x \in G$, $x^2 = e$, δείξτε ότι η ομάδα G είναι αντιμεταθετική.

9. Βρείτε όλα τα σώματα με τρία στοιχεία.

10. Έστω $(R, +, \cdot)$ ένας δακτύλιος. Στο R ορίζουμε δύο εσωτερικούς νόμους $\oplus, \odot$ ως εξής:

$$a \oplus b = a + b + 1, \quad a \odot b = a + b + ab$$

Δείξτε ότι $(R, \oplus, \odot)$ είναι επίσης δακτύλιος.

11. Έστω K ένα σώμα, $a \in K$. Επί του $K \times K$ ορίζουμε δύο εσωτερικούς νόμους $\oplus, \odot$ ως εξής:

$$\begin{aligned}(x, y) \oplus (u, v) &= (x + u, y + v) \\ (x, y) \odot (u, v) &= (xu + yua, xv + yv)\end{aligned}$$

Αν η εξίσωση $x^2 = a$ δεν έχει λύση στο K , δείξτε ότι $(K \times K, \oplus, \odot)$ είναι σώμα. (Εφαρμογή: $K = \mathbb{R}, a = -1$).

12. Ν' αποδείξετε ότι οι πίνακες $\begin{pmatrix} x+y & 4y \\ -y & x-y \end{pmatrix}$ με x, y ρητούς, αποτελούν ως προς την πρόσθεση και τον πολλαπλασιασμό σώμα αντιμεταθετικό.

13. Ν' αποδείξετε ότι οι πίνακες $\begin{pmatrix} a & -\bar{\beta} \\ \beta & \bar{a} \end{pmatrix}$ με a, β μιγαδικούς ($\bar{a}$, ο συζυγής του a), αποτελούν σώμα μη αντιμεταθετικό.

14. Έστω K το σύνολο των συναρτήσεων $f : \mathbb{R} \rightarrow \mathbb{R}$ με τιμή $f(x) = a \sin x + b \cos x$, όπου $a, b \in \mathbb{R}$. Ορίζουμε ένα εσωτερικό νόμο $*$ ως εξής:

$$f * g(x) = \int_0^{2\pi} f(t)g(x-t)dt \quad (\text{συνέλιξη των } f, g)$$

Αν $+$ είναι η πρόσθεση δύο συναρτήσεων, δείξτε ότι $(K, +, *)$ είναι σώμα.

15. Να λυθούν στο $\mathbb{Z}$ οι εξισώσεις

$$i) 2x + 7y = 12 \quad ii) 5x + 8y = 20$$

16. Να λυθούν οι εξισώσεις

$$i) 2\bar{x} = \bar{3} \text{ στο } \mathbb{Z}_{17} \quad ii) \bar{6}\bar{x} = \bar{3} \text{ στο } \mathbb{Z}_{13}$$

$$\text{iii) } \overline{13}\bar{x} = \bar{5} \text{ στο } \mathbb{Z}_{16} \quad \text{iv) } 2(x+1) \equiv 4(x-1) \text{ στο } \mathbb{Z}_6$$

17. Να βρεθούν τα αντιστρέψιμα στοιχεία της πολλαπλασιαστικής ημιομάδας $\mathbb{Z}_{15}^* = \mathbb{Z}_{15} - \{0\}$, και τα αντίστροφά τους.

18. Έστω p πρώτος αριθμός. Ν' αποδείξετε ότι

- i) $\bar{p} = \bar{2} \pmod{6} \Rightarrow p = 2$
- ii) $\bar{p} = \bar{3} \pmod{6} \Rightarrow p \in \{3, -3\}$
- iii) $\bar{p} = \bar{4} \pmod{6} \Rightarrow p = -2$
- iv) $\bar{p} \neq \bar{0} \pmod{6}$
- v) $p > 3 \Rightarrow \bar{p} \in \{\bar{1}, \bar{5}\}$ στο $\mathbb{Z}_6$.

19. Έστω p πρώτος της μορφής $p = 6n - 1$ με $n \in \mathbb{N}$. Ν' αποδείξετε ότι στο $\mathbb{Z}_p$ έχουμε

- i) $(p-2)^{-1} = \overline{-3n}, (p-3)^{-1} = \overline{-2n}$
- ii) $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \bar{p-4} = \bar{6} \text{ ή } \bar{2}.$

20. Έστω a ένας ακέραιος, $m, n \in \mathbb{N}$. Ν' αποδείξετε ότι $a^{2m-1} \equiv a^{2n-1} \pmod{3}$

21. Για κάθε ακέραιο a , ν' αποδείξετε ότι

- i) $a^5 \equiv a \pmod{30}$
- ii) $a^{13} \equiv a \pmod{390}$
- iii) $a^{21} \equiv a \pmod{330}$

22. Να λυθούν οι ισοδυναμίες

$$\begin{aligned} \text{i) } 6x &\equiv 1 \pmod{7}, \quad 5x \equiv 0 \pmod{8} \\ \text{ii) } x &\equiv 1 \pmod{5}, \quad x \equiv 3 \pmod{11}, \quad x \equiv 6 \pmod{15} \end{aligned}$$

23. Αν σε μια ομάδα G ισχύει μια από τις παρακάτω προτάσεις, δείξτε ότι είναι αντιμεταθετική.

- (α) $\forall n \in \mathbb{Z}, (xy)^n = x^n y^n$ για όλα τα x, y
- (β) $(xy)^k = x^k y^k$ για $k = n-1, n, n+1$ και όλα τα x, y .

24. Σ' ένα δακτύλιο A έχουμε $(x+y)^2 = x^2 + y^2$ για όλα τα $x, y \in A$. Δείξτε ότι ο A είναι αντιμεταθετικός και ότι $2x = 0$ για κάθε x .

25. Έστω R ένας μοναδιαίος δακτύλιος και $a, \beta \in R$. Αν $a\beta + \beta a = 1$, $a^2\beta + \beta a^2 = a$, δείξτε ότι

- i) τα στοιχεία a^2, β αντιμετατίθενται
- ii) $2a\beta a = a$ και ότι το $\bar{a}$ αντιστρέφεται και μάλιστα $a^{-1} = 2\beta$.

26. Δείξτε ότι το σύνολο των πινάκων $\begin{pmatrix} a & \beta \\ 2\beta & a \end{pmatrix}$ με $a, \beta \in \mathbb{Z}_5$ είναι σώμα με 25 στοιχεία.

27. Έστω p πρώτος και G_p το σύνολο των πινάκων $\begin{pmatrix} a & \beta \\ \gamma & \delta \end{pmatrix}$ με $a, \beta, \gamma, \delta \in \mathbb{Z}_p$ και $a\delta - \beta\gamma = 1$. Ν' αποδείξετε ότι $(G_p, \cdot)$ είναι ομάδα τάξης $p(p^2 - 1)$.

3 | Δομές περιεχόμενες σε άλλες

1. ΥΠΟΟΜΑΔΑ, ΥΠΟΔΑΚΤΥΛΙΟΣ, ΥΠΟΣΩΜΑ

Μια αλγεβρική δομή A με ένα ή δύο εσωτερικούς νόμους μπορεί να περιέχεται σε άλλη δομή G με την έννοια ότι $A \subseteq G$ και οι νόμοι στη δομή A να είναι οι περιορισμοί των νόμων της G στο A . Θα λέμε τότε ότι A είναι υποδομή της G . Έτσι

Υποομάδα μιας ομάδας $(G, \cdot)$ είναι μια ομάδα $(A, \star)$, αν $A \subseteq G$ και $a \star b = a \cdot b$ για όλα τα $a, b \in A$.

Υποδακτύλιος του δακτυλίου $(R, +, \cdot)$ είναι ένας δακτύλιος $(A, +', \cdot')$, αν $A \subseteq R$ και $a +' b = a + b$, $a \cdot' b = a \cdot b$ για όλα τα $a, b \in A$.

Υπόσωμα του σώματος $(K, +, \cdot)$ είναι ένα σώμα $(A, +', \cdot')$, αν $A \subseteq K$ και το άθροισμα καθώς και το γινόμενο δύο στοιχείων του A συμπίπτει με το άθροισμα αντίστοιχα το γινόμενο αυτών στο K .

Οι νόμοι υποδομής μιας δομής συμβολίζονται όπως και οι νόμοι της δομής.

Πρόταση 1. Αν $(G, \cdot)$ μια ομάδα και A υποομάδα αυτής, τότε το ουδέ-

τερο της A είναι το ουδέτερο της G και το αντίστροφο του $a \in A$ είναι το αντίστροφο του a μέσα στη G .

Απόδειξη. Έστω e, e_A τα ουδέτερα των G αντίστοιχα A . Έχουμε $e_A = e \cdot e_A$, συνεπώς $e_A \cdot e_A = e \cdot e_A$, οπότε $e_A = e$, αφού κάθε στοιχείο της G είναι ομαλό. Αν a' το αντίστροφο του $a \in A$ στην ομάδα A και a'' στην G , έχουμε $e = aa' = aa''$, οπότε $a' = a''$. $\square$

Παραδείγματα.

1. Αν $(G, \cdot)$ είναι μια ομάδα με ουδέτερο e , δύο υποομάδες είναι $\{e\}$ και G . Πρόκειται για τη μικρότερη αντίστοιχα τη μεγαλύτερη υποομάδα της G .

2. Αν $(K, +, \cdot)$ δακτύλιος, δύο υποδακτύλιοι είναι τα σύνολα $\{0\}$ και R , ο μηδενικός και ολόκληρος ο δακτύλιος.

Ένας άλλος υποδακτύλιος είναι το σύνολο $A = \{ax ; x \in R\}$ όπου $a \in R$. Πραγματικά, $ax + ay = a(x + y) \in A$, αφού $x + y \in A$, $0 = a \cdot 0 \in A$, $-ax = a(-x) \in A$ και $ax \cdot ay = a(xay) \in A$.

3. Βρείτε όλες τις υποομάδες της ομάδας $(\mathbb{Z}, +)$.

Λύση. Μια υποομάδα είναι η $\{0\}$. Έστω A υποομάδα της $(\mathbb{Z}, +)$ διάφορη της $\{0\}$. Τότε υπάρχει $a \in A$, $a \neq 0$. Αφού το αντίθετο του a είναι $-a$, έχουμε $-a \in A$. Συνεπώς η υποομάδα A περιέχει το σύνολο $\{a, -a\}$ με $a \neq 0$. Θα περιέχει λοιπόν και θετικούς αριθμούς. Έστω m ο μικρότερος θετικός στο A .

Τότε $ma = m + m + \dots + m \in A$ (a φορές) $m(-a) = (-m) + (-m) + \dots + (-m) \in A$

δηλαδή $ma \in A$ για κάθε ακέραιο a , ή $m \cdot \mathbb{Z} \subseteq A$. Έστω $\beta \in A$. Αν v το υπόλοιπο της διαίρεσης του β με το m , έχουμε $\beta = ma + v$, όπου $0 \leq v < m$ και a το πηλίκο. Επειδή $ma \in A$, ο $v = \beta - ma \in A$. Συνεπώς πρέπει $v = 0$ ή $\beta = ma$. Αυτό σημαίνει ότι $m\mathbb{Z} \supseteq A$, οπότε $A = m \cdot \mathbb{Z}$.

4. Βρείτε όλους τους υποδακτύλιους του δακτύλιου $(\mathbb{Z}, +, \cdot)$.

Λύση. Έστω $(A, +, \cdot)$ ένας υποδακτύλιος. Επειδή $(A, +)$ είναι υποομάδα $\neq \{0\}$ της ομάδας $(\mathbb{Z}, +)$, έπεται ότι $A = m \cdot \mathbb{Z}$, όπου m ο μικρότερος θετικός στην A . Αν $x, y \in A$, έχουμε $x = ma$, $y = m\beta$ με $a, \beta \in \mathbb{Z}$, οπότε $x \cdot y = m(ma\beta) \in m\mathbb{Z}$. Άρα $A = m\mathbb{Z}$ είναι (για $m \geq 0$) ο οποιοσδήποτε υποδακτύλιος του $(\mathbb{Z}, +, \cdot)$.

5. $(\mathbb{Q}, +, \cdot)$ είναι υπόσωμα του $(\mathbb{R}, +, \cdot)$ και του $(\mathbb{C}, +, \cdot)$. Όμοια το

$(\mathbb{R}, +, \cdot)$ είναι υπόσωμα του $(\mathbb{C}, +, \cdot)$.

6. Έστω $(G, \cdot)$ μια ομάδα και Z το σύνολο των στοιχείων $a \in G$ τα οποία αντιμετατίθενται με όλα τα στοιχεία x της G , δηλαδή $ax = xa$. Το Z είναι υποομάδα της G και λέγεται κέντρο της G .

Πραγματικά, έστω $a, \beta \in Z$ και $x \in G$. Έχουμε $(a\beta)x = a(\beta x) = a(x\beta) = (ax)\beta = (xa)\beta = x(a\beta)$, δηλαδή $a \cdot \beta \in Z$. Προφανώς το ουδέτερο e της ομάδας G ανήκει στο Z και αν $a \in Z$, το $a^{-1} \in Z$, γιατί $ax = xa$ συνεπάγεται $axa^{-1} = (xa)a^{-1} = x(aa^{-1}) = xe = x$ και συνεπώς $a^{-1}x = a^{-1}(axa^{-1}) = (a^{-1}a)xa^{-1} = exa^{-1} = xa^{-1}$, δηλαδή $a^{-1} \in Z$.

2. ΙΔΙΟΤΗΤΕΣ ΥΠΟΟΜΑΔΩΝ

Έστω $(G, \cdot)$ μια ομάδα και e το ουδέτερο αυτής. Αν $A \subseteq G$, το σύνολο των αντιστρόφων των στοιχείων του A συμβολίζεται με A^{-1} . Συνεπώς

$$A^{-1} = \{a^{-1} ; a \in A\}.$$

Προφανώς $(A^{-1})^{-1} = A$ και αν $B \subseteq G$, $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

Παραδείγματα.

1. Έστω η πολλαπλασιαστική ομάδα $\mathbb{Z}_5^* = \mathbb{Z}_5 - \{0\}$ των ακεραίων mod 5 και το υποσύνολό της $A = \{\bar{2}, \bar{4}\}$. Έχουμε $A^{-1} = \{\bar{2}^{-1}, \bar{4}^{-1}\} = \{\bar{3}, \bar{4}\}$, γιατί $\bar{2}^{-1} = \bar{3}$, αφού $\bar{2} \cdot \bar{3} = \bar{6} = \bar{1}$, και $\bar{4}^{-1} = \bar{4}$, αφού $\bar{4} \cdot \bar{4} = \bar{16} = \bar{1}$.

2. Έστω η προσθετική ομάδα $\mathbb{Z}_5$ και το υποσύνολό της $A = \{\bar{2}, \bar{4}\}$. Τότε $A^{-1} = \{-\bar{2}, -\bar{4}\} = \{\bar{3}, \bar{1}\}$, γιατί $-\bar{2} = \bar{3}$, αφού $\bar{2} + \bar{3} = \bar{5} = \bar{0}$, και $-\bar{4} = \bar{1}$, αφού $\bar{4} + \bar{1} = \bar{5} = \bar{0}$.

Πρόταση 1. Έστω $(G, \cdot)$ μια ομάδα και $A \subseteq G$. Το $(A, \cdot)$ είναι υποομάδα της $(G, \cdot)$ τότε και μόνο, όταν

- i) $A \neq \emptyset$
- ii) $A \cdot A \subseteq A$
- iii) $A^{-1} \subseteq A$

Απόδειξη. Αν $(A, \cdot)$ είναι υποομάδα, οι παραπάνω ιδιότητες είναι προφανείς. Αποδεικνύουμε το αντίστροφο. Αφού $A \neq \emptyset$, υπάρχει ένα στοιχείο $a \in A$. Τότε από την iii) παίρνουμε ότι $a^{-1} \in A$ και από την ii) ότι $a \cdot a^{-1} = e \in A$. Εάν $a, \beta \in A$ από την ii) προκύπτει ότι $a \cdot \beta \in A$ και από την iii) $a^{-1} \in A$. Συνεπώς το $(A, \cdot)$ είναι υποομάδα. $\square$

Πρόταση 2. Έστω $(G, \cdot)$ μια ομάδα και $A \subseteq G$. Το $(A, \cdot)$ είναι υποομάδα της $(G, \cdot)$, τότε και μόνο, όταν $A \neq \emptyset$ και $A \cdot A^{-1} \subseteq A$.

Απόδειξη. Αν A είναι υποομάδα, οι συνθήκες ισχύουν. Αντίστροφα, έστω $a \in A$. Τότε $a \cdot a^{-1} \in A \cdot A^{-1} \subseteq A$ και συνεπώς $e = a \cdot a^{-1} \in A$. Επειδή $e \cdot A^{-1} \subseteq A \cdot A^{-1} \subseteq A$ και $eA^{-1} = A^{-1}$, έχουμε $A^{-1} \subseteq A$. Αν $a, \beta \in A$, τότε $a\beta = a(\beta^{-1})^{-1} \in AA^{-1} \subseteq A$, δηλαδή $A \cdot A \subseteq A$. Κατά την πρόταση 1 έπεται το συμπέρασμα. $\square$

Πρόταση 3. Έστω $(G_i), i \in I$ μια οικογένεια υποομάδων της ομάδας $(G, \cdot)$. Τότε η τομή $T = \bigcap_{i \in I} G_i$ είναι υποομάδα της G .

Απόδειξη. Προφανώς το ουδέτερο της G ανήκει σε κάθε υποομάδα, άρα και στην τομή T , δηλαδή $T \neq \emptyset$. Αν $a, \beta \in T$, τότε $a, \beta \in G_i$ για κάθε $i \in I$ και συνεπώς $a\beta^{-1} \in G_i$ για κάθε $i \in I$. Άρα $T \cdot T^{-1} \subseteq T$ και κατά την προηγούμενη πρόταση η τομή T είναι υποομάδα της G . $\square$

3. ΔΕΙΚΤΗΣ ΥΠΟΟΜΑΔΑΣ

Έστω $(A, \cdot)$ μια πεπερασμένη ομάδα και G μια υποομάδα της. Το πλήθος των στοιχείων της A συμβολίζεται με $|A|$ και λέγεται **τάξη** της ομάδας A . Αν η A είναι άπειρη, λέμε ότι η τάξη της είναι **άπειρη**. Προφανώς $1 \leq |G| \leq |A|$. Θα αποδείξουμε το

Θεώρημα (Lagrange) 1. Η τάξη μιας υποομάδας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας.

Λήμμα 1. Τα σύνολα $aG, \beta G$ με $a, \beta \in A$ είναι ξένα μεταξύ τους ή ίσα.

Απόδειξη. Έστω $aG \cap \beta G \neq \emptyset$. Αν g είναι στοιχείο της τομής, θα έχουμε $g = ax = \beta y$ με $x, y \in G$, οπότε $a = \beta yx^{-1}$ με $yx^{-1} \in G$ και

$$aG = (\beta yx^{-1})G = \beta(yx^{-1}G) = \beta G$$

$\square$

Λήμμα 2. $|aG| = |G|$.

Απόδειξη. Η συνάρτηση $f_a : G \rightarrow aG$ με τιμή $f_a(x) = ax$ είναι αμφιμονοσήμαντη, γιατί $ax = ay$ συνεπάγεται $x = y$. Συνεπώς είναι επί. Επειδή η A είναι πεπερασμένη, θα είναι πεπερασμένη και η υποομάδα της. Άρα $|aG| = |G|$. $\square$

Απόδειξη του Θεωρήματος: Έστω $a_1G, a_2G, \dots, a_nG$ τα διάφορα υποσύνολα της μορφής aG . Επειδή κάθε $x \in A$ ανήκει σ' ένα μόνο από αυτά.

έχουμε

$$A = a_1 G \cup a_2 G \cup \dots \cup a_n G$$

$$|A| = \sum_{i=1}^n |a_i G| = \sum_{i=1}^n |G| = n|G|$$

συνεπώς $|G|$ διαιρεί την τάξη $|A|$ της A . Το πηλίκο $\frac{|A|}{|G|}$ είναι το πλήθος των διαφόρων υποσυνόλων της μορφής aG , $a \in A$. $\square$

Ορισμός 1. Ο αριθμός αυτός λέγεται **δείκτης** της υποομάδας G στην A και συμβολίζεται με $(A : G)$. Τα σύνολα aG λέγονται **αριστερές κλάσεις** της υποομάδας G στην A .

Πόρισμα 1. $(A : G) = \frac{|A|}{|G|}$

Παράδειγμα 1. Έστω $\mathbb{Z}_{13}$ οι ακέραιοι mod 13 και $\mathbb{Z}_{13}^* = \mathbb{Z}_{13} - \{0\}$. Επειδή ο 13 είναι πρώτος αριθμός, το $\mathbb{Z}_{13}^*$ είναι πολλαπλασιαστική ομάδα. Το σύνολο $G = \{\bar{1}, \bar{5}, \bar{8}, \bar{12}\}$ είναι υποομάδα αυτής. Οι αριστερές κλάσεις της ομάδας G στη $\mathbb{Z}_{13}^*$ είναι

$$\begin{aligned}\bar{1} \cdot G &= G \\ \bar{2} \cdot G &= \{\bar{2}, \bar{10}, \bar{3}, \bar{11}\} \\ \bar{4} \cdot G &= \{\bar{4}, \bar{7}, \bar{6}, \bar{9}\}\end{aligned}$$

Συνεπώς $(\mathbb{Z}_{13}^* : G) = 3$, $|\mathbb{Z}_{13}^*| = 12$ και $3/12$.

Παράδειγμα 2. $6\mathbb{Z}$ είναι υποομάδα της $\mathbb{Z}$. Οι αριστερές κλάσεις της $6\mathbb{Z}$ στη $\mathbb{Z}$ είναι $6\mathbb{Z}$, $1+6\mathbb{Z}$, $2+6\mathbb{Z}$, $3+6\mathbb{Z}$, $4+6\mathbb{Z}$, $5+6\mathbb{Z}$ συνεπώς $(\mathbb{Z} : 6\mathbb{Z}) = 6$.

Παράδειγμα 3. $6\mathbb{Z}$ είναι υποομάδα της $2\mathbb{Z}$ γιατί, αν $x, y \in 6\mathbb{Z}$, έχουμε $x = 6a$, $y = 6\beta$ με $a, \beta \in \mathbb{Z}$, οπότε $x - y = 6a - 6\beta = 6(a - \beta) \in 6\mathbb{Z}$. Οι κλάσεις της $6\mathbb{Z}$ στην $2\mathbb{Z}$ είναι $6\mathbb{Z}$, $2+6\mathbb{Z}$, $4+6\mathbb{Z}$, συνεπώς $(2\mathbb{Z} : 6\mathbb{Z}) = 3$.

4. ΥΠΟΟΜΑΔΑ ΠΑΡΑΓΟΜΕΝΗ ΑΠΟ ΥΠΟΣΥΝΟΛΟ ΟΜΑΔΑΣ

Έστω $(G, \cdot)$ μια ομάδα και $S \subseteq G$. Θεωρούμε όλες τις υποομάδες A της G που περιέχουν το S . Μια τέτοια υποομάδα είναι η ίδια η ομάδα G . Η τομή τους είναι μια υποομάδα της G , που περιέχει το S , αφού το S περιέχεται σε όλες τις υποομάδες που θεωρήσαμε.

Η υποομάδα αυτή συμβολίζεται με $\langle S \rangle$ και λέγεται υποομάδα της G **παραγόμενη** από το S . Τα στοιχεία του S λέγονται **γεννήτορες** της $\langle S \rangle$. Προφανώς $\langle G \rangle = G$.

Αν A είναι υποομάδα της G και $S \subseteq A$, θα έχουμε $\langle S \rangle \subseteq A$. Έτσι $\langle S \rangle$ είναι η μικρότερη υποομάδα της G , που περιέχει το S .

Είναι εύκολο να βρούμε τα στοιχεία της υποομάδας $\langle S \rangle$. Παρατηρούμε ότι για κάθε $s \in S$ και κάθε φυσικό m , το γινόμενο $s \cdot s \cdots s$, συμβολικά s^m , ανήκει στην υποομάδα $\langle S \rangle$.

Αν για αρνητικό ακέραιο n και $a \in G$ ορίσουμε

$$a^n = (a^{-1})^{-n} \quad \text{και} \quad a^0 = e$$

τότε για κάθε ακέραιο αρνητικό n , $s^n \in \langle S \rangle$, αφού $s^n = (s^{-1})^{-n}$ με $s^{-1} \in \langle S \rangle$ και $-n$ φυσικός. Έτσι $s^m \in \langle S \rangle$ για κάθε ακέραιο m και κάθε $s \in S$. Συνεπώς για οποιαδήποτε $s_1, s_2, \dots, s_k \in S$ και οποιουδήποτε ακεραίου $m_1, m_2, \dots, m_k$ το στοιχείο

$$s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} \in S$$

Αλλά το σύνολο $T = \{s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} ; k = \text{φυσικός}, s_i \in S, m_i \in \mathbb{Z}\}$ είναι υποομάδα της G . Άρα η

Πρόταση 1. Η υποομάδα που παράγεται από το S είναι

$$\langle S \rangle = \{s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} ; k \in \mathbb{N}, s_i \in S, m_i \in \mathbb{Z}\}.$$

Πρόταση 2. Σε κάθε ομάδα G και για κάθε $a \in G$, έχουμε

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}$$

για οποιουδήποτε ακεραίου m, n .

Απόδειξη. Διακρίνουμε περιπτώσεις (i) $m > 0, n > 0$ κ.λ.π. □

5. ΥΠΟΟΜΑΔΑ ΠΑΡΑΓΟΜΕΝΗ ΑΠΟ ΜΟΝΟΣΥΝΟΛΟ

Έστω $(G, \cdot)$ μια ομάδα και $a \in G$. Θα αναζητήσουμε την υποομάδα που παράγεται από το $S = \{a\}$. Λέμε ότι παράγεται από το στοιχείο a και τη συμβολίζουμε με $\langle a \rangle$ αντί $\langle \{a\} \rangle$.

Σύμφωνα με την πρόταση 1, έχουμε

$$\langle a \rangle = \{a^n ; n \in \mathbb{Z}\}$$

Αν ο νόμος της ομάδας συμβολίζεται προσθετικά, το ουδέτερο αυτής συμβολίζεται όπως έχουμε αναφέρει (§1, Κεφ.2) με 0 και το αντίστροφο του a με

$-a$ (λέγεται τότε αντίθετο του a). Η n -δύναμη a^n του a με n φυσικό είναι $a + a + \dots + a$ (n φορές) και συμβολίζεται με $n \cdot a$. Η n -δύναμη a^n του a με n ακέραιο αρνητικό είναι $(-a) + (-a) + \dots + (-a)$ ($|n|$ φορές) και συμβολίζεται πάλι με $n \cdot a$. Οι ιδιότητες των δυνάμεων της πρότασης 2 για την ομάδα $G, +$) γράφονται

$$na + ma = (n + m)a$$

$$m(na) = (mn)a.$$

Πρόταση 1. Η υποομάδα που παράγεται από ένα στοιχείο a της ομάδας G έχει μια από τις παρακάτω μορφές:

$$i) \langle a \rangle = \{e, a, a^2, \dots, a^{d-1}\} \quad \text{με} \quad a^d = e$$

$$ii) \langle a \rangle = \{\dots a^{-n}, \dots, a^{-2}, a^{-1}, e, a, a^2, \dots, a^n, \dots\}$$

Απόδειξη. Αν όλες οι δυνάμεις a^n με $n \in \mathbb{Z}$ είναι διάφορες, η $\langle a \rangle$ είναι της μορφής (ii). Έστω ότι δύο δυνάμεις a^n, a^m με $n \neq m$ είναι ίσες. Τότε, αν $n > m$, $a^{n-m} = e$ με $n - m > 0$. Έστω d ο μικρότερος φυσικός με την ιδιότητα $a^d = e$ και a^n ένα τυχαίο στοιχείο της $\langle a \rangle$. Διαιρούμε τον n με τον d , οπότε $n = \pi d + v$ με $0 \leq v < d$. Έχουμε

$$a^n = a^{\pi d + v} = (a^d)^\pi \cdot a^v = e^\pi \cdot a^v = ea^v = a^v$$

Τα στοιχεία a^v με $0 \leq v < d$ είναι διάφορα ανά δύο, γιατί, αν $a^v = a^{v_1}$ με $0 \leq v < v_1 < d$, θα είναι $a^{v_1-v} = e$ με $0 < v_1 - v < d$, πράγμα άτοπο. Άρα η $\langle a \rangle$ είναι της μορφής (i). $\square$

Ορισμός 1. Αν μια ομάδα $(G, \cdot)$ παράγεται από ένα στοιχείο της a λέγεται **κυκλική ομάδα**.

Οι ομάδες $(\mathbb{Z}, +)$ και $(\mathbb{Z}_m, +)$ είναι κυκλικές, γιατί $\mathbb{Z} = \langle 1 \rangle$ και $\mathbb{Z}_m = \langle \bar{1} \rangle$.

Παραδείγματα.

1. Έστω $C^* = \mathbb{C} - \{0\}$ η πολλαπλασιαστική ομάδα των μιγαδικών αριθμών $\neq 0$. Βρείτε την υποομάδα που παράγεται από τον αριθμό $a = \frac{1 + i\sqrt{3}}{2}$.

Λύση. Είναι $a^2 = \frac{-1 + i\sqrt{3}}{2}$, $a^3 = -1$, $a^4 = -a$, $a^5 = -a^2$ και $a^6 = 1$. Συνεπώς $a^v \cdot a^{6-v} = 1$ για $0 \leq v \leq 6$, δηλαδή τα αντίστροφα των $a, a^2, \dots, a^5$ είναι μεταξύ αυτών. Άρα

$$\langle a \rangle = \{1, a, a^2, a^3, a^4, a^5\}$$

2. Έστω G το σύνολο των αντιστρέψιμων πινάκων 2×2 με στοιχεία πραγματικών αριθμούς. Είναι μια πολλαπλασιαστική ομάδα. Βρείτε την υποομάδα που παράγεται από τον πίνακα A και την υποομάδα που παράγεται από το σύνολο των πινάκων $\{A, B\}$, όπου

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Λύση. i) Έχουμε $A^2 = I$, $A^3 = A$, $A^{-1} = A$ συνεπώς $\langle A \rangle = \{I, A\}$.
ii) Είναι $B^2 = I$, $AB = -I = BA$. Έτσι θέτοντας $S = \{A, B\}$, έχουμε $S^{-1} = \{A, B\}$, άρα $\langle S \rangle = \{I, A, B, AB\}$.

3. Έστω a ένας φυσικός. Βρείτε την υποομάδα της $(\mathbb{Z}, +)$ που παράγεται από το a .

Λύση. Για κάθε φυσικό n , το $a + \dots + a = na \in \langle a \rangle$. Επίσης για κάθε ακέραιο αρνητικό m το $ma \in \langle a \rangle$. Συνεπώς $\langle a \rangle \supseteq a \cdot \mathbb{Z}$. Επειδή $a\mathbb{Z}$ είναι υποομάδα της $(\mathbb{Z}, +)$ και $a = a \cdot 1 \in a\mathbb{Z}$, έπεται ότι $\langle a \rangle = a \cdot \mathbb{Z}$.

4. Η προσθετική ομάδα των μιγαδικών $(\mathbb{C}, +)$ παράγεται από το σύνολο $\mathbb{R} \cup \mathbb{R}i$.

5. Η πολλαπλασιαστική ομάδα $(\mathbb{Q}, \cdot)$ των θετικών ρητών παράγεται από το σύνολο P των πρώτων αριθμών.

Γιατί κάθε ακέραιος $a > 0$ είναι γινόμενο δυνάμεων πρώτων αριθμών $a = p_1^{a_1} \cdots p_k^{a_k}$, οπότε $\frac{a}{\beta} = p_1^{a_1} \cdots p_k^{a_k} \cdots s_1^{\beta_1} \cdots s_\lambda^{\beta_\lambda}$ με $a_i, \beta_i \in \mathbb{Z}$.

6. ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ

Ορισμός 1. Τάξη ενός στοιχείου a της ομάδας $(G, \cdot)$ λέγεται η τάξη της υποομάδας που παράγεται από αυτό.

Αν η ομάδα G είναι πεπερασμένη, η τάξη κάθε στοιχείου της a είναι πεπερασμένη και κατά το θεώρημα Lagrange η τάξη του $|\langle a \rangle|$ διαιρεί την τάξη $|G|$ της G .

Φυσικά μπορεί η τάξη μιας ομάδας να είναι άπειρη και η τάξη ενός στοιχείου της πεπερασμένη.

Αν η τάξη μιας ομάδας G είναι ένας πρώτος αριθμός p , η ομάδα G είναι κυκλική και παράγεται από ένα οποιοδήποτε στοιχείο της $a \neq 1$. Γιατί η τάξη της υποομάδας $\langle a \rangle$ είναι > 1 και διαιρεί την τάξη της G , δηλαδή τον p . Συνεπώς $|\langle a \rangle| = p$. Αφού $\langle a \rangle \subseteq G$ και $|\langle a \rangle| = |G|$, έχουμε $\langle a \rangle = G$.

Θεώρημα 1. Έστω G μια πεπερασμένη ομάδα και a ένα στοιχείο της. Ισχύει $a^{|G|} = e$.

Απόδειξη. Έστω d η τάξη του a . Τότε $a^d = e$. Επειδή κατά το θεώρημα Lagrange ο d διαιρεί την τάξη της G , έχουμε $|G| = d \cdot n$ με n φυσικό. Συνεπώς

$$a^{|G|} = a^{dn} = (a^d)^n = e^n = e \quad \square$$

Από το θεώρημα αυτό προκύπτει μια απόδειξη του θεωρήματος Fermat χωρίς τη χρήση της συνάρτησης του Euler (2§5):

Θεώρημα (Fermat) 2. Αν p είναι πρώτος αριθμός και a ένας ακέραιος, ο p διαιρεί τον $a^p - a$.

Απόδειξη. Ο δακτύλιος $\mathbb{Z}_p$ είναι σώμα, αφού ο p είναι πρώτος. Η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^* = \mathbb{Z}_p - \{\bar{0}\}$ έχει τάξη $p - 1$. Συνεπώς $\bar{a}^{p-1} = \bar{1}$ ή $\bar{a}^p = \bar{a}$ ή $\overline{a^p - a} = \bar{0}$. Αυτό σημαίνει ότι $p/a^p - a$. $\square$

Πόρισμα. Αν ο $p \nmid a$, τότε $p/a^{p-1} - 1$.

Γιατί $p/a(a^{p-1} - 1)$, ο p είναι πρώτος και $p \nmid a$.

Παράδειγμα 1. Δείξτε ότι το υπόλοιπο της διαίρεσης του 9^{124} με 13 είναι 9.

Πραγματικά $9^{124} = (9^{12})^{10} \cdot 9^4$ και εργαζόμενοι στο σώμα $\mathbb{Z}_{13}$ παίρνουμε

$$\begin{aligned} \overline{9^{124}} &= (\overline{9^{12}})^{10} \cdot \bar{9}^4 = \bar{1}^{10} \cdot (-\bar{4})^4 = \bar{4}^4 = \bar{16} \cdot \bar{16} = \\ &= \bar{3} \cdot \bar{3} = \bar{9}, \text{ που σημαίνει ότι } 9^{124} = \\ &= 13 \cdot a + 9. \end{aligned}$$

Παράδειγμα 2. Βρείτε όλες τις ομάδες τάξης 4.

Έστω $(G, \cdot)$ μια ομάδα τάξης 4, $a \in G$, $a \neq e$. Η τάξη του a διαιρεί την τάξη της G , συνεπώς είναι 2 ή 4. Αν είναι 4, τότε $G = \{e, a, a^2, a^3\}$. Έστω ότι δεν υπάρχει στοιχείο της G τάξης 4. Αν $a, \beta \in G - \{e\}$, θα έχουν τάξη 2, συνεπώς $a^2 = e$, $\beta^2 = e$. Έστω $G = \{e, a, \beta, x\}$. Επειδή $a\beta \neq a, \beta, e$, θα έχουμε $x = a\beta = \beta a$. Έτσι $G = \{e, a, \beta, a\beta\}$ με $a^2 = e$, $\beta^2 = e$.

Η ομάδα αυτή λέγεται ομάδα του Klein. Άρα μια ομάδα τάξης 4 είναι κυκλική ή η ομάδα του Klein.

7. ΥΠΟΟΜΑΔΕΣ ΚΥΚΛΙΚΗΣ ΟΜΑΔΑΣ

Είδαμε ότι η τάξη μιας υποομάδας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας. Θ' αποδείξουμε ότι στις κυκλικές ομάδες ισχύει το αντίστροφο:

Πρόταση 1. Έστω $G = \{e, x, x^2, \dots, x^{n-1}\}$ μια πεπερασμένη κυκλική ομάδα τάξης n . Αν d είναι ένας διαιρέτης της τάξης n της G , υπάρχει μια μόνο υποομάδα της G τάξης d .

Απόδειξη. Η υποομάδα $\langle x^{\frac{n}{d}} \rangle$ έχει τάξη d , γιατί $(x^{\frac{n}{d}})^d = x^n = e$ και για κάθε $d' < d$ είναι $\frac{n}{d} \cdot d' < \frac{n}{d} \cdot d = n$, δηλαδή $(x^{\frac{n}{d}})^{d'} \neq e$.

Αν $\langle x^k \rangle$ είναι μια άλλη υποομάδα της G τάξης d , θα έχουμε $(x^k)^d = e$, συνεπώς n/kd . Θέτοντας $\frac{kd}{n} = \beta$, έχουμε $k = \frac{n}{d}\beta$ και συνεπώς $x^k = x^{\frac{n}{d}\beta} = (x^{\frac{n}{d}})^\beta \in \langle x^{\frac{n}{d}} \rangle$, οπότε $\langle x^k \rangle \subseteq \langle x^{\frac{n}{d}} \rangle$ και καθώς $\langle x^k \rangle, \langle x^{\frac{n}{d}} \rangle$ έχουν την ίδια τάξη, θα συμπίπτουν. $\square$

Πρόταση 2. Έστω μια κυκλική ομάδα $G = \{e, x, x^2, \dots, x^{n-1}\}$. Το στοιχείο x^m παράγει μια υποομάδα τάξης $\frac{n}{(m, n)}$.

Απόδειξη. Έστω $d = (m, n)$, $m = dm_1$, $n = dn_1$, όπου $(m_1, n_1) = 1$. Έχουμε $(x^m)^{\frac{n}{d}} = (x^n)^{\frac{m}{d}} = e^{\frac{m}{d}} = e$. Αν $(x^m)^k = e$, τότε $x^{mk} = e$, n/mk , $mk = n\lambda$, $dm_1k = dn_1\lambda$, $m_1k = n_1\lambda$, n_1/k , $k = n_1\beta = \frac{n}{d}\beta \geq \frac{n}{d}$ δηλαδή ο μικρότερος k με $(x^m)^k = e$ είναι ο $k = \frac{n}{d}$. Άρα $|\langle x^m \rangle| = \frac{n}{d} = \frac{n}{(m, n)}$. $\square$

Πρόταση 3. Έστω G μια κυκλική ομάδα.

- i) Αν η G είναι άπειρη, για κάθε φυσικό d υπάρχει μία μόνο υποομάδα δείκτου d .
- ii) Αν η G είναι πεπερασμένη, έστω $n = |G|$ και d ένας διαιρέτης της τάξης n , υπάρχει μία μόνο υποομάδα δείκτου d .

Απόδειξη. Μια υποομάδα A της κυκλικής ομάδας $G = \langle x \rangle$ ορίζεται από τον ελάχιστο φυσικό m με $x^m \in A$.

- i) Έστω $A = \langle x^d \rangle$ και ένα στοιχείο x^n της G . Θέτοντας $n = dm + v$ με $0 \leq v \leq d - 1$ βλέπουμε ότι το x^n γράφεται υπό τη μορφή

$$x^n = (x^d)^m \cdot x^v \in \langle x^d \rangle \cdot x^v, \quad \text{συνεπώς} \\ G = \langle x^d \rangle \cup \langle x^d \rangle x \cup \dots \cup \langle x^d \rangle x^{d-1}$$

δηλαδή η A έχει δείκτη d στην G . Έτσι ο δείκτης της υποομάδας A ισούται με τον ελάχιστο εκθέτη d για τον οποίο $x^d \in A$. Άρα είναι μοναδική.

- ii) Έστω $n = md$. Υπάρχει μια μόνο υποομάδα A τάξης m . Ο δείκτης αυτής είναι $(G : A) = \frac{|G|}{|A|} = \frac{n}{m} = d$. Επειδή μια υποομάδα δείκτου d έχει τάξη $m = \frac{n}{d}$, είναι μοναδική. $\square$

Παράδειγμα. Να βρεθούν οι υποομάδες της $\mathbb{Z}_{18}$.

Απάντηση. Οι ακέραιοι 1, 5, 7, 11, 13, 17 είναι σχετικά πρώτοι με τον 18. Συνεπώς $\langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle = \langle \bar{13} \rangle = \langle \bar{17} \rangle = \mathbb{Z}_{18}$. Το στοιχείο $\bar{2}$ παράγει την υποομάδα

$$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16}\} \quad \text{τάξης } 9$$

το στοιχείο $\bar{3}$ την υποομάδα

$$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\} \quad \text{τάξης } 6$$

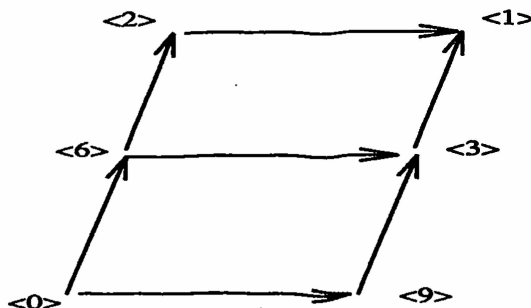
και το $\bar{9}$, την υποομάδα

$$\langle \bar{9} \rangle = \{\bar{0}, \bar{9}\} \quad \text{τάξης } 2$$

Γεννήτορες της $\langle \bar{2} \rangle$ είναι τα στοιχεία $a \cdot \bar{2}$, όπου ο a είναι σχετικά πρώτος με τον 9, δηλαδή τα $\bar{2}, \bar{4}, \bar{8}, \bar{10}, \bar{14}, \bar{16}$. Συνεπώς έχουμε δύο το πολύ υποομάδες της $\langle \bar{2} \rangle$, τις $\langle \bar{6} \rangle$ και $\langle \bar{12} \rangle$. Αλλά

$$\langle \bar{6} \rangle = \{\bar{0}, \bar{6}, \bar{12}\} = \langle \bar{12} \rangle$$

Έτσι το σύνολο των υποομάδων της $\mathbb{Z}_{18}$ διατεταγμένο με τη σχέση $\subseteq$ είναι



ΑΣΚΗΣΕΙΣ

1. Βρείτε τις υποομάδες των ομάδων

$$\alpha) G = \{1, -1, i, -i\}, \quad \beta) (\mathbb{Z}_4, +), \quad \gamma) (\mathbb{Z}_{36}, +).$$

2. Βρείτε ένα υποσύνολο του $\mathbb{Z}_6^*$, που είναι ομάδα ως προς τον πολλαπλασιασμό.

3. Έστω $\mathbb{R}^*$ η πολλαπλασιαστική ομάδα των πραγματικών αριθμών ($\mathbb{R}^* = \mathbb{R} - \{0\}$). Στο σύνολο $G = \mathbb{R}^* \times \mathbb{R}$ ορίζουμε ένα εσωτερικό νόμο "·" θέτοντας

$$(x, y) \cdot (x', y') = (xx', \frac{y'}{x} + x'y)$$

- i) Δείξτε ότι $(G, \cdot)$ είναι ομάδα.
- ii) Βρείτε μια συνάρτηση $f : \mathbb{R}^* \rightarrow \mathbb{R}$ τέτοια, ώστε η γραφική παράσταση αυτής $\{(x, f(x)); x \in \mathbb{R}^*\}$ να είναι υποομάδα της ομάδας G .
- iii) Δείξτε ότι τα καρτεσιανά γινόμενα $\{1\} \times \mathbb{R}$ και $\{1, -1\} \times \mathbb{R}$ είναι υποομάδες της G .

4. Ποιά από τα παρακάτω σύνολα είναι υποδακτύλιοι του δακτυλίου $(\mathbb{C}, +, \cdot)$.

- i) $\{a + \beta i; a, \beta \in \mathbb{Z}\}$
- ii) $\{a + \beta i; a^2 + \beta^2 \leq 1\}$
- iii) $\{\frac{m}{2^n}; m \in \mathbb{Z}, n \in \mathbb{Z} \text{ με } n \geq 0\}$

5. Έστω G η ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_{15}$. Δείξτε ότι τα υποσύνολα $\{\bar{1}, \bar{4}\}$ και $\{\bar{1}, \bar{14}\}$ είναι υποομάδες της G .

6. Δείξτε ότι το σύνολο $A = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq \mathbb{Z}_6$ είναι υποδακτύλιος του $\mathbb{Z}_6$ μοναδιαίος με μονάδα $\neq \bar{1}$.

7. Δείξτε ότι το κέντρο Z ενός δακτυλίου A είναι υποδακτύλιος του A ($Z = \{a \in A; ax = xa \text{ για κάθε } x \in A\}$).

8. Έστω A ένας δακτύλιος. Αν για κάθε $x \in A$, το στοιχείο $x^2 - x$ ανήκει στο κέντρο Z του A , ν' αποδείξετε ότι ο A είναι αντιμεταθετικός.

9. Έστω $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, p πρώτος > 2 . Δείξτε ότι $G = \{\bar{x}^2; \bar{x} \in \mathbb{Z}_p^*\}$ είναι υποομάδα της $\mathbb{Z}_p^*$ τάξης $\frac{p-1}{2}$.

10. Ποιό είναι i) το μικρότερο υπόσωμα του σώματος των πραγματικών αριθμών ii) το μικρότερο υπόσωμα του σώματος των πραγματικών αριθμών στο οποίο η εξίσωση $x^2 = 2$ έχει λύση.

11. Βρείτε την υποομάδα της $(\mathbb{Z}_6, +)$ και της $(\mathbb{Z}_6^*, \cdot)$ που παράγει το σύνολο $\bar{2}$.

12. Έστω G μια ομάδα, H, K δύο διάφορες υποομάδες της δείκτου 2 στη G . Ν' αποδείξετε ότι η τομή $A = H \cap K$ είναι υποομάδα δείκτου 4 στη G .

13. Έστω G μια πεπερασμένη ομάδα και δύο στοιχεία της a, β . Δείξτε ότι:

- 1) αν τα στοιχεία $a, \beta, a\beta$ έχουν τάξη 2, τα a, β αντιμετατίθενται
- 2) τα a, a^{-1} έχουν την ίδια τάξη
- 3) τα $a, \beta a \beta^{-1}$ έχουν την ίδια τάξη
- 4) τα $a\beta, \beta a$ έχουν την ίδια τάξη.

14. Έστω G μια ομάδα και $a \in G$ τάξης 3. Δείξτε ότι (i) η εξίσωση $x^2 = a$ έχει λύση στη G (ii) κάθε στοιχείο τάξης 5 στη G είναι τετράγωνο κάποιου στοιχείου της G .

15. Έστω G μια πεπερασμένη ομάδα. Δείξτε ότι: (i) Έχει περιττό αριθμό στοιχείων τάξης 3. (ii) Το πλήθος των στοιχείων τάξης 5 είναι $0 \pmod{4}$.

16. Αν G μια ομάδα τάξης 27, δείξτε ότι είναι κυκλική ή $x^2 = e$ για κάθε $x \in G$, όπου e η μονάδα της G .

17. Έστω $(G, \cdot)$ η ομάδα των αντιστρέψιμων στοιχείων μιας ακεραίας περιοχής στην οποία $1 + 1 \neq 0$. Δείξτε ότι $\{x^2; x \in G\}$ είναι υποομάδα της G δείκτου 2, όταν η τάξη της G είναι πεπερασμένη.

18. Έστω G μια ομάδα τάξης $2n$ με ουδέτερο στοιχείο e . Υποθέτουμε ότι έχει δύο υποομάδες A, B με $A \cap B = \{e\}$. Δείξτε ότι $n = 2$, γράψτε τον πίνακα του εσωτερικού νόμου της ομάδας G και βρείτε όλες τις υποομάδες της.

19. Έστω E_n το σύνολο των πινάκων με στοιχεία πραγματικούς αριθμούς a, β της μορφής

$$M(a, \beta) = \begin{pmatrix} a & \beta & \cdots & \beta \\ \beta & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \beta \\ \beta & \cdots \beta & \cdots & a \end{pmatrix} \quad \text{τύπου } n \times n.$$

- i) Ν' αποδείξετε ότι ως προς την πρόσθεση και τον πολλαπλασιασμό των πινάκων το E_n είναι υποδακτύλιος του δακτυλίου των πινάκων τύπου $n \times n$.
- ii) Βρείτε τα αντιστρέψιμα στοιχεία του δακτυλίου E_n .

20. Δείξτε ότι ο δείκτης του κέντρου Z μιας πεπερασμένης ομάδας G είναι πρώτος αριθμός ($Z = \{a \in G; \forall x \in G, ax = xa\}$).

21. Μια κυκλική ομάδα τάξης 22 έχει ένα μόνο στοιχείο τάξης 2 και 10 στοιχεία τάξης 11.

22. Έστω H μια υποομάδα της ομάδας G και ένα στοιχείο της G τάξης 2. Δείξτε ότι τα αντίστροφα των στοιχείων της κλάσης Ha είναι τα στοιχεία της κλάσης aH .

23. Έστω K μια κυκλική ομάδα τάξης 12 με γεννήτορα a . Βρείτε τις αριστερές κλάσεις της υποομάδας $\langle a^2 \rangle$.

24. Έστω S_3 το σύνολο των αμφιμονοσήμαντων συναρτήσεων $f : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$. Να επαληθεύσετε ότι

$$\text{i) } S_3 = \left\{ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \right. \\ \left. f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

ii) $(S_3, \circ)$ είναι ομάδα με πίνακα εσωτερικού νόμου

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_5	f_6	f_4
f_3	f_3	f_1	f_2	f_6	f_4	f_5
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_4	f_6	f_2	f_1	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

- iii) Η ομάδα S_3 είναι μη αντιμεταθετική. Δείξτε ότι είναι η μικρότερης τάξης μη αντιμεταθετική ομάδα.
 iv) $H = \{f_1, f_4\}$ είναι υποομάδα της S_3 . Βρείτε τις αριστερές και δεξιές κλάσεις της H και δείξτε ότι $aH \neq Ha$ για κάθε $a \notin H$.
 v) $H = \{f_1, f_2, f_3\}$ είναι υποομάδα της S_3 τέτοια, ώστε $aH = Ha$ για κάθε $a \in S_3$.
 vi) $S_3 = \langle f_2, f_4 \rangle$.
 vii) Αν κάθε γνήσια υποομάδα μιας ομάδας είναι κυκλική, η ομάδα είναι κυκλική;

25. Έστω M το σύνολο των αντιστρέψιμων πινάκων $n \times n$ με στοιχεία πραγματικούς αριθμούς. Δείξτε ότι (i) είναι ομάδα ως προς τον πολλαπλασιασμό. (ii) Το υποσύνολο $K = \{A \in M; |A| = 1\}$ είναι υποομάδα της $(M, \cdot)$ τέτοια, ώστε $XK = KX$ για κάθε $X \in M$.

26. Έστω G μια αβελιανή ομάδα. Αν $G \neq \{0\}$ και η G έχει μόνο δύο υποομάδες $\{0\}, G$ λέγεται απλή ομάδα. Δείξτε ότι οι παρακάτω προτάσεις είναι ισοδύναμες:

- α) Η G είναι κυκλική ομάδα με τάξη πρώτο αριθμό.
 β) Η G είναι αβελιανή απλή ομάδα.

4 | Ομάδα πηλίκο δακτύλιος πηλίκο

Θα παρουσιάσουμε μια μέθοδο κατασκευής ομάδας (και δακτυλίου) από μια ομάδα G και μια υποομάδα της K (αντίστοιχα από ένα δακτύλιο και ένα υποδακτύλιο).

Η υποομάδα αυτή έχει επί πλέον ιδιότητες από μια τυχούσα υποομάδα και λέγεται **κανονική** υποομάδα. Το ρόλο της κανονικής υποομάδας στην περίπτωση δακτυλίου παίζει ένας υποδακτύλιος, που λέγεται **ιδεώδες**.

Με τη βοήθεια της κανονικής υποομάδας K ορίζουμε μια σχέση ισοδυναμίας $\sim$ στην ομάδα G έτσι, ώστε το σύνολο πηλίκο $G/\sim$ να γίνεται ομάδα ως προς την **επέκταση** του νόμου της ομάδας G στο σύνολο των υποσυνόλων της $P(G)$, η οποία λέγεται **ομάδα πηλίκο** της G με την K και συμβολίζεται με G/K .

Πλήρης αναλογία εμφανίζεται, αν αντικαταστήσουμε την ομάδα με δακτύλιο και την κανονική υποομάδα της με το ιδεώδες.

1. ΚΑΝΟΝΙΚΗ ΥΠΟΟΜΑΔΑ, ΟΜΑΔΑ ΠΗΛΙΚΟ

Για ν' αποδείξουμε ότι η τάξη μιας υποομάδας G πεπερασμένης ομάδας A διαιρεί την τάξη της A χρησιμοποιήσαμε τα σύνολα aG με $a \in A$, που τα ονομάσαμε αριστερές κλάσεις της υποομάδας G στην A . Στην πραγματικότητα τα σύνολα αυτά είναι κλάσεις μιας σχέσης ισοδυναμίας που ορίζεται με τη βοήθεια της υποομάδας G ως εξής:

$$x \sim y \Leftrightarrow x^{-1}y \in G$$

Εύκολα φαίνεται ότι είναι σχέση ισοδυναμίας. Πραγματικά:

$$x \sim x, \text{ αφού } x^{-1} \cdot x = e \in G$$

$$x \sim y \Rightarrow y \sim x, \text{ γιατί } y^{-1}x = (x^{-1}y)^{-1} \in G, \text{ αφού } x^{-1}y \in G$$

$$x \sim y, y \sim z \Rightarrow x \sim z, \text{ γιατί } x^{-1}z = (x^{-1}y)(y^{-1}z) \in G.$$

Η κλάση του a είναι aG . Πραγματικά, έστω $x \sim a$. Τότε $x^{-1}a \in G$ ή $a \in xG$, οπότε $aG = xG$ και $x \in aG$. Κάθε στοιχείο y του aG είναι ισοδύναμο με το a , γιατί $y = a\beta$ με $\beta \in G$ ή $a^{-1}y = \beta \in G$. Άρα η κλάση του a είναι πραγματικά aG .

Όμοια αποδεικνύεται ότι η σχέση

$$x \sim y \Leftrightarrow xy^{-1} \in G$$

είναι σχέση ισοδυναμίας με κλάσεις τα υποσύνολα Ga , που λέγονται δεξιές κλάσεις ως προς την υποομάδα G .

Το σύνολο των αριστερών κλάσεων ως προς την υποομάδα G συμβολίζεται με $(A/G)_a$ και των δεξιών με $(A/G)_s$. Προφανώς για πεπερασμένες ομάδες A έχουμε

$$|(A/G)_a| = \frac{|A|}{|G|} = |(A/G)_s|$$

Ορισμός 1. Αν για κάθε $a \in A$, η αριστερή κλάση aG ισούται με τη δεξιά κλάση Ga , η υποομάδα G λέγεται **κανονική υποομάδα** της A και γράφουμε $G \trianglelefteq A$.

Το σύνολο των κλάσεων συμβολίζεται με A/G και λέγεται **πηλίκο** της A με την G . Αν πολλαπλασιάσουμε δύο στοιχεία του συνόλου A/G σαν υποσύνολα της ομάδας A βρίσκουμε

$$aG \cdot \beta G = a(G\beta)G = a(\beta G)G = a\beta GG = a\beta G$$

Δηλαδή το γινόμενο δύο κλάσεων είναι επίσης μια κλάση.

Θεώρημα 1. Αν G είναι κανονική υποομάδα της ομάδας A το σύνολο πηλίκο $A/G = \{aG : a \in A\}$ είναι ως προς το νόμο

$$aG \cdot \beta G = a\beta G \quad (1)$$

ομάδα, η οποία λέγεται **ομάδα πηλίκο της A διά G** . Ο νόμος (1) είναι η επέκταση του νόμου της ομάδας A στο σύνολο των υποσυνόλων της $\mathcal{P}(A)$.

Απόδειξη. Παρατηρήσαμε ότι $xGyG = xyG$. Η κλάση $eG = G$ είναι το ουδέτερο, γιατί $G \cdot aG = eaG = aG$ και $aG \cdot G = aG$. Η προσεταιριστικότητα είναι προφανής: Έχουμε

$$\begin{aligned} xG \cdot (yG \cdot zG) &= xG \cdot yzG = x(yz)G \\ (xG \cdot yG) \cdot zG &= xyG \cdot zG = (xy)zG \text{ και } x(yz) = (xy)z \end{aligned}$$

Το αντίστροφο του xG , είναι $x^{-1}G$, γιατί $xG \cdot x^{-1}G = x \cdot x^{-1}G = eG = G$ και όμοια $x^{-1}G \cdot xG = G$. $\square$

Πόρισμα 1. Αν η ομάδα A είναι πεπερασμένη, η τάξη της A/G είναι $|A/G| = \frac{|A|}{|G|}$.

Παράδειγμα 1. Αν m φυσικός, $m\mathbb{Z}$ είναι υποομάδα της ομάδας $(\mathbb{Z}, +)$. Η ομάδα πηλίκο $\mathbb{Z}/m\mathbb{Z}$ είναι η ομάδα $\mathbb{Z}_m$.

Πραγματικά, ένα στοιχείο της $\mathbb{Z}/m\mathbb{Z}$ έχει τη μορφή $a + m\mathbb{Z}$ με $a \in \mathbb{Z}$. Προφανώς

$$\begin{aligned} a + m\mathbb{Z} = \beta + m\mathbb{Z} &\Leftrightarrow a + m\mathbb{Z} = \beta + m\mathbb{Z} \text{ με } x, y \in \mathbb{Z} \\ &\Leftrightarrow m \mid a - \beta \\ &\Leftrightarrow \bar{a} = \bar{\beta} \end{aligned}$$

και το άθροισμα $(a + m\mathbb{Z}) + (\beta + m\mathbb{Z}) = \bar{a} \oplus \bar{\beta}$.

Παράδειγμα 2. Έστω $\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ η πολλαπλασιαστική ομάδα του σώματος $\mathbb{Z}_5$. Το σύνολο $G = \{\bar{1}, \bar{4}\}$ είναι υποομάδα της $\mathbb{Z}_5^*$, γιατί $\bar{4}^2 = \bar{16} = \bar{1}$. Οι κλάσεις της G στην $\mathbb{Z}_5^*$ είναι G , $\bar{2}G = \{\bar{2}, \bar{3}\}$ και η ομάδα πηλίκο $\mathbb{Z}_5^*/G = \{G, \bar{2} \cdot G\}$ με μονάδα $G = \bar{1}G$, γιατί $G \cdot \bar{2}G = \bar{1}G \cdot \bar{2}G = \bar{2}G$. Προφανώς $(\bar{2} \cdot G)^2 = \bar{2}G \cdot \bar{2}G = \bar{4}G = G$, γιατί $\bar{4} \in G$.

Η χρησιμότητα της έννοιας της κανονικής υποομάδας επισημάνθηκε από τον Galois και χρησιμοποιήθηκε στη θεωρία των εξισώσεων.

Είδαμε παραπάνω ότι το γινόμενο δύο κλάσεων $aG, \beta G$ μιας κανονικής υποομάδας G είναι επίσης μια κλάση γG . Η ιδιότητα αυτή είναι χαρακτηριστική της κανονικότητας της υποομάδας.

Πρόταση 1. Το γινόμενο δύο οποιονδήποτε αριστερών κλάσεων $aG, \beta G$ είναι μια αριστερή κλάση γG τότε και μόνο, όταν η G είναι κανονική υποομάδα.

Απόδειξη. Αν η G είναι κανονική υποομάδα, το γινόμενο $aG \cdot \beta G = a\beta G$. Έστω ότι $aG \cdot \beta G = \gamma G$. Επειδή $a \cdot \beta = ae \cdot \beta e \in aG \cdot \beta G$, έχουμε $a\beta \in \gamma G$, συνεπώς $\gamma G = a\beta G$. Αν λοιπόν το γινόμενο δύο κλάσεων $aG, \beta G$ είναι μια κλάση, θα είναι $aG \cdot \beta G = a\beta G$. Ειδικά για τις κλάσεις eG, xG θα έχουμε

$$eG \cdot xG = exG, \quad GxG = xG, \quad x^{-1}GxG = G$$

και επειδή $x^{-1}Gx \subseteq x^{-1}GxG$,

$$\begin{array}{ccc} x^{-1}Gx \subseteq G & \text{ή} & Gx \subseteq xG \\ \text{όμοια } xGx^{-1} \subseteq G & \text{ή} & xG \subseteq Gx \end{array}$$

Άρα $xG = Gx$ και η G είναι κανονική. □

Πρόταση 2. Έστω H υποομάδα της A . Οι παρακάτω προτάσεις είναι ισοδύναμες.

1. H είναι κανονική υποομάδα
2. $x^{-1}Hx = H$ για όλα τα $x \in A$
3. $x^{-1}Hx \subseteq H$ για όλα τα $x \in A$
4. $Hx \subseteq xH$ για όλα τα $x \in A$
5. $Hx \supseteq xH$ για όλα τα $x \in A$

Απόδειξη $1 \Leftrightarrow 2$. Είναι $Hx = xH$, συνεπώς $x^{-1}Hx = H$.

Αντίστροφα, $x^{-1}Hx = H$ συνεπάγεται $x(x^{-1}Hx) = xH$ ή $Hx = xH$.

$2 \Rightarrow 3$. Προφανές.

$3 \Rightarrow 4$. Έχουμε $x(x^{-1}Hx) \subseteq xH$ ή $Hx \subseteq xH$.

$4 \Rightarrow 2$. Είναι $x^{-1}Hx \subseteq H$ για κάθε $x \in A$. Συνεπώς και $xHx^{-1} \subseteq H$ ή $xH \subseteq Hx$ ή $H \subseteq x^{-1}Hx$, οπότε $x^{-1}Hx = H$.

$3 \Rightarrow 5$. Είναι $xHx^{-1} \subseteq H$, οπότε $xH \subseteq Hx$.

$5 \Rightarrow 3$. Γιατί $Hx^{-1} \supseteq x^{-1}H$, οπότε $H \supseteq x^{-1}Hx$. □

Το γινόμενο δύο υποομάδων δεν είναι πάντοτε υποομάδα: Έστω I ο μοναδιαίος πίνακας 2×2 ,

$$A = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \quad H = \{I, A\}, \quad K = \{I, B\}$$

Προφανώς H, K είναι υποομάδες της ομάδας των αντιστρέψιμων πινάκων, ενώ το γινόμενο τους $HK = \{I, A, B, AB\}$ δεν είναι ομάδα, αφού $(AB)^2 \notin HK$.

Πρόταση 3. Έστω H, K υποομάδες της G . Αν $HK = KH$, το γινόμενο είναι υποομάδα της G . Αν η μία υποομάδα, είναι κανονική υποομάδα, το γινόμενο HK είναι υποομάδα της G .

Απόδειξη. Έχουμε

$$(HK)(HK)^{-1} = HKK^{-1}H^{-1} = HKH^{-1} = KHH^{-1} = KH = HK$$

άρα το γινόμενο HK είναι υποομάδα της G . Αν η K είναι κανονική, για κάθε $x \in G$ είναι $Kx = xK$, συνεπώς για κάθε $h \in H$ είναι $Kh = hK$, οπότε $KH = HK$ και κατά την πρώτη ιδιότητα HK είναι υποομάδα της G . $\square$

Πρόταση 4. Έστω G μια ομάδα και K μια κανονική υποομάδα της. Οι υποομάδες της ομάδας πηλίκο G/K είναι της μορφής H/K όπου H υποομάδα της G .

Απόδειξη. Έστω H^* μια υποομάδα της G/K και $H = \{x \in G; xK \in H^*\}$. Αν $x, y \in H$, έχουμε $xy^{-1}K = xK(yK)^{-1} \in H^*$, συνεπώς $xy^{-1} \in H$ και H είναι υποομάδα της G . $\square$

Πρόταση 5. Αν η G είναι κυκλική ομάδα και A μια υποομάδα της, το πηλίκο G/A είναι κυκλική ομάδα.

Απόδειξη. Έστω $G = \langle x \rangle$. Επειδή η G είναι αντιμεταθετική, κάθε υποομάδα της είναι κανονική. Τα στοιχεία της G/A είναι $x^n A$ με $n \in \mathbb{Z}$. Όμως $x^n A = (xA)^n$. Έτσι $G/A = \langle xA \rangle$. $\square$

Παράδειγμα. Έστω η ομάδα $\mathbb{Z}_7^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. Το υποσύνολο $A = \{\bar{1}, \bar{6}\}$ είναι υποομάδα της $\mathbb{Z}_7^*$. Βρείτε το πηλίκο $\mathbb{Z}_7^*/A$ και δείξτε ότι είναι κυκλική ομάδα με γεννήτορα $\bar{5}A$.

Απάντηση. Προφανώς $\mathbb{Z}_7^* = \langle \bar{5} \rangle = \{\bar{1}, \bar{5}, \bar{5}^2, \bar{5}^3, \bar{5}^4, \bar{5}^5\}$, αφού $\bar{5}^2 = \bar{4}, \bar{5}^3 = \bar{6}, \bar{5}^4 = \bar{2}, \bar{5}^5 = \bar{3}$. Οι κλάσεις mod A είναι $\bar{2}A = \{\bar{2}, \bar{5}\}, \bar{3}A = \{\bar{3}, \bar{4}\}$. Άρα

$$\mathbb{Z}_7^*/A = \{A, \bar{2}A, \bar{3}A\} = \langle \bar{5}A \rangle$$

2. ΔΑΚΤΥΛΙΟΣ ΠΗΛΙΚΟ

Έστω $(A, +, \cdot)$ ένας δακτύλιος και $(I, +)$ υποομάδα της προσθετικής ομάδας του δακτυλίου. Επειδή η πρόσθεση $+$ είναι αντιμεταθετική, η I είναι κανονική υποομάδα της $(A, +)$, συνεπώς το πηλίκο

$$A/I \text{ με πρόσθεση } (a + I) + (\beta + I) = (a + \beta) + I$$

είναι ομάδα. Αναζητούμε συνθήκες για το I ώστε το γινόμενο δύο κλάσεων να είναι μια κλάση. Έστω

$$(a + I)(\beta + I) = \gamma + I$$

Πρέπει $a \cdot \beta = (a + 0)(\beta + 0) \in \gamma + I$ ή $a\beta = \gamma + \delta$ με $\delta \in I$. Τότε $\gamma = a\beta - \delta$ και $\gamma + I = (a\beta - \delta) + I = a\beta + (-\delta + I) = a\beta + I$, δηλαδή

$$(a + I)(\beta + I) = a\beta + I \quad (1)$$

Για τις κλάσεις $0 + I = I$ και $x + I$ με $x \in A$, θα έχουμε

$$I \cdot (x + I) = 0 \cdot x + I = I$$

Επειδή $x \in x + I$, πρέπει για κάθε $x \in A$,

$$Ix \subseteq I, \quad \text{όμοια} \quad xI \subseteq I \quad (2)$$

Οι συνθήκες (2) εξασφαλίζουν την ανεξαρτησία της (1) από την επιλογή των αντιπροσώπων των κλάσεων $a + I$, $\beta + I$. Πραγματικά, αν $a + I = a' + I$, $\beta + I = \beta' + I$, έχουμε $a - a' \in I$, $\beta - \beta' \in I$, συνεπώς $a - a' = i \in I$, $\beta - \beta' = j \in I$ και

$$\begin{aligned} (a' + I)(\beta' + I) &= a'\beta' + I = (a - i)(\beta - j) + I \\ &= a\beta - i\beta - j\beta + I \\ &= a\beta + I \end{aligned}$$

γιατί $(-i)\beta \in I$ και $(-j)\beta \in I$.

Ορισμός 1. Μια υποομάδα $(I, +)$ της προσθετικής ομάδας του δακτυλίου A που πληρεί τις συνθήκες

$$IA \subseteq I \quad \text{και} \quad AI \subseteq I$$

λέγεται ιδεώδες του δακτυλίου A .

Θεώρημα 1. Αν I ιδεώδες του δακτυλίου A , το σύνολο A/I των κλάσεων $a + I$ γίνεται δακτύλιος ως προς τις επεκτάσεις των νόμων $+$, $\cdot$ στο σύνολο των υποσυνόλων του A , δηλαδή ως προς τους νόμους

$$(a + I) + (\beta + I) = (a + \beta) + I \quad (1)$$

$$(a + I) \cdot (\beta + I) = (a \cdot \beta) + I \quad (2)$$

Απόδειξη. Το A/I είναι ως προς την πρόσθεση (1) ομάδα (§1 θεώρ.1, γιατί $I \trianglelefteq A$). Προφανώς η πρόσθεση (1) είναι αντιμεταθετική, δηλαδή $(A/I, +)$ είναι ομάδα αντιμεταθετική. Το μηδέν της ομάδας αυτής είναι το $0 + I = I$. Η προσεταιριστικότητα του νόμου (2) και η επιμεριστικότητα αυτού με την (1) επαληθεύονται εύκολα:

$$(a + I)[(\beta + I) \cdot (\gamma + I)] = (a + I) \cdot (\beta\gamma + I) = a(\beta\gamma) + I$$

όμοια

$$[(a + I) \cdot (\beta + I)](\gamma + I) = (a\beta)\gamma + I = a(\beta\gamma) + I$$

$$(a + I)[(\beta + I) + (\gamma + I)] = (a + I) \cdot [(\beta + \gamma + I)] = a(\beta + \gamma) + I$$

$$(a + I)(\beta + I) + (a + I)(\gamma + I) = (a\beta + I) + (a\gamma + I) = (a\beta + a\gamma) + I,$$

γιατί $I + I = I$. Επειδή $a(\beta + \gamma) = a\beta + a\gamma$, η επιμεριστικότητα του νόμου $\cdot$ ως προς το νόμο $+$ δεξιά είναι προφανής. Όμοια αποδεικνύεται και η επιμεριστικότητα αριστερά. $\square$

Ορισμός 2. Αν I ιδεώδες του δακτυλίου A , ο δακτύλιος A/I λέγεται δακτύλιος πηλίκο του δακτυλίου A με το ιδεώδες I .

Παραδείγματα.

1. Τα ιδεώδη του δακτυλίου $(\mathbb{Z}, +, \cdot)$ είναι της μορφής $m\mathbb{Z}$.

Γνωρίζουμε ότι οι υποομάδες της προσθετικής ομάδας των ακεραίων είναι της μορφής $m\mathbb{Z}$ με m φυσικό. Συνεπώς ένα ιδεώδες I θα έχει τη μορφή $I = m\mathbb{Z}$. Εξετάζουμε, αν $I\mathbb{Z} \subseteq I$. Τυχόν στοιχείο του $I\mathbb{Z}$ έχει τη μορφή $(m\alpha)\beta = m(\alpha\beta) \in I$. Συνεπώς $I\mathbb{Z} \subseteq I$, όπως επίσης $\mathbb{Z}I = I\mathbb{Z} \subseteq I$. Άρα τα ιδεώδη του δακτυλίου $(\mathbb{Z}, +, \cdot)$ είναι της μορφής $I = m\mathbb{Z}$, όπου m ο μικρότερος φυσικός στο I . Ο δακτύλιος πηλίκο $\mathbb{Z}/m\mathbb{Z}$ είναι ο δακτύλιος των ακεραίων $\mathbb{Z}_m$.

2. Έστω F το σύνολο των συνεχών συναρτήσεων $f : \mathbb{R} \rightarrow \mathbb{R}$. Ως προς την πρόσθεση $(f+g)(x) = f(x)+g(x)$ και το γινόμενο $(f \cdot g)(x) = f(x)g(x)$

το σύνολο F είναι δακτύλιος. Έστω $x_0 \in \mathbb{R}$ και $F_0 = \{f \in F ; f(x_0) = 0\}$. Το F_0 είναι ιδεώδες του F .

Η επαλήθευση είναι απλή.

3. Οι συγχλίνουσες ακολουθίες (a_n) πραγματικών αριθμών αποτελούν ένα δακτύλιο $A = \mathbb{R}^{\mathbb{N}}$ ως προς την πρόσθεση και τον πολλαπλασιασμό:

$$(a_n) + (\beta_n) = (a_n + \beta_n) \quad , \quad (a_n) \cdot (\beta_n) = (a_n \beta_n)$$

Το σύνολο των μηδενικών ακολουθιών, έστω M , είναι ιδεώδες του δακτυλίου αυτού.

Γιατί το άθροισμα δύο μηδενικών ακολουθιών είναι μηδενική ακολουθία, και το γινόμενο μηδενικής επί συγχλίνουσα είναι μηδενική, δηλαδή $M \cdot \mathbb{R}^{\mathbb{N}} \subseteq M$ και $\mathbb{R}^{\mathbb{N}} \cdot M \subseteq M$.

Θα δούμε ότι το σύνολο πηλίκο A/M είναι το σώμα των πραγματικών αριθμών (βλ. §3, Κεφ.8).

Σχέση ισοδυναμίας modulo ένα ιδεώδες

Έστω I ένα ιδεώδες του δακτυλίου A .

Ορισμός 2. Σχέση ισοδυναμίας modulo I λέγεται η σχέση

$$a \sim \beta \Leftrightarrow a - \beta \in I$$

η οποία πραγματικά είναι σχέση ισοδυναμίας, γιατί

- (i) $a \sim a$, αφού $a - a = 0 \in I$
- (ii) $a \sim \beta \Rightarrow \beta \sim a$, γιατί $\beta - a = -(a - \beta) \in I$, αφού $a - \beta \in I$.
- (iii) $a \sim \beta, \beta \sim \gamma \Rightarrow a \sim \gamma$, γιατί $a - \gamma = (a - \beta) + (\beta - \gamma)$ και $a - \beta, \beta - \gamma \in I$.

Παρατήρηση. Αν το ιδεώδες I είναι mA και ο δακτύλιος A μοναδιαίος και αντιμεταθετικός, τότε η σχέση $a - \beta \in I$ γίνεται $a - \beta = m\gamma$ με $\gamma \in A$. Λέμε στην περίπτωση αυτή ότι $a \sim \beta \pmod{m}$ και όχι modulo I . Η κλάση ενός στοιχείου $a \pmod{I}$ είναι το σύνολο $a + I$. Πραγματικά, $x \in a + I$ τότε και μόνο, όταν $x = a + i$ με $i \in I$ ή $x - a \in I$, δηλαδή $x \sim a$. Συνεπώς ο δακτύλιος πηλίκο A/I είναι το πηλίκο $A/\sim$ με τους εσωτερικούς νόμους $(a + I) + (\beta + I) = (a + \beta) + I$, $(a + I)(\beta + I) = a\beta + I$.

ΑΣΚΗΣΕΙΣ

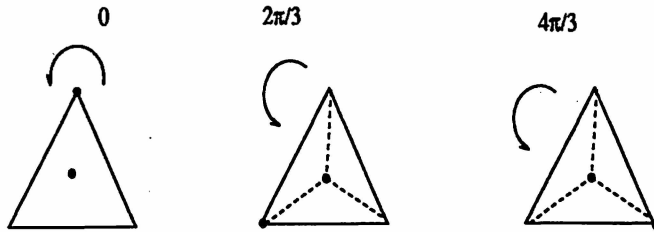
1. Βρείτε τα στοιχεία της ομάδας πηλίκο $\mathbb{Z}_5/G$, όπου $G = \{\bar{1}, \bar{4}\}$
2. Έστω G η ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_{15}$. Δείξτε ότι
 - i) $H = \{\bar{1}, \bar{4}\}$, $K = \{\bar{1}, \bar{14}\}$ είναι κανονικές υποομάδες της G .
 - ii) Η ομάδα πηλίκο G/K είναι κυκλική, ενώ η G/H δεν είναι κυκλική.
3. Βρείτε την ομάδα πηλίκο $\mathbb{Z}_6 / \langle 3 \rangle$.
4. Ποιά η τάξη του στοιχείου $5 + \langle 4 \rangle$ στην ομάδα πηλίκο $\mathbb{Z}_{12} / \langle 4 \rangle$.
5. Αν η ομάδα G είναι κυκλική τάξης 12 και a ένας γεννήτορας αυτής, βρείτε την ομάδα πηλίκο $G / \langle a^3 \rangle$.
6. Έστω $(G, \cdot)$ μια ομάδα και ότι για κάποιο φυσικό n είναι $(ab)^n = a^n b^n$ για όλα τα $a, b \in G$. Δείξτε ότι $\{x \in G; x^n = e\}$, $\{x^n; x \in G\}$ είναι κανονικές υποομάδες της G .
7. Έστω K η ομάδα πηλίκο $(\mathbb{R}, +) / (\mathbb{Z}, +)$. i) Βρείτε την τάξη του στοιχείου $\left(-\frac{2}{5}\right) + \mathbb{Z}$ της ομάδας K . ii) Δείξτε ότι το στοιχείο $\sqrt{2} + \mathbb{Z}$ δεν έχει πεπερασμένη τάξη στην ομάδα K .
8. Έστω Z το κέντρο μιας ομάδας G . Αν η ομάδα G/Z είναι κυκλική, δείξτε ότι η G είναι αντιμεταθετική. Βάσει αυτού, δείξτε ότι αν η τάξη μιας ομάδας G είναι p^2 , όπου p πρώτος, η ομάδα G είναι αντιμεταθετική.
9. Έστω $(G, +)$ η ομάδα των συναρτήσεων $f : \mathbb{R} \rightarrow \mathbb{R}$, όπου $+$ είναι η πρόσθεση των συναρτήσεων. Δείξτε ότι το σύνολο $K = \{f \in G; f(0) = 0\}$ είναι κανονική υποομάδα της G . Αν $a \in \mathbb{R}$ και $f_a \in G$ με $f_a(0) = a$, δείξτε ότι $G/K = \{f_a + K; a \in \mathbb{R}\}$.
10. Έστω M το σύνολο των πινάκων $\begin{pmatrix} a & 0 \\ \beta & \gamma \end{pmatrix}$ με στοιχεία από το σώμα $\mathbb{Z}_5$ και $a\gamma \neq 0$. Δείξτε ότι 1) ως προς τον πολλαπλασιασμό των πινάκων το M είναι ομάδα μη αντιμεταθετική. Βρείτε την τάξη της ομάδας αυτής. 2) Το σύνολο G των πινάκων στο M με $a = \gamma = 1$ αποτελούν κανονική υποομάδα της M . Δείξτε ότι η ομάδα πηλίκο M/G είναι αντιμεταθετική.
11. Έστω G μια κυκλική ομάδα τάξης m και ένας φυσικός αριθμός n . Δείξτε ότι (i) η συνάρτηση $\varphi_n : G \rightarrow G$ με τιμή $\varphi_n(a) = na$ είναι ενδομορφισμός της G . (ii) Αν $(n, m) = 1$, η φ_n είναι αμφιμονοσήμαντη. (iii) Αν $m = nk$, να επαληθεύσετε ότι $nG \cong \mathbb{Z}_k$ και $\ker \varphi_n = \mathbb{Z}_n$.

5 | Ομομορφισμοί ομάδων

Πολλές ομάδες φαινομενικά διάφορες μπορούν να ταυτιστούν από άποψη ιδιοτήτων και ο λογισμός σε μια ομάδα ανάγεται στο λογισμό σε μια άλλη ομάδα. Π.χ. ο λογισμός στην πολλαπλασιαστική ομάδα $(\mathbb{R}^+, \cdot)$ των θετικών πραγματικών αριθμών ανάγεται στην προσθετική ομάδα $(\mathbb{R}, +)$ με τη βοήθεια της συνάρτησης $x \mapsto \ln x$, που είναι αμφημονοσήμαντη του $\mathbb{R}^+$ επί του $\mathbb{R}$ και το γινόμενο $x \cdot y$ το απεικονίζει στο άθροισμα των εικόνων $\ln x, \ln y$ βάσει της ιδιότητας $\ln(x \cdot y) = \ln x + \ln y$

$$\begin{array}{ll} x \longrightarrow \ln x & x \cdot y \longrightarrow \ln x + \ln y \\ y \longrightarrow \ln y & x \cdot y = \ln^{-1}(\ln x + \ln y) \end{array}$$

Ας θεωρήσουμε και ένα άλλο παράδειγμα. Έστω G το σύνολο των στροφών ενός ισόπλευρου τριγώνου κατά γωνίες $0^\circ, \frac{2\pi}{3}, \frac{4\pi}{3}$ γύρω από το κέντρο του και στο επίπεδό του.



Κάθε στροφή είναι μια αμφιμονοσήμαντη συνάρτηση του επιπέδου του τριγώνου στον εαυτό του, που διατηρεί τις αποστάσεις. Αυτές οι συναρτήσεις στη Γεωμετρία λέγονται μετασχηματισμοί.

Η στροφή κατά 0° μετασχηματίζει κάθε σημείο στον εαυτό του, συνεπώς είναι η ταυτοτική συνάρτηση e . Αν ϕ είναι η στροφή κατά γωνία $\frac{2\pi}{3}$, το

γινόμενο $\phi \cdot \phi = \phi \circ \phi$ είναι η στροφή κατά γωνία $\frac{4\pi}{3}$. Συνεπώς $G = \{1, \phi, \phi^2\}$, όπου $\phi^2 = \phi \cdot \phi$. Ως προς τη σύνθεση $\circ$, η οποία συνήθως λέγεται γινόμενο, το G είναι ομάδα. Έχουμε $\phi \cdot \phi^2 = \phi^3 = e = \phi^2 \cdot \phi$. Η ομάδα αυτή $(G, \cdot)$ είναι σε σχέση με τη $(\mathbb{Z}_3, +)$ ανάλογη της σχέσης της ομάδας $(\mathbb{R}^+, \cdot)$ με την $(\mathbb{R}, +)$. Πραγματικά, έστω η συνάρτηση $f : \mathbb{Z}_3 \rightarrow G$ με τιμές $f(\bar{0}) = e$, $f(\bar{1}) = \phi$, $f(\bar{2}) = \phi^2$. Εύκολα επαληθεύουμε ότι

$$f(\bar{x} + \bar{y}) = f(\bar{x}) \cdot f(\bar{y}) \quad (1)$$

για όλα τα $\bar{x}, \bar{y} \in \mathbb{Z}_3$ και ότι η f είναι αμφιμονοσήμαντη της ομάδας $\mathbb{Z}_3$ επί της G . Έτσι $G = \{f(\bar{0}), f(\bar{1}), f(\bar{2})\}$, έχουμε δηλαδή μια νέα παράσταση των στοιχείων της G και το γινόμενο δύο στοιχείων $f(\bar{x})$, $f(\bar{y})$ της G αντιστοιχίζεται στο άθροισμα $\bar{x} + \bar{y}$. Συνεπώς μια ιδιότητα της ομάδας $\mathbb{Z}_3$, που θα εκφράζεται με την πράξη της και τα στοιχεία της, θα μεταφέρεται στην ομάδα G και αντίστροφα. Γι' αυτό λέμε ότι οι ομάδες $\mathbb{Z}_3, G$ ταυτίζονται με τη συνάρτηση f ή ότι είναι ισομόρφες.

Οι παρατηρήσεις αυτές μας οδηγούν στις γενικεύσεις και ορισμούς της επόμενης παραγράφου.

1. ΟΜΟΜΟΡΦΙΣΜΟΙ, ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ

Ορισμός 1. Έστω $(G, \cdot)$, $(E, *)$ δύο ομάδες. Μια συνάρτηση $f : G \rightarrow E$ λέγεται ομομορφισμός ή μορφισμός της G στην E , αν

$$f(x \cdot y) = f(x) * f(y)$$

για όλα τα $x, y \in G$.

επιμορφισμός, λέγεται ένας ομομορφισμός f επί της E ($: f(G) = E$)
μονομορφισμός, λέγεται ένας ομομορφισμός, που είναι συνάρτηση αμφι-
 μονοσήμαντη

ισομορφισμός, λέγεται ένας ομομορφισμός, που είναι μονομορφισμός
 και επιμορφισμός, δηλαδή αμφιμονοσήμαντη και επί
αυτομορφισμός, λέγεται ένας ισομορφισμός της ομάδας G στο εαυτό της
ενδομορφισμός, λέγεται ένας ομομορφισμός της ομάδας G στον εαυτό
 της.

Η ομάδα G λέγεται:

ομόμορφη της E , αν υπάρχει ένας επιμορφισμός $f : G \rightarrow E$. Γράφουμε
 $G \simeq E$.

ισόμορφη της E , αν υπάρχει ισομορφισμός $f : G \rightarrow E$. Γράφουμε τότε
 $G \cong E$.

Προφανώς η σύνθεση $h = f \circ g$ δύο ομομορφισμών f, g είναι ομομορφισμός,
 γιατί

$$h(x \cdot y) = f \circ g(x \cdot y) = f(g(x) \cdot g(y)) = f(g(x)) \cdot f(g(y)) = h(x) \cdot h(y)$$

Είναι εύκολο να δούμε ακόμη ότι, αν f είναι ισομορφισμός της $(G, \cdot)$ επί της
 $(E, *)$, η f^{-1} είναι ισομορφισμός της E επί της G , γιατί δύο οποιαδήποτε
 στοιχεία a, β της E έχουν την μορφή $f(x) = a, f(y) = \beta$ με $x, y \in G$ και

$$f^{-1}(a * \beta) = f^{-1}(f(x) * f(y)) = f^{-1}(f(x \cdot y)) = x \cdot y = f^{-1}(a) \cdot f^{-1}(\beta)$$

Κατά συνέπεια η σχέση $G \sim E$ τότε και μόνο, όταν υπάρχει ισομορφισμός
 $f : G \rightarrow E$, είναι μια σχέση ισοδυναμίας στο σύνολο των ομάδων.

Κάθε κλάση είναι όλες οι ομάδες που είναι ισόμορφες μεταξύ τους. Το
πρόβλημα της ταξινόμησης των ομάδων δοσμένης τάξης d είναι η εύρεση
 των μη ισόμορφων ομάδων τάξης d .

Π.χ. υπάρχουν δύο μόνο μη ισόμορφες ομάδες τάξης 4. Η μία είναι η $\mathbb{Z}_4$ και
 η άλλη η ομάδα Klein (§6, Κεφ.3) $G = \{e, a, \beta, a\beta\}$ με $a^2 = \beta^2 = (a\beta)^2 = e$.

Ορισμός 2. **Πυρήνας** ενός ομομορφισμού $f : G \rightarrow E$ λέγεται το
 σύνολο

$$\text{Ker } f = \{x \in G; f(x) = 1_E\}.$$

Το σύνολο $f(G) = \{f(x); x \in G\}$ λέγεται **εικόνα** του f και γράφεται $\text{Im } f$.

Παραδείγματα

1. Η συνάρτηση $f : x \rightarrow |x|$ είναι ομομορφισμός της $(\mathbb{C}^*, \cdot)$ επί της $(\mathbb{R}^+, \cdot)$, γιατί $f(x \cdot y) = |xy| = |x| \cdot |y| = f(x)f(y)$. Ο πυρήνας του f είναι $\{x \in \mathbb{C}^*; |x| = 1\}$, δηλαδή ο μοναδιαίος κύκλος κέντρου 0.

2. Η συνάρτηση $f : z \rightarrow z^2$ είναι ομομορφισμός της $(\mathbb{C}^*, \cdot)$ στον εαυτό της (άρα ενδομορφισμός αυτής), γιατί

$$f(z \cdot w) = (zw)^2 = z^2 \cdot w^2 = f(z) \cdot f(w)$$

Ο πυρήνας αυτού είναι $\{z \in \mathbb{C}^*; z^2 = 1\} = \{1, -1\}$.

3. Η συνάρτηση $f : z \rightarrow \operatorname{Re} z$ είναι ομομορφισμός της $(\mathbb{C}, +)$ επί της $(\mathbb{R}, +)$, γιατί, αν $z = x + iy$, $\operatorname{Re} z = x$, $f(z) = x$ και $f(z + z') = f((x + x') + i(y + y')) = x + x' = f(z) + f(z')$. Ο πυρήνας είναι $\{z \in \mathbb{C}; \text{με } f(z) = 0\} = \{z = x + iy; x = 0\} = \{iy; y \in \mathbb{R}\} = i\mathbb{R}$.

4. Αν $(G, \cdot)$ είναι μια ομάδα, $a \in G$ και $f_a : G \rightarrow G$ με $f_a(x) = axa^{-1}$, η συνάρτηση f_a είναι αυτομορφισμός της G , γιατί

$$f_a(xy) = axya^{-1} = axa^{-1} \cdot aya^{-1} = f_a(x)f_a(y) \quad ,$$

$$f_a(x) = f_a(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$$

και $y = f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$.

Συνοψίζουμε τα διάφορα είδη ομομορφισμών που διακρίναμε:

$$\text{ομομορφισμός} + \begin{cases} \text{επί} \\ \text{αμφιμονοσήμαντη} \\ \text{επί, αμφιμονοσήμαντη} \\ \text{στον εαυτό της} \\ \text{επί, αμφιμονοσήμαντη} \\ \text{στον εαυτό της} \end{cases} = \begin{cases} \text{επιμορφισμός} \\ \text{μονομορφισμός} \\ \text{ισομορφισμός} \\ \text{ενδομορφισμός} \\ \text{αυτομορφισμός} \end{cases}$$

Θεώρημα 1. Έστω $(G, \cdot), (E, *)$ δύο ομάδες με μονάδες $1_G, 1_E$ και $f : G \rightarrow E$ ένας ομομορφισμός. Τότε

- i) $f(1_G) = 1_E$
- ii) $f(x^{-1}) = f(x)^{-1}$ και $f(x^n) = f(x)^n$ για κάθε $n \in \mathbb{Z}$
- iii) A υποομάδα της $G \Rightarrow f(A)$ υποομάδα της E
- iv) B υποομάδα της $E \Rightarrow f^{-1}(B)$ υποομάδα της G

v) Αν η f είναι ισομορφισμός, $| \langle x \rangle | = | \langle f(x) \rangle |$

Απόδειξη.

- i) Έχουμε $f(1_G) = f(1_G \cdot 1_G) = f(1_G) * f(1_G)$ και $f(1_G) = f(1_G) * 1_E$.
 Συνεπώς $f(1_G) * 1_E = f(1_G) * f(1_G)$ ή $1_E = f(1_G)$.
- ii) Προφανώς $f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(1_G) = 1_E$ και όμοια $f(x^{-1}) * f(x) = 1_E$. Συνεπώς $f(x^{-1}) = f(x)^{-1}$.
 Αν n είναι φυσικός, έχουμε $f(x^n) = f(x \cdot x \cdots x) = f(x) * f(x) * \cdots * f(x) = f(x)^n$. Αν $n = 0$, $f(1_G) = 1_E$ ή $f(x^0) = f(x)^0$. Αν n αρνητικός ακέραιος, είναι $f(x^{-n}) = f(x)^{-n}$ ή $f(y^n) = f(y)^n$, όπου $y = x^{-1}$. Όταν όμως το x διατρέχει την ομάδα G , το $y = x^{-1}$ διατρέχει επίσης την G . Άρα $f(x^n) = f(x)^n$ για κάθε $x \in G$ και $n \in \mathbb{Z}$.
- iii) Αν $x, y \in f(A)$, είναι $x = f(a)$, $y = f(\beta)$ με $a, \beta \in A$, οπότε $x * y^{-1} = f(a) * f(\beta)^{-1} = f(a \cdot \beta^{-1}) \in f(A)$.
- iv) Έστω $a, \beta \in f^{-1}(B)$. Τότε $f(a), f(\beta) \in B$, $f(a)^{-1} * f(\beta) = f(a^{-1}\beta) \in B$, οπότε $a^{-1} \cdot \beta \in f^{-1}(B)$ και $f^{-1}(B)$ είναι υποομάδα της G .
- v) Έστω ότι υπάρχει φυσικός n με $x^n = 1_G$. Τότε $f(1_G) = f(x^n) = f(x \cdot x \cdots x) = f(x) * f(x) * \cdots * f(x) = f(x)^n = 1_E$. Αν η τάξη του x είναι πεπερασμένη, έστω d , τότε d είναι ο μικρότερος φυσικός με $x^d = 1_G$. Συνεπώς η τάξη d' του $f(x)$ είναι πεπερασμένη και $d' \geq d$. Αντίστροφα, αν $f(x)^m = 1_E$, είναι $f(x^m) = 1_E = f(1_G)$, συνεπώς $x^m = 1_G$ και $d' \leq d$. Άρα $d' = d$. Αν η τάξη του x είναι άπειρη, έχουμε $x^m \neq x^n$ για $m \neq n$, οπότε και $f(x)^m \neq f(x)^n$ για $m \neq n$, δηλαδή και η τάξη του $f(x)$ είναι άπειρη. $\square$

Παρατήρηση. Αν οι νόμοι των ομάδων συμβολίζονται προσθετικά και f είναι ομομορφισμός της $(G, +)$ στην $(E, +)$, τότε έχουμε

$$f(0_G) = 0_E, \quad f(-x) = -f(x), \quad f(n \cdot x) = n \cdot f(x)$$

αντί των

$$f(1_G) = 1_E, \quad f(x^{-1}) = f(x)^{-1}, \quad f(x^n) = f(x)^n$$

Πρόταση 1. Έστω K κανονική υποομάδα της ομάδας $(G, \cdot)$. Η συνάρτηση $\phi_K : G \rightarrow G/K$ με τιμή $\phi_K(x) = xK$ είναι επιμορφισμός.

Απόδειξη. Είναι για όλα τα $x, y \in G$

$$\phi_K(xy) = xyK = xK \cdot yK = \phi_K(x) \cdot \phi_K(y)$$

Η ϕ_K λέγεται **κανονικός επιμορφισμός** της G επί της G/K . □

Πρόταση 2. Έστω f ένας ομομορφισμός της ομάδας G στην G_1 . Τότε ο πυρήνας K του f είναι κανονική υποομάδα της G και ο f είναι μονομορφισμός τότε και μόνο, όταν $K = \{1_G\}$.

Απόδειξη. Σύμφωνα με το θεώρημα 1 ο πυρήνας K είναι υποομάδα της G , γιατί $K = f^{-1}(1_{G_1})$. Είναι κανονική, γιατί για κάθε $x \in G$,

$$f(x^{-1}Kx) = f(x)^{-1} * f(K) * f(x) = f(x)^{-1} * \{1_{G_1}\} * f(x) = f(x)^{-1} * f(x) = 1_{G_1}$$

δηλαδή $x^{-1}Kx \subseteq K$.

Έστω ότι $K = \{1_G\}$ και $f(x) = f(y)$. Τότε $f(x^{-1}y) = f(x)^{-1} * f(y) = 1_{G_1}$, συνεπώς $x^{-1}y \in K$, $x^{-1}y = 1_G$, $x = y$, δηλαδή η f είναι αμφιμονοσήμαντη. Αντίστροφα, αν η f είναι αμφιμονοσήμαντη και $x \in \text{Ker } f$, έχουμε $f(x) = 1_{G_1} = f(1_G)$, συνεπώς $x = 1_G$ και $\text{Ker } f = \{1_G\}$. □

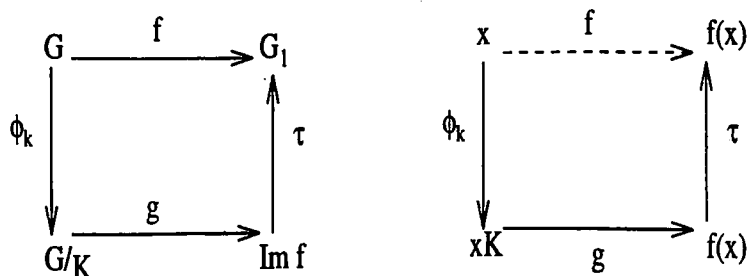
2. ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΟΥ ΟΜΑΔΩΝ

Το παρακάτω θεώρημα είναι γνωστό ως **πρώτο θεώρημα ισομορφισμού ομάδων**.

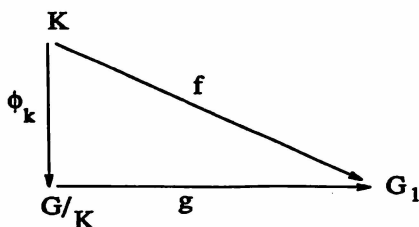
Θεώρημα 1. Ένας ομομορφισμός f με πυρήνα K της ομάδας G στην G_1 αναλύεται σε γινόμενο:

- α) του κανονικού επιμορφισμού $\phi_K : G \rightarrow G/K$ με $\phi_K(x) = xK$,
- β) ενός ισομορφισμού $g : G/K \rightarrow \text{Im } f$ με $g(xK) = f(x)$,
- γ) ενός ομομορφισμού $\tau : \text{Im } f \rightarrow G_1$ με $\tau(f(x)) = f(x)$

δηλαδή $f = \tau \circ g \circ \phi_K$. Λέμε τότε ότι το παρακάτω διάγραμμα είναι **αντιμεταθετικό**



Αν ο f είναι επιμορφισμός, τότε το διάγραμμα γίνεται



$$x \mapsto xK \mapsto f(x)$$

$$f = g \circ \phi_K$$

και $G/K \cong G_1$.

Απόδειξη. Η συνάρτηση $g: G/K \rightarrow \text{Im } f$ με $g(xK) = f(x)$ είναι καλά ορισμένη, γιατί, αν $xK = yK$, έχουμε $x = ya$ με $a \in K$, οπότε $f(x) = f(y)f(a) = f(y) * 1_{G_1} = f(y)$, δηλαδή $g(xK) = g(yK)$. Είναι ομομορφισμός, γιατί

$$g(xK \cdot yK) = g(xyK) = f(xy) = f(x)f(y) = g(xK)g(yK)$$

και ισομορφισμός, γιατί $g(xK) = 1_G$, συνεπάγεται $f(x) = 1_G$ ή $x \in \text{Ker } f$, δηλαδή $xK = K = 1_{G/K}$, που σημαίνει ότι ο πυρήνας του g είναι η μονάδα του G/K . Τέλος $\tau \circ g \circ \phi_K(x) = \tau \circ g(xK) = \tau(f(x)) = f(x)$ για κάθε $x \in G$, δηλαδή $f = \tau \circ g \circ \phi_K$.

Αν η f είναι επιμορφισμός της G επί της G_1 , τότε η ομάδα πηλίκο $G/\text{Ker } f \cong G_1$. Ένας ισομορφισμός είναι η συνάρτηση $g: xK \mapsto f(x)$, όπου $K = \text{Ker } f$. Γιατί $\text{Im } f = G_1$. $\square$

Θεώρημα 2. Έστω G μια ομάδα και H, K δύο κανονικές υποομάδες αυτής. Έστω $H \subset K$. Η ομάδα πηλίκο K/H είναι κανονική υποομάδα της G/H και το πηλίκο

$$(G/H) / (K/H) \cong G/K$$

Απόδειξη. Θεωρούμε τη συνάρτηση $\phi: G/H \rightarrow G/K$ με τιμή $\phi(xH) = xK$. Είναι καλά ορισμένη, γιατί, αν $xH = yH$, έχουμε $x = ya$ με $a \in H$ και συνεπώς $\phi(xH) = yaK = yK = \phi(yH)$. Η ϕ είναι ομομορφισμός, γιατί $\phi(xH \cdot yH) = \phi(xyH) = xyK = xKyK = \phi(xH) \cdot \phi(yH)$. Ο πυρήνας της ϕ είναι

$$\{xH; \phi(xH) = K\} = \{xH; xK = K\} = \{xH; x \in K\} = K/H$$

Βάσει του θεωρήματος 1 έπεται το συμπέρασμα. $\square$

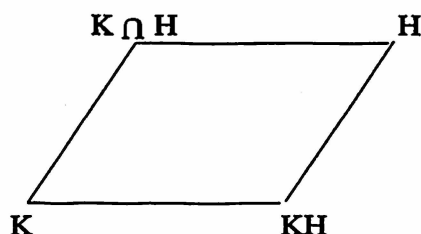
Θεώρημα 3. Έστω G μια ομάδα, H μια κανονική υποομάδα και K μια υποομάδα της G . Τότε $H \cap K$ είναι κανονική υποομάδα της K , H κανονική υποομάδα της ομάδας $HK = KH$ και $K/K \cap H \cong KH/H$.

Απόδειξη. Σύμφωνα με την πρόταση 3§1 Κεφ.4, η KH είναι υποομάδα της G . Προφανώς περιέχει την H σαν υποομάδα, η οποία είναι κανονική υποομάδα, γιατί για οποιοδήποτε $kh \in KH$ έχουμε

$$(kh)^{-1}H(kh) = h^{-1}k^{-1}Hkh = h^{-1}Hh = H$$

Έστω τώρα η συνάρτηση $\phi : K \rightarrow KH/H$ με τιμή $\phi(k) = kH$. Είναι επιμορφισμός, γιατί

$$\phi(kk') = (kk')H = kH \cdot k'H = \phi(k)\phi(k').$$



και κάθε στοιχείο της KH/H είναι της μορφής $(kh)H$ με $k \in K, h \in H$, το οποίο γράφεται $(kh)H = khH = kH = \phi(k)$. Ο πυρήνας του επιμορφισμού ϕ είναι

$$\{x \in K; xH = H\} = \{x \in K; x \in H\} = K \cap H$$

Σύμφωνα με το θεώρημα 1' προκύπτει το συμπέρασμα. □

3. ΤΑΞΙΝΟΜΗΣΗ ΚΥΚΛΙΚΩΝ ΟΜΑΔΩΝ

Σαν πρώτη εφαρμογή του θεωρήματος ισομορφισμού των ομάδων θα αναζητήσουμε τις μη ισόμορφες κυκλικές ομάδες.

Θεώρημα 1. Μια άπειρη κυκλική ομάδα είναι ισόμορφη με την ομάδα των ακεραίων. Μια κυκλική ομάδα πεπερασμένης τάξης m είναι ισόμορφη με την ομάδα $\mathbb{Z}_m$.

Απόδειξη. Έστω $G = \langle a \rangle$ μια κυκλική ομάδα και $f : \mathbb{Z} \rightarrow G$ με τιμή $f(n) = a^n$. Η f είναι ομομορφισμός, γιατί $f(nm) = a^{nm} = a^n \cdot a^m = f(n)f(m)$. Προφανώς είναι επιμορφισμός. Αν K ο πυρήνας του f , έχουμε

$$\mathbb{Z}/K \cong G.$$

Αν η G είναι άπειρη, τότε $a^n \neq a^m$ για $n \neq m$ δηλαδή ο f είναι ισομορφισμός, οπότε $K = \{0\}$ και $\mathbb{Z}/K \cong \mathbb{Z}$. Άρα $G \cong \mathbb{Z}$. Αν η G είναι πεπερασμένη,

έστω τάξης m , τότε $K = \{n \in \mathbb{Z}; a^n = e\} = \{n \in \mathbb{Z}; n/m\} = m\mathbb{Z}$, οπότε $G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. $\square$

Συνεχίζουμε με άλλες εφαρμογές του θεωρήματος ισομορφισμού.

Εφαρμογή 1. 'Εστω S ο μοναδιαίος κύκλος στο μιγαδικό επίπεδο, $S = \{z; |z| = 1\}$. Προφανώς S είναι υποομάδα της πολλαπλασιαστικής ομάδας $\mathbb{C}^* = \mathbb{C} - \{0\}$ των μιγαδικών αριθμών. Η συνάρτηση $\phi: \mathbb{R} \rightarrow S$ με τιμή $\phi(x) = \cos 2\pi x + i\sin 2\pi x$ είναι ομομορφισμός της ομάδας $(\mathbb{R}, +)$ επί της S . Ο πυρήνας της ϕ είναι $\mathbb{Z}$, γιατί $\phi(x) = 1$ τότε και μόνο, όταν $\cos 2\pi x = 1$ και $\sin 2\pi x = 0$ ή $x \in \mathbb{Z}$. 'Αρα $S \cong \mathbb{R}/\mathbb{Z}$.

Εφαρμογή 2. 'Εστω G μια ομάδα και $Z(G) = \{a \in G; (\forall x \in G) xa = ax\}$. Για κάθε $a \in G$, η συνάρτηση $f_a: G \rightarrow G$ με $f_a(x) = axa^{-1}$ είναι αυτομορφισμός της G , που λέγεται εσωτερικός αυτομορφισμός της G . Το γινόμενο δύο εσωτερικών αυτομορφισμών f_a, f_b είναι ο αυτομορφισμός f_{ab} , γιατί

$$f_a \circ f_b(x) = f_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = f_{ab}(x)$$

συνεπώς f_e είναι μοναδιαίο στοιχείο και $f_{a^{-1}}$ το αντίστροφο του f_a , αφού $f_a f_{a^{-1}} = f_{aa^{-1}} = f_e = f_{a^{-1}} f_a$. 'Ετσι το σύνολο $I(G)$ των εσωτερικών αυτομορφισμών είναι ομάδα. Η συνάρτηση $a \mapsto f_a$ είναι επιμορφισμός της G στην $I(G)$. Ο πυρήνας είναι $\{a \in G; g(a) = f_e\} = \{a \in G; f_a = f_e\} = \{a \in G; axa^{-1} = x\} = \{a \in G; ax = xa\} = Z(G)$. Συνεπώς $G/Z(G) \cong I(G)$.

Εφαρμογή 3. Προφανώς $m\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$. Συνεπώς

$$(\mathbb{Z}/m\mathbb{Z}) / (m\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

Εφαρμογή 4. 'Εστω $GL(n, K)$ το σύνολο των αντιστρέψιμων πινάκων $n \times n$ με συντελεστές από το σώμα K . Προφανώς είναι μια πολλαπλασιαστική ομάδα. Η ορίζουσα $D: GL(n, K) \rightarrow K^*$ είναι ομομορφισμός ομάδων. Ο πυρήνας είναι το σύνολο των πινάκων A με $|A| = 1$ και συμβολίζεται με $SL(n, K)$. 'Αρα

$$GL(n, K)/SL(n, K) \cong K^*.$$

4. ΑΥΤΟΜΟΡΦΙΣΜΟΙ, ΑΝΑΛΛΟΙΩΤΕΣ ΥΠΟΟΜΑΔΕΣ

Έστω $(G, \cdot)$ μια ομάδα. Για κάθε $a \in G$ ορίζεται μια συνάρτηση $f_a : G \rightarrow G$ με τιμή

$$f_a(x) = axa^{-1} \quad (1)$$

Η συνάρτηση f_a είναι αυτομορφισμός της ομάδας G και λέγεται **εσωτερικός** αυτομορφισμός αυτής. Πραγματικά: Είναι ομομορφισμός, γιατί

$$f_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f_a(x)f_a(y).$$

Είναι αμφιμονοσήμαντη, γιατί $\ker f_a = \{e\}$, αφού $f_a(x) = e$ τότε και μόνο, όταν $e = axa^{-1}$ ή $a^{-1}ea = x$ ή $x = e$.

Τέλος η f_a είναι επί της G , γιατί για κάθε $y \in G$ έχουμε $f_a(a^{-1}ya) = a(a^{-1}ya)a^{-1} = y$.

Ορισμός 1. Οι αυτομορφισμοί της μορφής (1) λέγονται **εσωτερικοί** αυτομορφισμοί της ομάδας G .

Πρόταση 1. Το σύνολο $I(G)$ των εσωτερικών αυτομορφισμών της ομάδας G είναι κανονική υποομάδα της ομάδας των αυτομορφισμών της G .

Απόδειξη. Προφανώς για οποιαδήποτε $a, \beta \in G$,

$$\begin{aligned} f_{a\beta}(x) &= a\beta x(a\beta)^{-1} = a\beta x\beta^{-1}a^{-1} = af_{\beta}(x)a^{-1} \\ &= f_a(f_{\beta}(x)) = f_a \circ f_{\beta}(x), \end{aligned}$$

δηλαδή $f_a \circ f_{\beta} = f_{a\beta} \in I(G)$. Επί πλέον, αν e το ουδέτερο της ομάδας, έχουμε $f_e(x) = exe^{-1} = x = 1_G(x)$, δηλαδή $f_e = 1_G$ και τέλος $(f_a)^{-1} = f_{a^{-1}}$, αφού $f_{a^{-1}} \circ f_a = f_{aa^{-1}} = f_e$. Έτσι $I(G)$ είναι υποομάδα της ομάδας των αυτομορφισμών $\text{Aut}(G)$ της G . Είναι κανονική υποομάδα αυτής, γιατί για κάθε αυτομορφισμό f της G και κάθε εσωτερικό αυτομορφισμό f_a έχουμε

$$\begin{aligned} f f_a f^{-1}(x) &= f(f_a(f^{-1}(x))) = f(af^{-1}(x)a^{-1}) = \\ &= f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a)^{-1} \\ &= f_{f(a)}(x) \end{aligned}$$

δηλαδή $f f_a f^{-1} = f_{\beta}$ με $\beta = f(a)$ ή $fI(G)f^{-1} \subseteq I(G)$. □

Πόρισμα. Το κέντρο Z της ομάδας G (§1, Κεφ.3) είναι κανονική υποομάδα της G και

$$G/Z \cong I(G)$$

Γιατί η συνάρτηση $h : G \rightarrow I(G)$ με τιμή $h(a) = f_a$ είναι ομομορφισμός με πυρήνα Z , αφού $f_a = 1_G$ τότε και μόνο, όταν για κάθε $x \in G$, $axa^{-1} = x$ ή $ax = xa$ ή $a \in Z$.

Ορισμός 2. Μια υποομάδα H της G λέγεται **αναλλοίωτη** (ή χαρακτηριστική) υποομάδα της G , αν για κάθε αυτομορφισμό f της G , $f(H) = H$.

Η συνθήκη αυτή είναι ισοδύναμη της $f(H) \subseteq H$ για κάθε $f \in \text{Aut}G$. Γιατί έχουμε και $f^{-1}(H) \subseteq H$ ή $H \subseteq f(H)$, άρα $f(H) = H$.

Παράδειγμα. Το κέντρο Z μιας ομάδας είναι αναλλοίωτη υποομάδα της G .

Πραγματικά, έστω $f \in \text{Aut}G$. Για κάθε $x \in Z$ και κάθε $a \in G$ έχουμε $xa = ax$ συνεπώς $f(x)f(a) = f(a)f(x)$. Επειδή κάθε $\beta \in G$ είναι της μορφής $f(a)$ με $a \in G$, έχουμε $f(x)\beta = \beta f(x)$ για κάθε $\beta \in G$, δηλαδή $f(x) \in Z$ ή $f(Z) \subseteq Z$. Άρα $f(Z) = Z$ και η ομάδα Z είναι αναλλοίωτη.

Υποομάδα των μεταθετών

Η ομάδα G είναι αντιμεταθετική, αν για οποιαδήποτε $a, \beta \in G$ είναι $a\beta = \beta a$ ή $a^{-1}\beta^{-1}a\beta = e$. Συνεπώς σε μια μη αντιμεταθετική ομάδα υπάρχουν στοιχεία a, β με $a^{-1}\beta^{-1}a\beta \neq e$. Το στοιχείο $a^{-1}\beta^{-1}a\beta$ λέγεται **μεταθέτης** των a, β και συμβολίζεται με $[a, \beta]$. Έτσι

$$[a, \beta] = a^{-1}\beta^{-1}a\beta$$

Προφανώς $\beta a[a, \beta] = a\beta$ και $[a, \beta]^{-1} = [\beta, a]$.

Η υποομάδα της G που παράγεται από το σύνολο των μεταθετών $[a, \beta]$ με $a, \beta \in G$ λέγεται **υποομάδα των μεταθετών** ή **πρώτη παράγωγος** υποομάδα της G και συμβολίζεται με G' . Είναι προφανές ότι η ομάδα των μεταθετών G' είναι αναλλοίωτη υποομάδα της G , γιατί για κάθε αυτομορφισμό f , έχουμε

$$f([a, \beta]) = f(a^{-1}\beta^{-1}a\beta) = f(a)^{-1}f(\beta)^{-1}f(a)f(\beta) = [f(a), f(\beta)]$$

και συνεπώς ένα γινόμενο μεταθετών απεικονίζεται σε γινόμενο μεταθετών. Άρα $f(G') \subseteq G'$, οπότε $f(G') = G'$. Είναι $G' = \{e\}$ τότε και μόνο, όταν η G είναι αντιμεταθετική. Η υποομάδα των μεταθετών της G' λέγεται **δεύτερη παράγωγος** υποομάδα της G και συμβολίζεται με G'' . Συνεπώς $G'' = (G')'$. Γενικά ορίζουμε m -παράγωγο υποομάδα της G , την υποομάδα

$$G^{(m)} = (G^{(m-1)})'$$

Θεώρημα 1. Η υποομάδα των μεταθετών G' μιας ομάδας G είναι κανονική υποομάδα. Το πηλίκο G/H της G με μια κανονική υποομάδα H είναι αντιμεταθετική ομάδα τότε και μόνο, όταν $G' \subseteq H$.

Απόδειξη. Έστω $z \in G'$ και $a \in G$. Έχουμε

$$[a, z^{-1}] = a^{-1}(z^{-1})^{-1}az^{-1} = a^{-1}zaz^{-1} \in G'$$

συνεπώς $a^{-1}za = [a, z^{-1}]z \in G'$, δηλαδή $G' \trianglelefteq G$. Έστω ότι η ομάδα G/H είναι αντιμεταθετική. Αν $x, y \in G$, έχουμε

$$\begin{aligned} H &= [xH, yH] = (xH)^{-1}(yH)^{-1}xHyH = x^{-1}Hy^{-1}HxHyH \\ &= x^{-1}y^{-1}xyH = [x, y] \cdot H \end{aligned}$$

συνεπώς $[x, y] \in H$ και $G' \subseteq H$.

Έστω τώρα ότι $G' \subseteq H$. Τότε

$$xHyH = xyH = xy[x, y]H = yxH = yHxH$$

δηλαδή η ομάδα G/H είναι αντιμεταθετική. □

Πόρισμα. Η ομάδα G/G' είναι αντιμεταθετική.

Παράδειγμα. Έστω $G = \{e, a, \beta, \gamma, \delta, \epsilon\}$. Ο πίνακας

	e	a	β	γ	δ	ϵ
e	e	a	β	γ	δ	ϵ
a	a	β	e	δ	ϵ	γ
β	β	e	a	ϵ	γ	δ
γ	γ	ϵ	δ	e	β	a
δ	δ	γ	ϵ	a	e	β
ϵ	ϵ	δ	γ	β	a	e

$$G = \{e, a, a^2, \gamma, a\gamma, a^2\gamma\}$$

ορίζει ένα εσωτερικό νόμο επί του G , ως προς τον οποίο το G είναι ομάδα (είναι η ομάδα των μετασχηματισμών που απεικονίζουν ισόπλευρο τρίγωνο στον εαυτό του βλ.Κεφ.14). Βρείτε την ομάδα G' .

Η ομάδα G έχει τρεις υποομάδες, τις $G_1 = \{e, a, \beta\}$, $G_2 = \{e, \gamma\}$, $G_3 = \{e, \delta\}$. Η ομάδα G_2 δεν είναι κανονική υποομάδα της G , γιατί $aG_2 = \{a, \delta\} \neq G_2a = \{a, \epsilon\}$. Όμοια η G_3 δεν είναι κανονική υποομάδα της G , αφού $aG_3 = \{a, \epsilon\} \neq G_3a = \{a, \gamma\}$. Άρα πρέπει $G' = G_1$.

ΑΣΚΗΣΕΙΣ

1. Βρείτε τους ενδομορφισμούς, τους επιμορφισμούς και αυτομορφισμούς των ομάδων $(\mathbb{Z}, +)$, $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_m, +)$.

2. Βρείτε τους ισομορφισμούς της ομάδας $G = \{e, a, a^2, a^3\}$ επί της $G' = \{1, -1, i, -i\}$.

3. Έστω A μια αντιμεταθετική ομάδα και $\text{Hom } A$ το σύνολο των ομομορφισμών $f : A \rightarrow A$. Στο σύνολο $\text{Hom } A$ ορίζουμε πρόσθεση και πολλαπλασιασμό ως εξής:

$$(f + g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(g(x))$$

Δείξτε ότι $(\text{Hom}, +, \cdot)$ είναι δακτύλιος.

4. Δείξτε ότι η συνάρτηση $\varphi : x \mapsto \sin x + i \cos x$ είναι ένας ομομορφισμός της ομάδας $(\mathbb{R}, +)$ μέσα στην ομάδα $(\mathbb{C}^*, \cdot)$. Δείξτε ότι $\mathbb{R}/\langle 2\pi \rangle$ είναι ισόμορφη της ομάδας $\{z; |z| = 1\}$.

5. Βρείτε τον ομομορφισμό h της ομάδας $\mathbb{Z}_6$ στην $\mathbb{Z}_2$ με $h(5) = \bar{2}$ και τον πυρήνα του.

6. Έστω G μια ομάδα και e το ουδέτερο αυτής. Ορίζουμε μια ακολουθία υποομάδων (G_n) της G ως εξής: $G_0 = G$, $G_{n+1} = \langle xyx^{-1}y^{-1}; x \in G_n, y \in G \rangle$. Δείξτε ότι: i) για κάθε αυτομορφισμό f της G και κάθε φυσικό n , $f(G_n) \subseteq G_n$.

ii) G_n είναι κανονική υποομάδα της G .

iii) Η υποομάδα G_n/G_{n+1} περιέχεται στο κέντρο της G/G_{n+1} .

7. Δείξτε ότι $\mathbb{Z}/2\mathbb{Z} \cong 3\mathbb{Z}/6\mathbb{Z}$.

8. Έστω G_0, G_1, G_2 ομάδες, f_1 επιμορφισμός της G_0 επί της G_1 , f_2 ομομορφισμός της G_0 μέσα στην G_2 τέτοιος, ώστε $\ker f_1 \subseteq \ker f_2$.

i) Δείξτε ότι υπάρχει ένας ομομορφισμός $g : G_1 \rightarrow G_2$ και ένας μόνο, ώστε $f_2 = g \circ f_1$.

ii) Δείξτε ότι $\ker g = f_1(\ker f_2)$.

9. Έστω m, n φυσικοί. Δείξτε ότι $\mathbb{Z}_{mn}/m\mathbb{Z}_{mn} \cong \mathbb{Z}_n$.

10. Αν οι m, n είναι σχετικά πρώτοι, δείξτε ότι $\mathbb{Z}_{mn}^*/m\mathbb{Z}_m^* \cong \mathbb{Z}_n^*$.

11. Έστω E το σύνολο των κανονικών υποομάδων K της ομάδας G για τις οποίες το πηλίκο G/K είναι ομάδα αντιμεταθετική. Ν' αποδείξετε ότι $G' = \bigcap_{K \in E} K$.

12. Αν A είναι αναλλοίωτη υποομάδα της B και η B είναι αναλλοίωτη υποομάδα της G , δείξτε ότι η A είναι αναλλοίωτη υποομάδα της G .

6 | Ευθέα γινόμενα

1. ΕΥΘΥ ΓΙΝΟΜΕΝΟ ΟΜΑΔΩΝ, ΔΑΚΤΥΛΙΩΝ

Θα αναφέρουμε μια ακόμη μέθοδο κατασκευής ομάδων με τη βοήθεια δύο ή περισσότερων ομάδων, η οποία εφαρμόζεται και στις αλγεβρικές δομές των ημιομάδων, μονοειδών και δακτυλίων. Η μέθοδος είναι πολύ χρήσιμη στο πρόβλημα της ταξινόμησης των ομάδων δοσμένης τάξης, όπως και η μέθοδος κατασκευής της ομάδας πηλίκο, που είδαμε στο Κεφ.4.

Έστω A, B δύο ομάδες με ουδέτερα e_A, e_B . Το καρτεσιανό γινόμενο $A \times B$ γίνεται ομάδα ως προς το νόμο

$$(a, \beta) \cdot (a', \beta') = (aa', \beta\beta') \quad (1)$$

με ουδέτερο $e = (e_A, e_B)$. Πραγματικά, ο νόμος είναι εσωτερικός, αφού $aa' \in A$ και $\beta\beta' \in B$, όταν $a, a' \in A$ και $\beta, \beta' \in B$. Είναι προσεταιριστικός, γιατί

$$\begin{aligned} (a, \beta) \cdot [(a', \beta') \cdot (a'', \beta'')] &= (a, \beta) \cdot (a'a'', \beta'\beta'') = (a(a'a''), \beta(\beta'\beta'')) \\ [(a, \beta) \cdot (a', \beta')] \cdot (a'', \beta'') &= \dots = ((aa')a'', (\beta\beta')\beta'') \end{aligned}$$

$$\text{και} \quad a(a'a'') = (aa')a'' \quad , \quad \beta(\beta'\beta'') = (\beta\beta')\beta''.$$

Το στοιχείο (e_A, e_B) είναι πραγματικά ουδέτερο, γιατί $(a, \beta) \cdot (e_A, e_B) = (a \cdot e_A, \beta \cdot e_B) = (a, \beta)$ και $(e_A, e_B) \cdot (a, \beta) = (e_A \cdot a, e_B \cdot \beta) = (a, \beta)$. Το αντίστροφο του (a, β) είναι το (a^{-1}, β^{-1}) , γιατί $(a, \beta)(a^{-1}, \beta^{-1}) = (aa^{-1}, \beta\beta^{-1}) = (e_A, e_B)$ και όμοια $(a^{-1}, \beta^{-1})(a, \beta) = (e_A, e_B)$.

Ορισμός 1. Η ομάδα $A \times B$ με εσωτερικό νόμο που ορίζεται από την ισότητα (1) λέγεται **ευθύ γινόμενο** των A, B .

Αν οι ομάδες A, B είναι πεπερασμένες, τότε $|A \times B| = |A| \cdot |B|$. Αν οι νόμοι των A, B συμβολίζονται προσθετικά, αντί $A \times B$ γράφουμε συνήθως $A \oplus B$ και λέμε ότι $A \oplus B$ είναι **ευθύ άθροισμα** των A, B .

Παραδείγματα.

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι μια ομάδα τάξης 4 με στοιχεία $e = (\bar{0}, \bar{0}), a = (\bar{1}, \bar{0}), \beta = (\bar{0}, \bar{1}), \gamma = (\bar{1}, \bar{1})$ και πίνακα εσωτερικού νόμου

$\cdot$	e	a	β	γ	
e	e	a	β	γ	$a^2 = e$
a	a	e	γ	β	$\beta^2 = e$
β	β	γ	e	a	$a\beta = \gamma$
γ	γ	β	a	e	

δηλαδή $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι η ομάδα Klein.

Παρατήρηση. Η ομάδα $\mathbb{Z}_2$ είναι κυκλική. Το παράδειγμα αποδεικνύει ότι το ευθύ γινόμενο κυκλικών ομάδων δεν είναι πάντοτε κυκλική ομάδα.

2. $\mathbb{Z}_2 \times \mathbb{Z}_3$ είναι μια κυκλική ομάδα τάξης 6.

Πραγματικά, $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (\bar{1}, \bar{1}) \rangle$, γιατί

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{2})\}$$

$$\begin{aligned} (\bar{1}, \bar{1})^2 &= (\bar{0}, \bar{2}) \\ (\bar{1}, \bar{1})^3 &= (\bar{1}, \bar{0}) \\ (\bar{1}, \bar{1})^4 &= (\bar{0}, \bar{1}) \\ (\bar{1}, \bar{1})^5 &= (\bar{1}, \bar{2}) \\ (\bar{1}, \bar{1})^6 &= (\bar{0}, \bar{0}) \end{aligned}$$

και

Πρόταση 1. Αν A, B, Γ είναι τρεις ομάδες,

$$A \times (B \times \Gamma) \cong (A \times B) \times \Gamma$$

Απόδειξη. Ένα οποιοδήποτε στοιχείο της ομάδας $A \times (B \times \Gamma) = G$ είναι της μορφής $a = (a, (\beta, \gamma))$ και της $(A \times B) \times \Gamma = G'$ της μορφής $((a, \beta), \gamma) = a'$. Η συνάρτηση $f : G \rightarrow G'$ με τιμή $f(a) = a'$ είναι ισομορφισμός. Η επαλήθευση είναι απλή. $\square$

Ορισμός 2. Αν $G_1, G_2, \dots, G_n$ είναι n ομάδες, το καρτεσιανό γινόμενο $G = G_1 \times G_2 \times \dots \times G_n$ γίνεται ομάδα ως προς το νόμο

$$(a_1, a_2, \dots, a_n) \cdot (\beta_1, \beta_2, \dots, \beta_n) = (a_1\beta_1, a_2\beta_2, \dots, a_n\beta_n)$$

η οποία λέγεται **ευθύ γινόμενο** των $G_1, G_2, \dots, G_n$. Η μονάδα είναι το στοιχείο $e = (e_1, e_2, \dots, e_n)$, όπου e_i μοναδιαίο της G_i και $(a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$.

Θεώρημα 1. Η ομάδα $G = \mathbb{Z}_m \times \mathbb{Z}_n$ είναι κυκλική τότε και μόνο, όταν οι m, n είναι σχετικά πρώτοι, δηλαδή $(m, n) = 1$.

Απόδειξη. Έστω $0_m, 1_m$ το μηδέν και η μονάδα του $\mathbb{Z}_m$. Προφανώς $(1_m, 1_n)^{mn} = (mn \cdot 1_m, mn \cdot 1_n) = (n \cdot (m \cdot 1_m), m \cdot (n \cdot 1_n)) = (0_m, 0_n) =$ ουδέτερο της G . Αν $(1_m, 1_n)^\lambda = (0_m, 0_n)$, θα έχουμε $(\lambda \cdot 1_m, \lambda \cdot 1_n) = (0_m, 0_n)$, συνεπώς $\lambda \cdot 1_m = 0_m, \lambda \cdot 1_n = 0_n$, άρα $m/\lambda, n/\lambda$ και επειδή οι m, n είναι σχετικά πρώτοι $m/\lambda, n/\lambda$, δηλαδή ο μικρότερος φυσικός για τον οποίο $(1_m, 1_n)^\lambda = 1_G$ είναι ο $mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. Άρα η G είναι κυκλική. $\square$

Αν οι m, n δεν είναι σχετικά πρώτοι, η ομάδα $\mathbb{Z}_m \times \mathbb{Z}_n$ δεν είναι κυκλική.

Π.χ. η $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι ομάδα τάξης 4 και όλα τα στοιχεία της $\neq (1_2, 1_2)$ έχουν τάξη $2 < 4$, ενώ η κυκλική ομάδα τάξης 4 έχει ένα τουλάχιστον στοιχείο τάξης 4. Γενικά, αν $d = (m, n) > 1$, έχουμε $m = m_1d, n = n_1d$ και για κάθε στοιχείο $(h, k) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$(h, k)^{m_1n_1d} = (m_1n_1d \cdot h, m_1n_1d \cdot k) = (0_m, 0_n)$$

δηλαδή η τάξη του είναι $\leq m_1n_1d < mn$

Πόρισμα 1. Αν οι $n_1, n_2, \dots, n_k$ είναι αμέραι ανά δύο σχετικά πρώτοι

$$\mathbb{Z}_{n_1n_2\dots n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$$

Πόρισμα 2 Έστω $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ η ανάλυση του n σε γινόμενο πρώτων παραγόντων $p_1, p_2, \dots, p_m$ διαφόρων ανά δύο. Τότε

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \dots \times \mathbb{Z}_{p_m^{a_m}}$$

Εφαρμογή. Βρείτε τρεις μη ισόμορφες ομάδες τάξης 24.

Η $\mathbb{Z}_{24} = \mathbb{Z}_3 \times \mathbb{Z}_8$ είναι κυκλική τάξης 24, η $G_2 = \mathbb{Z}_4 \times \mathbb{Z}_6$ δεν είναι κυκλική, όπως και η $G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$. Οι ομάδες G_2, G_3 δεν είναι ισόμορφες, γιατί ένας ισομορφισμός $f: G_1 \rightarrow G_2$ απεικονίζει το μηδέν στο μηδέν και το x^m στο $f(x)^m$. Όμως $(1_4, 1_6)^6 = (\bar{2}, \bar{0})$ και για κάθε $(a, \beta, \gamma) \in G_3$, $(a, \beta, \gamma)^6 = (6a, 6\beta, 6\gamma) = (0_2, 0_2, 0_6)$, όπου 0_k το μηδέν του $\mathbb{Z}_k$.

Θεώρημα 2. Έστω $G = G_1 \times G_2 \times \cdots \times G_n$ και $a = (a_1, a_2, \dots, a_n) \in G$. Αν κάθε $a_i \in G_i$ είναι πεπερασμένης τάξης m_i , το a είναι πεπερασμένης τάξης $d = \varepsilon.χ.π. (m_1, m_2, \dots, m_n)$.

Απόδειξη. Για να είναι $a^k = e$, πρέπει $(a_1^k, a_2^k, \dots, a_n^k) = (e_1, e_2, \dots, e_n)$ ή $a_i^k = e_i$ για κάθε $i = 1, 2, \dots, n$. Συνεπώς $m_i/k (i = 1, 2, \dots, n)$. Επειδή η τάξη του a είναι ο μικρότερος θετικός k με $a^k = e$, έπεται το συμπέρασμα. $\square$

Ορισμός 3. Έστω $A_1, A_2, \dots, A_n$ δακτύλιοι. Ευθύ γινόμενο αυτών λέγεται ο δακτύλιος $A_1 \times A_2 \times \cdots \times A_n$ με πράξεις

$$(a_1, a_2, \dots, a_n) + (\beta_1, \beta_2, \dots, \beta_n) = (a_1 + \beta_1, a_2 + \beta_2, \dots, a_n + \beta_n)$$

$$(a_1, a_2, \dots, a_n) \cdot (\beta_1, \beta_2, \dots, \beta_n) = (a_1\beta_1, a_2\beta_2, \dots, a_n\beta_n).$$

2. ΕΣΩΤΕΡΙΚΟ ΕΥΘΥ ΓΙΝΟΜΕΝΟ ΟΜΑΔΩΝ

Έστω $G = A \times B$ το ευθύ γινόμενο των ομάδων A, B με μοναδιαία $1_A, 1_B$. Θα βρούμε δύο κανονικές υποομάδες G_1, G_2 της G ισόμορφες των A αντίστοιχα B τέτοιες, ώστε

$$G = G_1 \cdot G_2, \quad G_1 \cap G_2 = \{1_G\}$$

Το σύνολο $G_1 = A \times \{1_B\}$ είναι υποομάδα της G , γιατί

$$(a, 1_B) \cdot (\beta, 1_B)^{-1} = (a, 1_B) \cdot (\beta^{-1}, 1_B) = (a\beta^{-1}, 1_B) \in G_1$$

Είναι κανονική υποομάδα, γιατί για κάθε $(x, y) \in G$ και κάθε $(a, 1_B) \in G_1$ έχουμε

$$(x, y)^{-1}(a, 1_B)(x, y) = (x^{-1}, y^{-1})(a, 1_B)(x, y) =$$

$$= (x^{-1}ax, y^{-1}1_By) = (x^{-1}ax, 1_B) \in G_1$$

Όμοια το σύνολο $G_2 = \{1_A\} \times B$ είναι κανονική υποομάδα της G . Κάθε στοιχείο (a, β) της G γράφεται:

$$(a, \beta) = (a, 1_B) \cdot (1_A, \beta) \in G_1 \cdot G_2$$

συνεπώς $G = G_1 \cdot G_2$. Αν $(a, 1_B) = (1_A, \beta)$ είναι στοιχείο της τομής $G_1 \cap G_2$, θα έχουμε $a = 1_A$, $1_B = \beta$, δηλαδή το στοιχείο αυτό είναι $(1_A, 1_B) = 1_G$. Οι ομάδες A και G_1 είναι ισόμορφες. Ένας ισομορφισμός είναι προφανώς η συνάρτηση $a \mapsto (a, 1_B)$. Όμοια οι B, G_2 είναι ισόμορφες. Από τις παρατηρήσεις αυτές οδηγούμαστε στον παρακάτω ορισμό.

Ορισμός 1. Μια ομάδα G λέγεται **εσωτερικό ευθύ γινόμενο** ή απλά **ευθύ γινόμενο** των υποομάδων της G_1, G_2 , αν οι G_1, G_2 είναι κανονικές υποομάδες αυτής και

$$G = G_1 \cdot G_2, \quad G_1 \cap G_2 = \{1_G\}.$$

Πρόταση 1. Αν μια ομάδα G είναι ευθύ γινόμενο των κανονικών υποομάδων της A, B , τότε

- (i) $a \cdot \beta = \beta \cdot a$ για όλα τα $a \in A, \beta \in B$,
- (ii) κάθε στοιχείο της G γράφεται κατά ένα μόνο τρόπο σαν γινόμενο $a \cdot \beta$ με $a \in A, \beta \in B$
- (iii) Η συνάρτηση $f: A \times B \rightarrow G$ με $f(a, \beta) = a\beta$ είναι ισομορφισμός.

Απόδειξη.(i) Έστω $[a, \beta] = a\beta a^{-1}\beta^{-1}$. Προφανώς $[a, \beta]\beta a = a\beta$. Συνεπώς αρκεί ν' αποδείξουμε ότι $[a, \beta] = e$. Έχουμε

$$[a, \beta] = (a\beta a^{-1})\beta^{-1} \in B, \quad [a, \beta] = a(\beta a^{-1}\beta^{-1}) \in A$$

γιατί $A, B \trianglelefteq G$. Άρα $[a, \beta] = e$.

- (ii) Αν $a\beta = a_1\beta_1$ με $a, a_1 \in A$ και $\beta, \beta_1 \in B$ έχουμε $a_1^{-1}a = \beta_1\beta^{-1} \in A \cap B$, συνεπώς $a_1^{-1}a = \beta_1\beta^{-1} = e$, δηλαδή $a = a_1, \beta = \beta_1$.
- (iii) Προφανώς $f((a, \beta) \cdot (a', \beta')) = f(aa', \beta\beta') = (aa')(\beta\beta') = aa'\beta\beta' = a(a'\beta)\beta' = a(\beta a')\beta' = a\beta a'\beta' = f(a, \beta) \cdot f(a', \beta')$ δηλαδή η f είναι επιμορφισμός. Ο πυρήνας είναι $\{(a, \beta); f(a, \beta) = 1_G\} = \{(a, \beta); a\beta = 1_G\}$. Επειδή $1_G \cdot 1_G = 1_G$ και κάθε στοιχείο γράφεται σαν γινόμενο στοιχείων των A, B κατά ένα μόνο τρόπο, είναι $a = 1_G, \beta = 1_G$, δηλαδή $(a, \beta) = 1_{A \times B}$. Άρα η f είναι ισομορφισμός. $\square$

Πρόταση 2. Αν η ομάδα G είναι ευθύ γινόμενο των υποομάδων της A, B , τότε $G/A \cong B$.

Απόδειξη. Έστω xA ένα στοιχείο της ομάδας G/A , όπου $x \in G$. Το στοιχείο x θα γράφεται μονοσήμαντα υπό τη μορφή $x = a\beta$ με $(a, \beta) \in A \times B$. Θα έχουμε $a\beta = \beta a$ και $xA = a\beta A = \beta aA = \beta A$. Συνεπώς $G/A = \{\beta A; \beta \in B\}$. Η συνάρτηση $f: G/A \rightarrow B$ με τιμή $f(\beta A) = \beta$ είναι ομομορφισμός, γιατί

$$f(\beta A \cdot \beta' A) = f(\beta\beta' A) = \beta\beta' = f(\beta A)f(\beta' A)$$

Είναι επιπλέον επιμορφισμός και ισομορφισμός, γιατί $\text{Ker } f = \{\beta A : \beta = 1_B\} = \{A\} = 1_{G/A}$. $\square$

Γενίκευση του ορισμού 1:

Ορισμός 2. Έστω G μια ομάδα και $G_1, G_2, \dots, G_n$ υποομάδες της. Λέμε ότι η G είναι ευθύ γινόμενο των υποομάδων της $G_i (i = 1, 2, \dots, n)$ και γράφουμε $G = G_1 \times G_2 \times \dots \times G_n$, αν

- i) Οι υποομάδες G_i είναι κανονικές υποομάδες της $G (i = 1, 2, \dots, n)$
- ii) $G = G_1 G_2 \dots G_n$
- iii) $G_i \cap G_1 G_2 \dots G_{i-1} = \{1\}$, $i = 2, 3, \dots, n$

Θεώρημα 1. Μια ομάδα G είναι ευθύ γινόμενο των υποομάδων της $G_1, G_2, \dots, G_n$ τότε και μόνο, όταν

- 1. Δύο οποιαδήποτε στοιχεία $a_i \in G_i$ και $a_j \in G_j (i \neq j)$ αντιμετατίθενται.
- 2. Κάθε $x \in G$ γράφεται κατά ένα μόνο τρόπο ως γινόμενο $x_1 x_2 \dots x_n$ με $x_i \in G_i$.

Απόδειξη. Έστω ότι η G είναι ευθύ γινόμενο των υποομάδων $G_i (i = 1, 2, \dots, n)$ και ότι $a_i \in G_i, a_j \in G_j$ με $i \neq j$. Ας υποθέσουμε ότι $j < i$. Τότε $G_j \subseteq G_1 G_2 \dots G_j \dots G_{i-1}$ και συνεπώς $G_j \cap G_i \subseteq (G_1 G_2 \dots G_{i-1}) \cap G_i = \{e\}$, δηλαδή $G_j \cap G_i = \{e\}$. Επειδή

$$[a_i, a_j] = a_i a_j a_i^{-1} a_j^{-1} = a_i (\beta_j^{-1} a_i^{-1} \beta_j) \in a_i G_i = G_i, \quad \beta_j = a_j^{-1}$$

$$[a_i, a_j] = a_i a_j a_i^{-1} a_j^{-1} = (a_i a_j a_i^{-1}) a_j^{-1} \in G_j a_j^{-1} = G_j$$

έπεται ότι $[a_i, a_j] = e$, άρα $a_i a_j = a_j a_i$.

Έστω τώρα ότι κάποιο $x \in G$ γράφεται κατά δύο τρόπους σαν γινόμενο στοιχείων των G_i :

$$x = x_1 x_2 \dots x_n = h_1 h_2 \dots h_n \text{ με } x_i, h_i \in G_i \quad (1)$$

$$\begin{aligned} \text{Τότε} \quad x_n h_n^{-1} &= x_{n-1}^{-1} x_{n-2}^{-1} \dots x_1^{-1} h_1 h_2 \dots h_{n-1} && \text{λόγω της ισότητας (1)} \\ &= (x_1^{-1} h_1) \dots (x_{n-1}^{-1} h_{n-1}) \end{aligned}$$

Συνεπώς $x_n h_n^{-1} \in G_n \cap G_1 G_2 \cdots G_{n-1}$, οπότε $x_n h_n^{-1} = 1$ ή $x_n = h_n$. Η (1) γίνεται $x_1 x_2 \cdots x_{n-1} = h_1 h_2 \cdots h_{n-1}$. Συνεχίζοντας με τον ίδιο τρόπο παίρνουμε διαδοχικά $x_{n-1} = h_{n-1}, \dots, x_1 = h_1$.

Αντίστροφα: Η συνθήκη (ii) του ορισμού είναι προφανής, όπως και η (iii), γιατί, αν $x_i \in G_i \cap G_1 G_2 \cdots G_{i-1}$, έχουμε $x_i = x_1 x_2 \cdots x_{i-1}$ ή $x_1 x_2 \cdots x_{i-1} x_i^{-1} = e = e \cdots e \cdot e$, οπότε $x_k = e$ λόγω του μονοσήμαντου της γραφής κάθε στοιχείου υπό μορφή γινομένου στοιχείων των G_i .

Θ' αποδείξουμε τώρα ότι $G_i \trianglelefteq G$. Έστω $a_i \in G_i$ και $x \in G$. Τότε $x = x_1 x_2 \cdots x_n$ με $x_j \in G_j$ και συνεπώς για $i \neq 1$,

$$\begin{aligned} x^{-1} a_i x &= x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1} a_i x_1 x_2 \cdots x_{n-1} x_n \\ &= x_n^{-1} x_{n-1}^{-1} \cdots (x_1^{-1} a_i) x_1 x_2 \cdots x_{n-1} x_n \\ &= x_n^{-1} x_{n-1}^{-1} \cdots (a_i x_1^{-1}) x_1 x_2 \cdots x_{n-1} x_n \\ &= x_n^{-1} x_{n-1}^{-1} \cdots x_2^{-1} a_i x_2 \cdots x_{n-1} x_n \end{aligned}$$

Με την υπόθεση ότι $i \neq 2$, βρίσκουμε με τον ίδιο τρόπο ότι

$$\begin{aligned} x^{-1} a_i x &= x_n^{-1} x_{n-1}^{-1} \cdots x_3^{-1} a_i x_3 \cdots x_{n-1} x_n \\ \text{και γενικά} \quad x^{-1} a_i x &= x_n^{-1} x_{n-1}^{-1} \cdots x_i^{-1} a_i x_i \cdots x_{n-1} x_n \end{aligned}$$

Επειδή $x_i^{-1} a_i x_i = h_i \in G_i$, παίρνουμε τελικά $x^{-1} a_i x = x_i^{-1} a_i x_i \in G_i$, άρα $G_i \trianglelefteq G$. $\square$

Η πρόταση 2 γενικεύεται ως εξής:

Πρόταση 3. Αν η ομάδα G είναι ευθύ γινόμενο των υποομάδων της $G_1, G_2, \dots, G_n$, τότε

$$G/G_i \cong G_1 \times G_2 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

Απόδειξη. Κάθε στοιχείο της ομάδας G/G_i είναι της μορφής xG_i με $x \in G$. Αλλά $x = x_1 x_2 \cdots x_i \cdots x_n$ με $x_j \in G_j (j = 1, 2, \dots, n)$. Συνεπώς $xG_i = (x_1 x_2 \cdots x_i \cdots x_n)G_i = (x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n) x_i G_i$ (αφού $x_k x_i = x_i x_k$ για $i \neq k$) $= (x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n)G_i$. Εύκολα επαληθεύουμε ότι η συνάρτηση $f : G/G_i \rightarrow G_1 \times G_2 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$ με $f(xG_i) = x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n$ είναι ισομορφισμός. $\square$

Ορισμός 3. Μια ομάδα G που δεν αναλύεται σε ευθύ γινόμενο υποομάδων της λέγεται **ανάγωγος**.

Η ύπαρξη ανάγωγων ομάδων προκύπτει από την πρόταση:

Πρόταση 4. Μια κυκλική ομάδα τάξης p^m , όπου p πρώτος, είναι ανάγωγος.

Απόδειξη. Έστω G μια κυκλική ομάδα τάξης p^m και έστω $G = A \times B$, όπου A, B κανονικές υποομάδες της $\neq G, \{1_G\}$. Η τάξη της A διαιρεί την τάξη της G . Συνεπώς $|A| = p^a$ με $0 < a < m$. Όμοια $|B| = p^b$ με $0 < b < m$. Έστω $a \leq b$. Τότε p^a/p^b . Συνεπώς η B έχει μια κυκλική υποομάδα τάξης p^a . Επειδή είναι μοναδική, θα ταυτίζεται με την A . Έτσι $A \subseteq B$ και $A \cap B = A = \{e\}$, πράγμα άτοπο. $\square$

3. ΕΦΑΡΜΟΓΗ : ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΟΜΑΔΩΝ ΤΑΞΗΣ ≤ 7 .

Αν η τάξη μιας ομάδας είναι ένας πρώτος αριθμός p , η ομάδα είναι ισόμορφη της $\mathbb{Z}_p$. Έτσι οι ομάδες τάξης $p = 1, 2, 3, 4, 7$ είναι κυκλικές και ισόμορφες των $\{1\}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7$.

Ομάδες τάξης 4. i) Η κυκλική ομάδα τάξης 4, η $\mathbb{Z}_4$.

ii) Η ομάδα του Klein $\mathbb{Z}_2 \times \mathbb{Z}_2$ (§6, Κεφ.3).

Ομάδες τάξης 6. i) Υπάρχει στοιχείο τάξης 6. Θα είναι η κυκλική ομάδα $\mathbb{Z}_6$.

ii) Δεν υπάρχει στοιχείο τάξης 6. Η τάξη ενός στοιχείου θα είναι τότε 1, 2 ή 3. Θ' αποδείξουμε ότι υπάρχει στοιχείο τάξης 3. Αν υποθέσουμε ότι όλα τα στοιχεία της G έχουν τάξη 2 (ή 1), τότε σύμφωνα με το λήμμα που ακολουθεί θα είχαμε $|G| = 2^n = 6$, πράγμα άτοπο.

Λήμμα 1. Αν σε μια πεπερασμένη ομάδα G κάθε στοιχείο $\neq 1$ έχει τάξη 2, τότε η ομάδα είναι αντιμεταθετική και $|G| = 2^n$.

Πραγματικά, αν $a \in G$ τότε $a^2 = 1, a = a^{-1}$ και συνεπώς

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

δηλαδή η ομάδα G είναι αντιμεταθετική. Θ' αποδείξουμε ότι $|G| = 2^n$ για κάποιο φυσικό n . Κάνουμε επαγωγή ως προς $m = |G|$. Αν $m = 1$, έχουμε $n = 0$. Έστω $|G| = m, a \in G$. Η υποομάδα $K = \{e, a\}$ είναι κανονική. Η ομάδα πηλίκο G/K έχει τάξη $\frac{|G|}{|K|} = \frac{m}{2}$. Συνεπώς $\frac{m}{2} = 2^n$ ή $m = 2^{n+1}$.

Έστω λοιπόν a ένα στοιχείο τάξης 3 στη ζητούμενη ομάδα G . Τότε η ομάδα $\langle a \rangle = \{1, a, a^2\}$ έχει δείκτη 2 στην G . Υπάρχει συνεπώς $\beta \in G, \beta \notin \langle a \rangle$ και τέτοιο, ώστε

$$G = \langle a \rangle \cup \beta \langle a \rangle = \{1, a, a^2, \beta, \beta a, \beta a^2\}$$

$\square$

Λήμμα 2. Αν μια υποομάδα H της G έχει δείκτη 2 στην ομάδα G , θα είναι κανονική υποομάδα αυτής.

Απόδειξη. Αφού $(G : H) = 2$, υπάρχουν δύο κλάσεις ως προς H , μια είναι η H και η άλλη η Hg με $g \notin H$. Έτσι $G = H \cup Hg, g \notin H$. Είναι $gH \cap H = \emptyset$, γιατί διαφορετικά $g \in H$. Είναι ακόμη $G = gH \cup H$, συνεπώς $Hg = gH$. Αν $h \in H$, προφανώς $Hh = H = hH$. Άρα $Hx = xH$ για κάθε $x \in G$ και η H είναι κανονική υποομάδα της G . $\square$

Επανερχόμαστε στο πρόβλημα της ταξινόμησης των ομάδων τάξης 6: Αφού η ομάδα $\langle a \rangle$ έχει δείκτη 2 στην G , θα είναι κανονική υποομάδα αυτής. Το πηλίκο $G/\langle a \rangle$ έχει τάξη 2, συνεπώς είναι κυκλική υποομάδα τάξης 2. Έτσι

$$G/\langle a \rangle = \{\langle a \rangle, \beta \langle a \rangle\}$$

και

$$\beta^n \in \beta^n \langle a \rangle = (\beta \langle a \rangle)^n = \begin{cases} \langle a \rangle ; n = \text{άρτιος} \\ \beta \langle a \rangle ; n = \text{περιττός} \end{cases}$$

Η τάξη συνεπώς του β είναι άρτιος αριθμός και διαιρέτης του 6. Αφού δεν είναι 6, θα είναι 2, δηλαδή $\beta^2 = e$. Παρατηρούμε τώρα ότι $\beta^{-1}a\beta \in \langle a \rangle$, γιατί η $\langle a \rangle$ είναι κανονική υποομάδα. Αν $\beta^{-1}a\beta = a$, θα είχαμε $a\beta = \beta a$ και η ομάδα G θα ήταν αντιμεταθετική. Η τάξη όμως του $a\beta$ θα ήταν τότε ίση με ε.κ.π. $(2, 3) = 6$, πράγμα άτοπο. Συνεπώς $\beta^{-1}a\beta = a^2$ και

$$G = \langle a, \beta \rangle \quad \text{με} \quad a^3 = \beta^2 = e, \quad \beta a \beta = a^2 \quad (1)$$

Ο πίνακας του εσωτερικού νόμου της ομάδας G που παράγεται από δύο στοιχεία a, β συνδεόμενα με τις παραπάνω σχέσεις ορίζεται πλήρως:

$\cdot$	e	a	a^2	β	$a\beta$	$a^2\beta$
a	a	a^2	e	$a\beta$	$a^2\beta$	β
a^2	a^2	e	a	$a^2\beta$	β	$a\beta$
β	β	$a^2\beta$	$a\beta$	e	a^2	a
$a\beta$	$a\beta$	β	βa	a	e	a^2
$a^2\beta$	$a^2\beta$	$a\beta$	β	a^2	a	e

$$\beta a = a^2 \beta^{-1} = a^2 \beta$$

άρα και η ομάδα G ορίζεται πλήρως με τις σχέσεις (1). Μια τέτοια ομάδα είναι η συμμετρική ομάδα S_3 (βλ. Κεφ. 14).

Παρατήρηση. Από το παράδειγμα αυτό της Ταξινόμησης των ομάδων τάξης 6 φαίνεται η δυσκολία του γενικού προβλήματος της ταξινόμησης των ομάδων πεπερασμένης τάξης n . Όπως αναφέραμε στην εισαγωγή, την περασμένη δεκαετία λύθηκε το πρόβλημα της ταξινόμησης των πεπερασμένων απλών ομάδων.

ΑΣΚΗΣΕΙΣ

1. Έστω $\mathbb{R}^*$ η πολλαπλασιαστική ομάδα $\mathbb{R} - \{0\}$, $\mathbb{R}^+$ η ομάδα των θετικών πραγματικών αριθμών και G_n η ομάδα $\{1, -1\}$. Δείξτε ότι $\mathbb{R}^* \cong \mathbb{R}^+ \times G_n$.

2. Γράψτε τον πίνακα του εσωτερικού νόμου $\mathbb{Z}_2 \times \mathbb{Z}_4$.

3. Δείξτε ότι οι ομάδες $\mathbb{Z}_3 \times \mathbb{Z}_3$ και $\mathbb{Z}_9$ δεν είναι ισόμορφες.

4. Η ομάδα $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}_4$ έχει στοιχεία πεπερασμένης τάξης;

5. Ν' αποδείξετε ότι $\mathbb{Z}_4 \times \mathbb{Z}_6 / \langle (0, 2) \rangle$ είναι ομάδα ισόμορφη της $\mathbb{Z}_4 \times \mathbb{Z}_2$.

6. Δείξτε ότι οι ομάδες $\mathbb{Z}_m \times \mathbb{Z}_m$, $\mathbb{Z}_{m^2}$ δεν είναι ισόμορφες ($m > 1$).

7. Βρείτε τις κυκλικές υποομάδες της ομάδας $\mathbb{Z}_4 \times \mathbb{Z}_4$ τάξης 4.

8. Βρείτε με ποιά ομάδα τάξης 4 είναι ισόμορφη η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle (1, 0) \rangle$.

9. Βρείτε τις ομάδες $\mathbb{Z} \times \mathbb{Z} / \langle (0, 1) \rangle$, $\mathbb{Z} \times \mathbb{Z} / \langle (1, 2) \rangle$.

10. Αν $(m, n) = 1$, δείξτε ότι $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

11. Έστω A, B, Γ τρεις αντιμεταθετικές ομάδες. Δείξτε ότι $\Gamma \cong A \times B$ τότε και μόνο, όταν υπάρχουν συναρτήσεις p, q, p', q' με πεδία ορισμού και τιμών καθοριζόμενα από το διάγραμμα

$$\begin{array}{ccc} A & \xrightarrow{q} & \Gamma \\ \xleftarrow{p} & & \xleftarrow{q'} \\ & & B \\ & & \xrightarrow{p'} \end{array}$$

τέτοιες, ώστε

$$pq = 1_A, \quad p'q' = 1_B, \quad p'q = pq' = \theta, \quad qp + q'p' = 1_\Gamma$$

12. Έστω $G = \mathbb{Z} \times \mathbb{Z}$, $m \in \mathbb{N}$ και $G_m = \{x^m; x \in G\}$. Δείξτε ότι G_m είναι κανονική υποομάδα της G και ότι $G/G_m \cong \mathbb{Z}_m \times \mathbb{Z}_m$.

13. Έστω A, B δύο ομάδες και ένας ομομορφισμός $h: A \rightarrow B$. Δείξτε ότι η γραφική παράσταση H του h στην ομάδα $A \times B$ είναι μια υποομάδα της. Αν A, B είναι αβελιανές ομάδες, δείξτε ότι $A \oplus B/H \cong B$.

14. Βρείτε ομάδα G τάξης 10 τέτοια, ώστε να περιέχει μια κανονική υποομάδα K τάξης 2 και το πηλίκο G/K να είναι κυκλική ομάδα. Είναι η G αντιμεταθετική; Είναι κυκλική;

15. Δεχόμεθα ότι κάθε ομάδα τάξης p^2 , όπου $p =$ πρώτος, είναι αντιμεταθετική (ασκ.8, Κεφ.4). Βρείτε τις ομάδες τάξης p^2 .

7 | Ομομορφισμοί δακτυλίων

1. ΟΜΟΜΟΡΦΙΣΜΟΙ, ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ

Έστω δύο δακτύλιοι $(A, +, \cdot)$, $(B, +, \cdot)$ με μηδενικά στοιχεία $0_A, 0_B$.

Ορισμός 1. Μια συνάρτηση $f : A \rightarrow B$ λέγεται **ομομορφισμός** του δακτυλίου A στον δακτύλιο B , αν για όλα τα $a, \beta \in A$

$$f(a + \beta) = f(a) + f(\beta) \quad , \quad f(a \cdot \beta) = f(a) \cdot f(\beta)$$

Πυρήνας του ομομορφισμού f λέγεται το σύνολο

$$\text{Ker } f = \{x \in A; f(x) = 0_B\}$$

Επιμορφισμός λέγεται ένας ομομορφισμός $f : A \rightarrow B$ με $f(A) = B$

Ισομορφισμός του δακτυλίου A επί του δακτυλίου B λέγεται ένας ομομορφισμός του A επί του B , ο οποίος είναι αμφιμονοσήμαντη συνάρτηση.

Ένας ισομορφισμός της προσθετικής ομάδας $(A, +)$ επί της προσθετικής ομάδας $(B, +)$ δεν είναι ισομορφισμός του δακτυλίου $(A, +, \cdot)$ επί του

$(B, +, \cdot)$. Π.χ. η συνάρτηση $f : \mathbb{Z} \rightarrow 2\mathbb{Z}$ με τιμή $f(n) = 2n$ είναι ισομορφισμός της προσθετικής ομάδας $(\mathbb{Z}, +)$ επί της $(2\mathbb{Z}, +)$, όχι όμως του δακτυλίου $(\mathbb{Z}, +, \cdot)$ επί του $(2\mathbb{Z}, +, \cdot)$ γιατί

$$f(m+n) = 2(m+n) = 2m + 2n = f(m) + f(n)$$

$$f(m) = f(n) \Rightarrow 2m = 2n \Rightarrow m = n$$

$$f(m \cdot n) = 2(mn) \text{ και } f(m) \cdot f(n) = 2m \cdot 2n = 4mn \neq f(mn)$$

Θεώρημα 1. Αν I ιδεώδες του δακτυλίου A , η συνάρτηση $p : A \rightarrow A/I$ με τιμή $p(a) = a + I$ είναι επιμορφισμός του δακτυλίου A επί του A/I , ο οποίος λέγεται **κανονικός επιμορφισμός**.

Απόδειξη. Έχουμε

$$f(a + \beta) = (a + \beta) + I = (a + I) + (\beta + I) = f(a) + f(\beta)$$

$$f(a\beta) = a\beta + I = (a + I)(\beta + I) = f(a)f(\beta) \quad \square$$

Θεώρημα 2. Έστω f ένας ομομορφισμός του δακτυλίου A στο δακτύλιο B . Τότε

- i) $f(0_A) = 0_B$
- ii) $f(-a) = -f(a)$
- iii) Αν S υποδακτύλιος του A , $f(S)$ είναι υποδακτύλιος του B
- iv) Αν I ιδεώδες του A , $f(I)$ είναι ιδεώδες του B
- v) Αν T υποδακτύλιος του B , $f^{-1}(T)$ είναι υποδακτύλιος του A
- vi) Αν J ιδεώδες του B , $f^{-1}(J)$ είναι ιδεώδες του A . Συνεπώς $\text{Ker } f = f^{-1}(0)$ είναι ιδεώδες του A . Θα δούμε αργότερα ότι κάθε ιδεώδες είναι πυρήνας ενός ομομορφισμού δακτυλίων.
- vii) Αν ο A είναι μοναδιαίος με μονάδα 1_A και $f(1_A) \neq 0_B$, τότε $f(1_A)$ είναι μονάδα του $f(A)$.

Απόδειξη. Επειδή ο f είναι ομομορφισμός της προσθετικής ομάδας $(A, +)$ στην $(B, +)$, οι ιδιότητες i, ii) είναι προφανείς.

iii) Έστω $x, y \in f(S)$. Τότε $x = f(a), y = f(\beta)$ με $a, \beta \in S$ και $x - y = f(a) - f(\beta) = f(a - \beta) \in f(S)$, συνεπώς $f(S)$ είναι προσθετική υποομάδα της $(B, +)$. Έχουμε επί πλέον $xy = f(a)f(\beta) = f(a\beta) \in f(S)$. Άρα $f(S)$ είναι υποδακτύλιος του B .

iv) Σύμφωνα με την προηγούμενη ιδιότητα $f(I)$ είναι υποδακτύλιος του B . Αν $x \in f(I)$ και $y \in f(A)$, τότε $x = f(a), y = f(\beta)$ με $a \in I$ και $\beta \in A$ οπότε $xy = f(a)f(\beta) = f(a\beta) \in f(IA) \subseteq f(I)$, δηλαδή $f(I)f(A) \subseteq f(I)$ και όμοια $f(A)f(I) \subseteq f(I)$. Άρα $f(I)$ ιδεώδες του $f(A)$.

- v) , vi) Αποδεικνύονται όπως οι iii), vi).
vii) Για όλα τα $a \in A$,

$$f(a) = f(1_A a) = f(1_A) f(a)$$

$$f(a) = f(a 1_A) = f(a) f(1_A) = f(1_A) f(a) ,$$

δηλαδή $f(1_A)$ είναι ουδέτερο για τον πολλαπλασιασμό. Αν $f(1_A) \neq 0_B$, είναι μοναδιαίο του δακτυλίου $f(A)$. $\square$

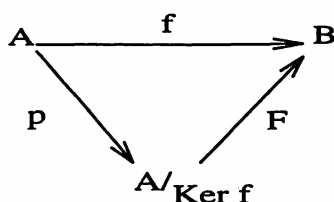
Θεώρημα 3 (Ισομορφισμού δακτυλίων). Έστω f ομομορφισμός του δακτυλίου $(A, +, \cdot)$ στον δακτύλιο $(B, +, \cdot)$ με πυρήνα K . Τότε K είναι ιδεώδες του A και

$$A/\text{Ker } f \cong f(A)$$

Απόδειξη. Επειδή $K = f^{-1}(0_B)$, κατά το προηγούμενο θεώρημα το K είναι ιδεώδες του A . Η συνάρτηση $F : A/\text{Ker } f \rightarrow f(A)$ με τιμή $F(a + K) = f(a)$ είναι καλά ορισμένη και ισομορφισμός της προσθετικής ομάδας του A/K επί της προσθετικής ομάδας του $f(A)$ (βλ. Θεώρ. §2 Κεφ.5). Είναι ισομορφισμός των δακτυλίων, γιατί

$$F((a + K)(\beta + K)) = F(a\beta + K) = f(a\beta) = f(a)f(\beta) = F(a + K)F(\beta + K)$$

Πόρισμα. Αν $f : A \rightarrow B$ είναι ομομορφισμός δακτυλίων, $p : A \rightarrow A/\text{Ker } f$ ο κανονικός επιμορφισμός και F ο ισομορφισμός του $A/\text{Ker } f$ επί του $f(A)$, το παρακάτω διάγραμμα είναι αντιμεταθετικό



$$F \circ p = f.$$

Θεώρημα 4. Έστω I ιδεώδες του A και $p : A \rightarrow A/I$ ο κανονικός επιμορφισμός. Υπάρχει μια συνάρτηση αμφιμονοσήμαντη και γνήσια αύξουσα του συνόλου των ιδεωδών του A/I επί του συνόλου των ιδεωδών του A , που περιέχουν το I . Είναι η συνάρτηση $J \mapsto p^{-1}(J)$.

Απόδειξη. Αν J ιδεώδες του A/I , $p^{-1}(J)$ θα είναι ιδεώδες του A (θεώρ.2). Το ιδεώδες αυτό περιέχει προφανώς το $p^{-1}(0_{A/I}) = \text{Ker } p = I$. Για ν' αποδείξουμε ότι η f είναι αμφιμονοσήμαντη, αρκεί ν' αποδείξουμε ότι αντιστρέφεται ή ότι

$$p \circ f(J) = J , \quad f \circ p(K) = K \text{ με } K \supseteq I , \quad \text{οπότε } f^{-1} = p.$$

Προφανώς $p \circ f(J) = p \circ p^{-1}(J) = J$. Έστω $x \in f \circ p(K) = p^{-1}(p(K))$. Τότε $p(x) = p(y)$ με $y \in K$ ή

$$p(x - y) = 0, \quad x - y \in \text{Ker } p = I, \quad x = (x - y) + y \subseteq I + K = K$$

δηλαδή $f \circ p(K) \subseteq K$. Επειδή και $f \circ p(K) \supseteq K$, έπεται ότι $f \circ p(K) = K$, όταν $K \supseteq I$. Τέλος η f είναι προφανώς γνήσια αύξουσα. $\square$

2. ΧΑΡΑΚΤΗΡΙΣΤΙΚΗ, ΠΡΩΤΑ ΥΠΟΣΩΜΑΤΑ

Έστω A ένας δακτύλιος και $x \in A$. Για κάθε ακέραιο m , το γινόμενο $m \cdot x$ ορίζεται ως εξής:

$$\text{Αν } m > 0, \quad m \cdot x = x + x + \cdots + x \quad (m \text{ φορές})$$

$$\text{Αν } m = 0, \quad m \cdot 0 = 0$$

$$\text{Αν } m < 0, \quad m \cdot x = (-m)(-x) = (-x) + (-x) + \cdots + (-x), \quad (|m| \text{ φορές})$$

Εύκολα επαληθεύουμε ότι για οποιαδήποτε $x, y \in A$ και $m, n \in \mathbb{Z}$ ισχύουν

$$(m + n) \cdot x = m \cdot x + n \cdot x$$

$$m \cdot (x + y) = m \cdot x + m \cdot y$$

$$m \cdot (n \cdot x) = (mn) \cdot x$$

$(mn) \cdot 1 = (m \cdot 1) \cdot (n \cdot 1)$, αν ο A είναι μοναδιαίος με μονάδα 1.

Ορισμός 1. Αν υπάρχει φυσικός m τέτοιος, ώστε $m \cdot x = 0$ για κάθε $x \in A$, θα υπάρχει ο μικρότερος φυσικός p για τον οποίο $p \cdot x = 0$ για κάθε $x \in A$. Ο φυσικός p λέγεται **χαρακτηριστική** του δακτυλίου A και γράφουμε $\text{Char } A = p$. Αν για κάθε φυσικό m είναι $m \cdot x \neq 0$ για ένα τουλάχιστο $x \in A$, ορίζουμε $\text{Char } A = 0$.

Παραδείγματα. $\text{Char } \mathbb{Z} = 0$, $\text{Char } \mathbb{Z}_m = m$.

Πρόταση 1. Η χαρακτηριστική ακεραίας περιοχής K είναι 0 ή πρώτος αριθμός.

Απόδειξη. Έστω ότι η χαρακτηριστική του K είναι $p \neq 0$. Τότε $p \cdot 1 = 0$. Αν ο p δεν ήταν πρώτος, θα είχαμε $p = a \cdot \beta$ με $1 < a < p$ και $1 < \beta < p$, οπότε $(a \cdot \beta) \cdot 1 = 0$ ή $(a \cdot 1) \cdot (\beta \cdot 1) = 0$, δηλαδή $a \cdot 1 = 0$ ή $\beta \cdot 1 = 0$, πράγμα άτοπο. Άρα ο p είναι πρώτος. $\square$

Πρέπει να παρατηρήσουμε ότι η χαρακτηριστική ενός δακτυλίου είναι δυνατόν να είναι πρώτος αριθμός και ο δακτύλιος να μην είναι ακέραια περιοχή.

Παράδειγμα. Ο δακτύλιος $\mathbb{Z}_3 \times \mathbb{Z}_3$ έχει χαρακτηριστική τον πρώτο αριθμό 3, αλλά έχει διαιρέτες του μηδενός. Π.χ. $(\bar{0}, \bar{2}) \cdot (\bar{1}, \bar{0}) = (\bar{0}, \bar{0})$ και ο παράγοντας αριστερά είναι $\neq (\bar{0}, \bar{0})$.

Θεώρημα 1. Έστω A ένας μοναδιαίος δακτύλιος με μονάδα 1. Τότε

- i) Η συνάρτηση $f : \mathbb{Z} \rightarrow A$ με τιμή $f(n) = n \cdot 1$ είναι ομομορφισμός δακτυλίων
- ii) Ο δακτύλιος A περιέχει υποδακτύλιο ισόμορφο με τον $\mathbb{Z}_m$ ή τον $\mathbb{Z}$ καθόσον $\text{Char } A = m$ ή $\text{Char } A = 0$.

Απόδειξη. i) Προφανώς $f(m+n) = (m+n) \cdot 1 = m \cdot 1 + n \cdot 1 = f(m) + f(n)$,
 $f(mn) = (mn) \cdot 1 = (m \cdot 1) \cdot (n \cdot 1) = f(m) \cdot f(n)$.

- ii) Ο πυρήνας του f είναι ιδεώδες του $\mathbb{Z}$. Αλλά κάθε γνήσιο ιδεώδες του $\mathbb{Z}$ είναι της μορφής $m\mathbb{Z}$ για κάποιο φυσικό m και $(0) = 0 \cdot \mathbb{Z}$. Συνεπώς θα έχουμε

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\cong f(\mathbb{Z}), \text{ δηλαδή } \mathbb{Z}_m \cong f(\mathbb{Z}) \\ \text{ή } \mathbb{Z}/(0) &\cong f(\mathbb{Z}), \text{ δηλαδή } \mathbb{Z} \cong f(\mathbb{Z}) \end{aligned}$$

Επειδή $\text{Ker } f = (0)$ τότε και μόνο, όταν $n \cdot 1 \neq 0$ για κάθε $n \neq 0$, έχουμε $\text{Ker } f = (0)$ τότε και μόνο, όταν $\text{Char } A = 0$.

Έστω $\text{Char } A = m$. Τότε $m \cdot 1 = 0, m \in \text{Ker } f, m\mathbb{Z} \subseteq \text{Ker } f$. Αν $n \in \text{Ker } f$, έχουμε $n \cdot 1 = 0$. Διαιρώντας τον n με τον m παίρνουμε $n = am + v$ με $0 \leq v < m$, οπότε $n \cdot 1 = 0$, αν $a \cdot m \cdot 1 + v \cdot 1 = 0$ ή $v \cdot 1 = 0$. Άρα $v = 0$, αφού m είναι ο ελάχιστος φυσικός με $m \cdot 1 = 0$. Δηλαδή $n = m \cdot a \in m\mathbb{Z}$ και $\text{Ker } f = m\mathbb{Z}$. $\square$

Θεώρημα 2. Αν K είναι ένα σώμα χαρακτηριστικής p , περιέχει υπόσωμα ισόμορφο του σώματος $\mathbb{Z}_p$. Αν το K είναι χαρακτηριστικής μηδέν, περιέχει υπόσωμα ισόμορφο του σώματος των ρητών $\mathbb{Q}$.

Απόδειξη. Αν $\text{Char } K = p$, ο δακτύλιος K περιέχει υποδακτύλιο ισόμορφο του $\mathbb{Z}_p$, που είναι σώμα, αφού ο p είναι πρώτος. Αν $\text{Char } K = 0$, το σώμα K περιέχει υποδακτύλιο ισόμορφο του $\mathbb{Z}$, άρα θα περιέχει και τα κλάσματα $\frac{m \cdot 1}{n \cdot 1} (m, n \in \mathbb{Z})$, δηλαδή το σώμα των ρητών $\mathbb{Q}$. $\square$

Ορισμός 2. Τα σώματα $\mathbb{Z}_p$ και $\mathbb{Q}$ λέγονται **πρώτα σώματα**.

Κάθε σώμα θα περιέχει σαν μικρότερο υπόσωμα το $\mathbb{Z}_p$ ή το $\mathbb{Q}$.

Ο λογισμός σ' ένα δακτύλιο χαρακτηριστικής $p \neq 0$ αλλάζει ριζικά. Σχετική είναι η παρακάτω

Πρόταση 2. Αν x, y στοιχεία ακέрайας περιοχής A χαρακτηριστικής $p \neq 0$ και $xy = yx$, τότε $(x + y)^p = x^p + y^p$.

Απόδειξη. Ισχύει ο τύπος του δυωνύμου

$$(x + y)^p = \sum_{k=0}^p \binom{p}{k} x^{p-k} y^k = x^p + \binom{p}{1} x^{p-1} y + \dots + \binom{p}{k} x^{p-k} y^k + \dots + y^p$$

όπου $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Αρκεί ν' αποδείξουμε ότι $p / \binom{p}{k}$. Ο αριθμός $\binom{p}{k} = \frac{p(p-1) \cdots (p-(k-1))}{k!}$ είναι ακέрайος. Οι παράγοντες του παρονομαστή $2, 3, \dots, k$ είναι μικρότεροι του p και συνεπώς δεν διαιρούν τον p , αφού ο p είναι πρώτος. Άρα $p / \binom{p}{k}$ για $1 \leq k \leq p-1$ και $\binom{p}{k} = 0$, οπότε $(x + y)^p = x^p + y^p$. $\square$

Πόρισμα 1. Σ' ένα αντιμεταθετικό δακτύλιο A χωρίς διαιρέτες του μηδενός, χαρακτηριστικής $p \neq 0$, η συνάρτηση $x \mapsto x^p$ είναι ομομορφισμός. Λέγεται ομομορφισμός του **Frobenius**.

Πόρισμα 2. Με τις προϋποθέσεις της πρότασης 2 είναι $(x + y)^{p^n} = x^{p^n} + y^{p^n}$ για $n = 1, 2, \dots$

Θεώρημα 3. Έστω K ένα σώμα με πεπερασμένο πλήθος στοιχείων. Τότε η χαρακτηριστική του K είναι $p \neq 0$ και $|K| = p^n$ για κάποιο φυσικό n .

Απόδειξη. Έστω $|K| = m$. Τα στοιχεία

$$1, 2 \cdot 1, 3 \cdot 1, \dots, n \cdot 1, \dots$$

του K δεν μπορεί να είναι όλα διάφορα, γιατί το K θα ήταν άπειρο. Συνεπώς υπάρχουν $n, n' \in \mathbb{N}$ με $n \cdot 1 = n' \cdot 1$. Αν $n > n'$, θα έχουμε $(n - n') \cdot 1 = 0$, συνεπώς η χαρακτηριστική του K είναι $p \neq 0$. Θεωρούμε το πρώτο υπόσωμα $\mathbb{Z}_p$ του K . Το K είναι ένας διανυσματικός χώρος επί του $\mathbb{Z}_p$. Έστω $x_1, x_2, \dots, x_n$ μια βάση του χώρου αυτού. Κάθε στοιχείο x του K θα είναι της μορφής

$$x = a_1 x_1 + a_2 x_2 + \dots + a_n x_n \quad \text{με } a_i \in \mathbb{Z}_p.$$

Το πλήθος των στοιχείων της μορφής αυτής είναι p^n . $\square$

Ορισμός 3. Ένα πεπερασμένο σώμα με p^n στοιχεία, όπου p η χαρακτηριστική του, συμβολίζεται με $GF(p^n)$ και λέγεται σώμα του **Galois** (Galois Fields).

3. ΔΥΟ ΕΠΕΚΤΑΣΕΙΣ ΔΑΚΤΥΛΙΟΥ

Θα μας απασχολήσουν τα εξής δύο προβλήματα:

Πρώτο πρόβλημα: Ένας δακτύλιος μπορεί να ταυτιστεί με υποδακτύλιο ενός μοναδιαίου δακτυλίου;

Δεύτερο πρόβλημα: Μια ακέραια περιοχή μπορεί να ταυτιστεί με ακέραια περιοχή που περιέχεται σ' ένα σώμα;

Τα δύο αυτά προβλήματα είναι χρήσιμα και μια μερική περίπτωση του δεύτερου προβλήματος είναι η επέκταση των ακεραίων στο σώμα των ρητών αριθμών.

I. Υπάρχουν δακτύλιοι που δεν είναι μοναδιαίοι. Π.χ. τα ακέραια πολλαπλασία ενός φυσικού m , δηλαδή το σύνολο $m\mathbb{Z}$, είναι ως προς την πρόσθεση και τον πολλαπλασιασμό των ακεραίων δακτύλιος. Δεν είναι μοναδιαίος, γιατί για κάθε me και κάθε $ma \in \mathbb{Z}$ έχουμε $(me) \cdot (ma) = m^2 ea \neq ma$, αφού $me \neq 1$. Όμως ο δακτύλιος $m\mathbb{Z}$ περιέχεται στο μοναδιαίο δακτύλιο $\mathbb{Z}$, ταυτίζεται με ένα υποδακτύλιο του μοναδιαίου δακτυλίου $\mathbb{Z}$.

Γενικότερα, αν ένας δακτύλιος A είναι **ισόμορφος** με υποδακτύλιο του δακτυλίου R , λέμε ότι ο R είναι **επέκταση** του A ή ότι ο A **εμφυτεύεται** στον δακτύλιο R . Μια χρήσιμη επέκταση ενός δακτυλίου γίνεται στο παρακάτω θεώρημα.

Θεώρημα 1. Έστω A ένας δακτύλιος και $R = A \times \mathbb{Z}$. Στο R ορίζουμε δύο εσωτερικούς νόμους $+$, $\cdot$ ως εξής:

$$(a, m) + (\beta, n) = (a + \beta, m + n)$$

$$(a, m) \cdot (\beta, n) = (a \cdot \beta + m \cdot \beta + n \cdot a, mn)$$

Το R γίνεται δακτύλιος μοναδιαίος, με μονάδα το $(0, 1)$ και ο δακτύλιος A είναι **ισόμορφος** με τον υποδακτύλιο $A \times \{0\}$. Ένας φυσικός ισομορφισμός είναι η συνάρτηση $a \mapsto (a, 0)$.

Η επαλήθευση των ιδιοτήτων των νόμων ενός δακτυλίου δεν παρουσιάζει δυσκολία. Μηδέν του δακτυλίου είναι το $\theta = (0_A, 0)$. Ότι το $(0, 1)$ είναι μονάδα του R προκύπτει αμέσως:

$$(a, m) \cdot (0, 1) = (a \cdot 0 + m \cdot 0 + 1 \cdot a, m \cdot 1) = (a, m)$$

και όμοια $(0, 1) \cdot (a, m) = (a, m)$. Εύκολα επίσης προκύπτει ότι η f είναι ομομορφισμός του A στον R , αφού

$$f(a + \beta) = (a + \beta, 0) = (a, 0) + (\beta, 0) = f(a) + f(\beta)$$

$$f(a\beta) = (a\beta, 0) = (a, 0) \cdot (\beta, 0) = f(a) \cdot f(\beta)$$

Έτσι $f(A) = \{(a, 0); a \in A\} = A \times \{0\}$ είναι υποδακτύλιος του R . Ο πυρήνας του f είναι $\{(a, 0) = 0\} = \{a; a = 0\} = \{0\}$, άρα είναι ισομορφισμός του A επί του $A \times \{0\}$. $\square$

II. Ο δακτύλιος των ακεραίων $\mathbb{Z}$ είναι ακέραια περιοχή. Περιέχεται στο σώμα των ρητών $\mathbb{Q}$. Κάθε ρητός είναι ένα "κλάσμα" $\frac{a}{\beta}$ με $a, \beta \in \mathbb{Z}, \beta \neq 0$. Ο ακέραιος a ταυτίζεται με το ρητό $\frac{a}{1}$ και έτσι το $\mathbb{Z}$ εμφυτεύεται στο σώμα $\mathbb{Q}$.

Θα ασχοληθούμε με το ανάλογο πρόβλημα για μια οποιαδήποτε ακέραια περιοχή A . Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι έχει μοναδιαίο στοιχείο, γιατί στην αντίθετη περίπτωση θεωρούμε μια επέκταση με μοναδιαίο στοιχείο.

Σώμα κλασμάτων

Θεώρημα 2. Έστω A μια αντιμεταθετική ακέραια περιοχή με μοναδιαίο στοιχείο και $S = A \times A^*$, όπου $A^* = A - \{0\}$. Η σχέση R , που ορίζεται ως εξής $(a, \beta)R(a', \beta') \Leftrightarrow a\beta' = \beta a'$, είναι μια σχέση ισοδυναμίας επί του S . Αν $\frac{a}{\beta}$ είναι η κλάση του (a, β) , το σύνολο πηλίκο S/R γίνεται σώμα ως προς τους εσωτερικούς νόμους

$$\frac{a}{\beta} + \frac{a'}{\beta'} = \frac{a\beta' + \beta a'}{\beta\beta'} \quad , \quad \frac{a}{\beta} \cdot \frac{a'}{\beta'} = \frac{aa'}{\beta\beta'}$$

Ο δακτύλιος A είναι ισόμορφος με τον υποδακτύλιο $A' = \{\frac{a}{1}; a \in A\}$ του S/R . Το σώμα S/R λέγεται **σώμα κλασμάτων** του δακτυλίου A .

Απόδειξη. (1) Η σχέση R είναι σχέση ισοδυναμίας:

- (i) $(a, \beta)R(a, \beta)$, γιατί $a\beta = \beta a$
- (ii) $(a, \beta)R(a', \beta') \Rightarrow (a', \beta')R(a, \beta)$, γιατί έχουμε διαδοχικά $a\beta' = \beta a'$, $\beta a' = a\beta'$, $a'\beta = \beta'a$
- (iii) $(a, \beta)R(a', \beta'), (a', \beta')R(a'', \beta'') \Rightarrow a\beta' = \beta a', a'\beta'' = \beta' a''$
 $\Rightarrow a\beta' a'\beta'' = \beta a' \beta' a''$
 $\Rightarrow a\beta'' = \beta a''$
 $\Rightarrow (a, \beta)R(a'', \beta'')$

(2) Οι εσωτερικοί νόμοι (1) είναι καλά ορισμένοι:

Έστω $\frac{a}{\beta} = \frac{x}{y}$, $\frac{a'}{\beta'} = \frac{x'}{y'}$. Τότε

$$\frac{x}{y} + \frac{x'}{y'} = \frac{xy' + yx'}{yy'} = \frac{a\beta' + \beta a'}{\beta\beta'},$$

γιατί $(xy' + yx')\beta\beta' = xy'\beta\beta' + yx'\beta\beta' = (x\beta)(y'\beta') + (x'\beta')(y\beta)$
 $= (ay)(y'\beta') + (a'y')(y\beta)$
 $= (a\beta' + \beta a')yy'$

συνεπώς $\frac{a}{\beta} + \frac{a'}{\beta'} = \frac{x}{y} + \frac{x'}{y'}$, δηλαδή το άθροισμα είναι ανεξάρτητο από την εκλογή των αντιπροσώπων των κλάσεων. Όμοια και το γινόμενο, αφού $\frac{a}{\beta} = \frac{x}{y}$, $\frac{a'}{\beta'} = \frac{x'}{y'}$ συνεπάγονται $ay = \beta x$ και $a'y' = \beta' x'$, οπότε

$$\frac{aa'}{\beta\beta'} = \frac{xx'}{yy'}$$

γιατί $(aa')(yy') = (ay)(a'y') = (\beta x)(\beta' x') = (\beta\beta')(xx')$

(3) Τα ουδέτερα των νόμων είναι $\frac{0}{1}$, $\frac{1}{1}$, γιατί

$$\frac{a}{\beta} + \frac{0}{1} = \frac{a \cdot 1 + \beta \cdot 0}{\beta \cdot 1} = \frac{a}{\beta} = \frac{0}{1} + \frac{a}{\beta}$$

$$\frac{a}{\beta} \cdot \frac{1}{1} = \frac{a \cdot 1}{\beta \cdot 1} = \frac{a}{\beta} = \frac{1}{1} \cdot \frac{a}{\beta}$$

Το αντίθετο του $\frac{a}{\beta}$ είναι το $\frac{-a}{\beta}$ και το αντίστροφο του $\frac{a}{\beta} (\neq \frac{0}{1})$, δηλαδή $a \neq 0$) είναι το $\frac{\beta}{a}$, αφού $\frac{a}{\beta} \cdot \frac{\beta}{a} = \frac{a\beta}{\beta a} = \frac{1}{1}$ λόγω της αντιμεταθετικότητας του πολλαπλασιασμού. Οι υπόλοιπες ιδιότητες της πρόσθεσης και του πολλαπλασιασμού των κλάσεων, που χαρακτηρίζουν το σώμα, επαληθεύονται εύκολα.

(4) Η συνάρτηση $f: A \rightarrow A'$ με $f(a) = \frac{a}{1}$ είναι ισομορφισμός, γιατί

$$f(a + \beta) = \frac{a + \beta}{1} = \frac{a}{1} + \frac{\beta}{1} = f(a) + f(\beta)$$

$$f(a \cdot \beta) = \frac{a\beta}{1} = \frac{a}{1} \cdot \frac{\beta}{1} = f(a) \cdot f(\beta)$$

$$f(a) = f(\beta) \Rightarrow \frac{a}{1} = \frac{\beta}{1} \Rightarrow a \cdot 1 = \beta \cdot 1 \Rightarrow a = \beta$$

Μοναδικότητα του σώματος των κλασμάτων

Ταυτίζουμε το στοιχείο a του δακτυλίου A με την εικόνα του $f(a) = \frac{a}{1}$. Το στοιχείο $\frac{1}{\beta} (\beta \neq 0)$ είναι αντίστροφο του β , γιατί $\beta \cdot \frac{1}{\beta} = \frac{\beta}{1} \cdot \frac{1}{\beta} = \frac{\beta}{\beta} = \frac{1}{1} = 1$. Έτσι κάθε στοιχείο του S/R γράφεται

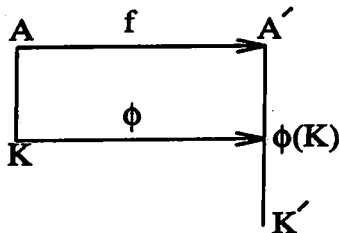
$$\frac{a}{\beta} = \frac{a}{1} \cdot \frac{1}{\beta} = a \cdot \beta^{-1}$$

Επειδή κάθε σώμα, που περιέχει τον δακτύλιο A , θα περιέχει και όλα τα γινόμενα $a \cdot \beta^{-1}$ με $a, \beta \in A$, έπεται ότι το σώμα S/R είναι το ελάχιστο σώμα, το οποίο περιέχει τον δακτύλιο A . Από την άποψη αυτή λέμε ότι το σώμα κλασμάτων του A ορίζεται μονοσήμαντα από τον δακτύλιο A .

Επειδή είναι η πρώτη επέκταση αλγεβρικής δομής, που μας απασχόλησε, θα αναπτύξουμε αυστηρότερα την έννοια της μοναδικότητας της επέκτασης.

Θεώρημα 3. Έστω A, A' δύο ακέραιες περιοχές με μοναδιαία στοιχεία και K, K' τα σώματα κλασμάτων αυτών. Αν οι ακέραιες περιοχές A, A' είναι ισόμορφες, έστω $A \cong A'$, υπάρχει ισομορφισμός ϕ του K μ' ένα υπόσωμα του K' τέτοιος, ώστε $\phi(a) = f(a)$ για κάθε $a \in A$.

Απόδειξη. Στο θεώρημα αντιστοιχίζεται το διάγραμμα



$$K \xrightarrow{\phi} K'$$

$$\frac{a}{\beta} \mapsto \frac{f(a)}{f(\beta)}$$

Ορίζουμε τη συνάρτηση $\phi : K \rightarrow K'$ θέτοντας $\phi\left(\frac{a}{\beta}\right) = \frac{f(a)}{f(\beta)}$. Η συνάρτηση ϕ είναι καλά ορισμένη.

Πραγματικά, αν $\beta \neq 0$, είναι $f(\beta) \neq 0$. Αν $\frac{a}{\beta} = \frac{a'}{\beta'}$ στο σώμα K , έχουμε $a\beta' = \beta a'$, συνεπώς $f(a\beta') = f(\beta a')$ ή $f(a)f(\beta') = f(\beta)f(a')$, δηλαδή $\frac{f(a)}{f(\beta)} = \frac{f(a')}{f(\beta')}$ ή $\phi\left(\frac{a}{\beta}\right) = \phi\left(\frac{a'}{\beta'}\right)$.

Προφανώς $\phi(xy) = \phi(x)\phi(y) \quad \phi(x+y) = \phi(x) + \phi(y)$

για όλα τα $x, y \in K$. Π.χ. είναι, αν $x = \frac{a}{\beta}, y = \frac{a'}{\beta'}$,

$$\phi(xy) = \phi\left(\frac{a}{\beta} \cdot \frac{a'}{\beta'}\right) = \phi\left(\frac{aa'}{\beta\beta'}\right) = \frac{f(aa')}{f(\beta\beta')} = \frac{f(a)f(a')}{f(\beta)f(\beta')} = \phi(x)\phi(y).$$

Τέλος η ϕ είναι αμφιμονοσήμαντη, γιατί, αν $\phi\left(\frac{a}{\beta}\right) = \phi\left(\frac{a'}{\beta'}\right)$, έχουμε $\frac{f(a)}{f(\beta)} = \frac{f(a')}{f(\beta')}$, συνεπώς $f(a)f(\beta') = f(\beta)f(a')$, ή $f(a\beta') = f(\beta a')$, οπότε $a\beta' = \beta a'$ ή $\frac{a}{\beta} = \frac{a'}{\beta'}$, αφού η f είναι ισομορφισμός. Προφανώς για κάθε $a \in A$,

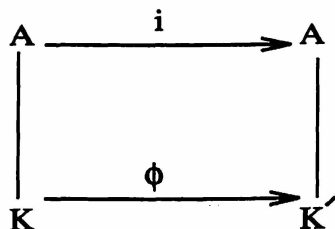
$$\phi(a) = \phi\left(\frac{a}{1}\right) = \frac{f(a)}{f(1)} = f(a)$$

γιατί $f(1)$ είναι η μονάδα του A' . □

Πόρισμα 1. Κάθε σώμα, το οποίο περιέχει μια ακέραια περιοχή, περιέχει το σώμα κλασμάτων αυτής.

Πόρισμα 2. Δύο οποιαδήποτε σώματα κλασμάτων μιας ακέραιας περιοχής A είναι ισόμορφα.

Θεωρούμε το διάγραμμα με $A' = A$ και f την ταυτοτική συνάρτηση i :



$$a \xrightarrow{i} a$$

$$\phi\left(\frac{a}{\beta}\right) = \frac{i(a)}{i(\beta)} = \frac{a}{\beta}$$

Προφανώς $\phi(K) = K'$, άρα $K \stackrel{\phi}{\cong} K'$.

Δακτύλιος κλασμάτων ως προς υπο-ημιομάδα

Έστω A ένας μοναδιαίος και αντιμεταθετικός δακτύλιος και S μια ημιομάδα της ημιομάδας $(A, \cdot)$. Στο σύνολο $A \times S$ ορίζουμε μια σχέση R θέτοντας

$$(a, s)R(a', s') \Leftrightarrow (\exists s_1 \in S) \quad s_1(s'a - sa') = 0$$

Είναι μια σχέση ισοδυναμίας. Η κλάση του (a, s) συμβολίζεται με $\frac{a}{s}$. Αν ο δακτύλιος A είναι ακέραια περιοχή, η σχέση αυτή συμπίπτει με τη σχέση

ισοδυναμίας του θεωρήματος 2. Στο σύνολο πηλίκο $A \times S/R$ ορίζουμε δύο εσωτερικούς νόμους

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} \quad , \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

Αποδεικνύεται ότι οι νόμοι είναι καλά ορισμένοι και ότι το πηλίκο $A \times S/R$ είναι μοναδιαίος και αντιμεταθετικός δακτύλιος B . Αποδεικνύεται ακόμη ότι η συνάρτηση $f_S : A \rightarrow A \times S/R$ με τιμή $f_S(a) = \frac{a}{1}$ είναι ομομορφισμός δακτυλίων και ότι κάθε στοιχείο της εικόνας $f_S(S)$ είναι στο B αντιστρέψιμο $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$.

Παρατήρηση. Αν A είναι αθέριια περιοχή και $S = A$, ο δακτύλιος των κλασμάτων ταυτίζεται με το σώμα των κλασμάτων.

ΑΣΚΗΣΕΙΣ

1. Βρείτε τους ενδομορφισμούς του δακτυλίου $(\mathbb{Z}, +, \cdot)$. Το άθροισμα δύο ενδομορφισμών είναι ενδομορφισμός;

2. Δείξτε ότι $\text{End } \mathbb{Z}_4 = \{1, 0\}$ και $\text{End } \mathbb{Z}_6 = \{1, 0, \bar{x} \mapsto \overline{3x}, \bar{x} \mapsto \overline{4x}\}$.

3. Βρείτε τον ομομορφισμό $h : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2$ με $h(\bar{5}) = \bar{2}$ και τον πυρήνα του.

4. Έστω $\mathbb{R}^*$ η πολλαπλασιαστική ομάδα $\mathbb{R} - \{0\}$ και $V^* = \mathbb{C} - \{0\}$.

1. Δείξτε ότι η συνάρτηση $h : z \mapsto |z|$ είναι ομομορφισμός της ομάδας V^* στην $\mathbb{R}^*$.

2. Βρείτε τον πυρήνα και την εικόνα του h .

3. Βρείτε τα σύνολα $h^{-1}(2), h^{-1}(-2)$.

5. Έστω $\mathbb{Z}[\sqrt{3}]$ το σύνολο των αριθμών $a + \beta\sqrt{3}$ με $a, \beta \in \mathbb{Z}$. Δείξτε ότι

i) $\mathbb{Z}[3]$ είναι υποδακτύλιος του $(\mathbb{Z}, +, \cdot)$.

ii) Κάθε στοιχείο του $\mathbb{Z}[\sqrt{3}]$ γράφεται μονοσήμαντα υπό τη μορφή $a + \beta\sqrt{3}$ με $a, \beta \in \mathbb{Z}$.

iii) Η συνάρτηση $f : a + \beta\sqrt{3} \mapsto a - \beta\sqrt{3}$ είναι αυτομορφισμός του δακτυλίου $\mathbb{Z}[\sqrt{3}]$.

6. Δείξτε ότι η συνάρτηση $\varphi : \mathbb{C} \rightarrow M_2(\mathbb{R})$ με τιμή $\varphi(a + \beta i) = \begin{pmatrix} a & \beta \\ -\beta & a \end{pmatrix}$

είναι ισομορφισμός του δακτυλίου $\mathbb{C}$ στο δακτύλιο $M_2(\mathbb{R})$.

7. Έστω n φυσικός τέτοιος, ώστε $\sqrt{n} \notin \mathbb{Q}$. Το σύνολο $\mathbb{Q}(\sqrt{n}) = \{a + \beta\sqrt{n}; a, \beta \in \mathbb{Q}\}$ είναι σώμα. Βρείτε τους αυτομορφισμούς του σώματος αυτού. Τα σώματα $\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2})$ είναι ισόμορφα;

8 | Ιδεώδη δακτυλίου πράξεις ιδεωδών

1. ΙΔΕΩΔΗ ΠΑΡΑΓΟΜΕΝΑ ΑΠΟ ΥΠΟΣΥΝΟΛΟ

Έστω $(A, +, \cdot)$ ένας δακτύλιος και $(I, +)$ μια υποομάδα της προσθετικής του ομάδας $(A, +)$. Επειδή η ομάδα $(A, +)$ είναι αντιμεταθετική, η I είναι κανονική υποομάδα της $(A, +)$. Συνεπώς το πηλίκο $A/I = \{a + I; a \in A\}$ είναι ομάδα αντιμεταθετική ως προς την πρόσθεση

$$(a + I) + (\beta + I) = (a + \beta) + I$$

Είδαμε στην §2 Κεφ.4 ότι ο νόμος

$$(a + I) \cdot (\beta + I) = a\beta + I$$

είναι εσωτερικός νόμος στο σύνολο A/I τότε και μόνο, όταν

$$AI \subseteq I \quad \text{και} \quad IA \subseteq I \quad (1)$$

Μια προσθετική υποομάδα I της ομάδας $(A, +)$ με τις ιδιότητες (1) την ονομάσαμε *αμφίπλευρο ιδεώδες* του A .

Αριστερό ιδεώδες του A λέγεται μια υποομάδα $(I, +)$ της $(A, +)$, αν

$$AI \subseteq I$$

Συνεπώς το υποσύνολο I του A είναι αριστερό ιδεώδες, αν

$$a - \beta \in I \quad \text{και} \quad x \cdot a \in I$$

για όλα τα $a, \beta \in I$ και $x \in A$.

Δεξιό ιδεώδες του A λέγεται μια υποομάδα $(I, +)$ της $(A, +)$, αν

$$IA \subseteq I$$

Έτσι ένα υποσύνολο I του A είναι δεξιό ιδεώδες, αν για όλα τα $a, \beta \in I$ και $x \in A$ έχουμε

$$a - \beta \in I, \quad ax \in I$$

Πραφανώς I είναι ιδεώδες του A , αν είναι δεξιό και αριστερό ιδεώδες αυτού.

Σε κάθε δακτύλιο A έχουμε δύο τουλάχιστον ιδεώδη, το μηδενικό ιδεώδες $\{0\}$ και τον ίδιο το δακτύλιο A . Κάθε ιδεώδες $\neq \{0\}$, A λέγεται γνήσιο. Αν ένα αριστερό ιδεώδες I περιέχει τη μονάδα ή γενικότερα ένα αντιστρέψιμο στοιχείο a του δακτυλίου A , τότε $I = A$. Γιατί $a^{-1} \cdot a = 1 \in I$ και για κάθε $\beta \in A$ έχουμε $\beta \cdot 1 = \beta \in I$.

Πρόταση 1. Ένας μοναδιαίος αντιμεταθετικός δακτύλιος A είναι σώμα τότε και μόνο, όταν δεν έχει γνήσια ιδεώδη.

Απόδειξη. Έστω ότι ο A είναι σώμα και I ένα ιδεώδες $\neq \{0\}$. Υπάρχει $\beta \in I, \beta \neq 0$. Το β θα είναι αντιστρέψιμο, άρα $I = A$.

Έστω ότι ο μοναδιαίος δακτύλιος A έχει δύο μόνο ιδεώδη. Αν $a \neq 0, a \in A$, το σύνολο Aa είναι ιδεώδες $\neq (0)$, γιατί $a = 1 \cdot a \in Aa$. Συνεπώς πρέπει $Aa = A$. Επειδή $1 \in A$, υπάρχει $a' \in A$ τέτοιο, ώστε $a'a = 1$. Αφού $aa' = a'a = 1$, το a αντιστρέφεται. Έτσι κάθε στοιχείο $a \neq 0$ αντιστρέφεται. $\square$

Πόρισμα. Ένας ομομορφισμός σώματος $K \xrightarrow{f} K$ είναι ο μηδενικός ομομορφισμός ή αυτομορφισμός, γιατί $\text{Ker } f = K$ ή $\{0\}$.

Ιδεώδες παραγόμενο από υποσύνολο S του A

Έστω S ένα υποσύνολο του δακτυλίου A μη κενό. Ο δακτύλιος A είναι ιδεώδες (δεξιό ή αριστερό ή αμφίπλευρο) που περιέχει το S . Έστω

$$(S)_a, \quad (S)_s, \quad (S)$$

η τομή των αριστερών ιδεωδών, αντίστοιχα δεξιών αντίστοιχα αμφίπλευρων που περιέχουν το S . Εύκολα επαληθεύουμε ότι είναι δεξιό, αντίστοιχα αριστερό, αντίστοιχα αμφίπλευρο ιδεώδες, που περιέχει το S . Το ιδεώδες αυτό θα λέγεται ιδεώδες (δεξιό, αριστερό, αμφίπλευρο) παραγόμενο από το S .

Θα επαληθεύσουμε π.χ. ότι $(S)_a$ είναι αριστερό ιδεώδες του A . Έστω $x, y \in (S)_a$ και $z \in A$. Τότε $x - y$ ανήκει σε κάθε αριστερό ιδεώδες I του A που περιέχει το S , οπότε $x - y \in I$, δηλαδή $x - y \in (S)_a$. Επίσης $z \cdot x$ ανήκει σε κάθε αριστερό ιδεώδες I του A , που περιέχει το S , γιατί $x \in I$ και $z \in A$. Συνεπώς $z \cdot x \in (S)_a$. Αν $S = \{a_1, a_2, \dots, a_n\}$, γράφουμε

$$(S)_a = (a_1, a_2, \dots, a_n)_a, (S)_\delta = (a_1, a_2, \dots, a_n)_\delta, (S) = (a_1, a_2, \dots, a_n).$$

Ένα ιδεώδες που παράγεται από ένα στοιχείο, θα λέγεται κύριο ιδεώδες.

Πρόταση 2. Έστω A ένας δακτύλιος και $\beta \in A$. Τότε

$$\text{i) } (\beta)_a = \beta\mathbb{Z} + A\beta$$

$$\text{ii) } (\beta)_\delta = \beta\mathbb{Z} + \beta A$$

Αν ο A είναι μοναδιαίος, τότε

$$(\beta)_a = A\beta \quad \text{και} \quad (\beta)_\delta = \beta A$$

Απόδειξη. i) Επειδή $(\beta)_a$ είναι ομάδα ως προς την πρόσθεση, έχουμε $\beta + \beta + \dots + \beta = \beta n \in \beta\mathbb{Z}$ και $(-\beta) + (-\beta) + \dots + (-\beta) = \beta(-n) \in \beta\mathbb{Z}$, συνεπώς $\beta\mathbb{Z} \subseteq (\beta)_a$. Για κάθε $x \in A$, πρέπει $x \cdot \beta \in (\beta)_a$, δηλαδή $A\beta \subseteq (\beta)_a$. Συνεπώς $\beta\mathbb{Z} + A\beta \subseteq (\beta)_a$. Αλλά $\beta\mathbb{Z} + A\beta$ είναι αριστερό ιδεώδες του A , γιατί είναι υποομάδα της $(A, +)$ και για κάθε $x \in A$ και κάθε $y \in \beta\mathbb{Z} + A\beta$, δηλαδή $y = \beta n + z\beta$ με $n \in \mathbb{Z}$ και $z \in A$, έχουμε

$$\begin{aligned} xy &= x\beta n + xz\beta = (xn)\beta + (xz)\beta \in A\beta + A\beta \\ &= A\beta \subseteq \beta\mathbb{Z} + A\beta \end{aligned}$$

Όμοια αποδεικνύεται ότι $\beta\mathbb{Z} + \beta A$ είναι το δεξιό ιδεώδες, που παράγεται από το β . Αν ο A είναι μοναδιαίος, $\beta\mathbb{Z} \subseteq A\beta$, γιατί $\beta n = \beta + \beta + \dots + \beta = (1 + 1 + \dots + 1)\beta \in A\beta$ και $\beta(-n) = (-\beta)n = (-\beta) + (-\beta) + \dots + (-\beta) = (-1 - 1 - \dots - 1)\beta \in A\beta$. Άρα

$$(\beta)_a = \beta\mathbb{Z} + A\beta \subseteq A\beta + A\beta = A\beta.$$

Όμοια $(\beta)_\delta = \beta A$.

□

Πρόταση 3. Σε κάθε μοναδιαίο δακτύλιο A και για κάθε υποσύνολο S του A έχουμε

$$(S)_a = \{a_1s_1 + a_2s_2 + \cdots + a_ns_n; a_i \in A, s_i \in S, n \in \mathbb{N}\}$$

$$(S)_s = \{s_1a_1 + s_2a_2 + \cdots + s_na_n; a_i \in A, s_i \in S, n \in \mathbb{N}\}$$

Απόδειξη. Είναι απλή και παραλείπεται. $\square$

Πόρισμα. Το αριστερό και δεξιό ιδεώδες που παράγονται από πεπερασμένο πλήθος στοιχείων $\beta_1, \beta_2, \dots, \beta_n$ είναι αντίστοιχα

$$(\beta_1, \beta_2, \dots, \beta_n)_a = A\beta_1 + A\beta_2 + \cdots + A\beta_n$$

$$(\beta_1, \beta_2, \dots, \beta_n)_s = \beta_1A + \beta_2A + \cdots + \beta_nA$$

και λέγονται πεπερασμένου τύπου.

Παράδειγμα 1. Τα στοιχεία 2, 3 του $\mathbb{Z}$ παράγουν το δεξιό ιδεώδες

$$(2, 3)_s = \{2 \cdot n + 3 \cdot m; n, m \in \mathbb{Z}\}$$

το οποίο περιέχει τη μονάδα, αφού υπάρχουν ακέραιοι n, m με $2n + 3m = 1$. Συνεπώς $(2, 3)_s = \mathbb{Z}$.

Παράδειγμα 2. Τα στοιχεία 6, 8 του $\mathbb{Z}$ παράγουν το δεξιό ιδεώδες (θα είναι ιδεώδες)

$$(6, 8)_s = \{6n + 8m; n, m \in \mathbb{Z}\}$$

το οποίο θα είναι της μορφής $\beta\mathbb{Z}$, (βλ. §2, Κεφ.4), όπου β ο ελάχιστος θετικός ακέραιος μέσα στο ιδεώδες. Έχουμε $\beta = 6n + 8m$ τότε και μόνο, όταν $2/\beta$ και $\frac{\beta}{2} = 3n + 4m$. Αν $2/\beta$, η δεύτερη ισότητα ισχύει, γιατί $1 = 3n_0 + 4m_0$ και $\frac{\beta}{2} = 3(n_0\frac{\beta}{2}) + 4(m_0\frac{\beta}{2})$. Άρα $(6, 8)_s = 2\mathbb{Z}$.

Παράδειγμα 3. Γενικά $(a, \beta)_s = d\mathbb{Z}$, όπου d ο μ.κ.δ. των a, β . Υπάρχουν ακέραιοι m, n τέτοιοι, ώστε $d = ma + n\beta$. Συνεπώς $d\mathbb{Z} \subseteq (a, \beta)_s = \{\lambda a + \mu \beta; \lambda, \mu \in \mathbb{Z}\}$. Επειδή $(a, \beta)_s = d'\mathbb{Z}$, θα πρέπει $d\mathbb{Z} \subseteq d'\mathbb{Z}$ ή d'/d . Αφού $a, \beta \in d'\mathbb{Z}$, πρέπει $d'/a, d'/\beta$. Άρα d/d' , οπότε $d = d'$.

2. ΠΡΑΞΕΙΣ ΜΕ ΙΔΕΩΔΗ

Ορισμός 1. Έστω I, J δύο δεξιά (αριστερά ή αμφίπλευρα) ιδεώδη του δακτυλίου A . Το άθροισμα τους, θεωρούμενα ως υποσύνολα του A , είναι

$$I + J = \{a + \beta; a \in I, \beta \in J\}$$

Εύκολα επαληθεύουμε ότι είναι ένα δεξιό ιδεώδες του A (αριστερό ή αμφίπλευρο), το οποίο λέγεται **άθροισμα** των ιδεωδών I, J .

Πραγματικά, αν $x = a + \beta \in I + J$, $x' = a' + \beta' \in I + J$, έχουμε $x - x' = (a - a') + (\beta - \beta') \in I + J$ και για κάθε $y \in A$, $xy = (a + \beta)y = ay + \beta y \in I + J$.

Παράδειγμα 1. Έστω $I = 4\mathbb{Z}, J = 6\mathbb{Z}$ δύο ιδεώδη του $\mathbb{Z}$. Έχουμε $I + J = \{4a + 6\beta; a, \beta \in \mathbb{Z}\} = 2\mathbb{Z}$, γιατί $4a + 6\beta = 2(2a + 3\beta) \in 2\mathbb{Z}$, δηλαδή $I + J \subseteq 2\mathbb{Z}$ και $2 = 6 - 4 \in I + J$, οπότε $2\mathbb{Z} \subseteq I + J$.

Ορισμός 2. Έστω I, J δύο δεξιά (αριστερά ή αμφίπλευρα) ιδεώδη ενός δακτυλίου A . Το γινόμενο των I, J ως υποσύνολο του A , είναι $IJ = \{a\beta; a \in I, \beta \in J\}$. Το υποσύνολο αυτό του A δεν είναι πάντοτε ιδεώδες αυτού. Γι' αυτό ορίζουμε σαν **γινόμενο** $I \cdot J$ των I, J το δεξιό (αριστερό ή αμφίπλευρο) ιδεώδες, που παράγεται από το συνολοθεωρητικό τους γινόμενο IJ . Έχουμε

$$I \cdot J = (IJ)_\delta = \{x \in A; x = a_1\beta_1 + a_2\beta_2 + \dots + a_n\beta_n, n \in \mathbb{N}, a_i \in I, \beta_j \in J\}.$$

Απόδειξη. Εύκολα επαληθεύεται ότι $I \cdot J$ είναι δεξιό ιδεώδες του A : Αν $x' = a'_1\beta'_1 + a'_2\beta'_2 + \dots + a'_m\beta'_m$ με $a'_i \in I, \beta'_j \in J$, έχουμε

$$x - x' = a_1\beta_1 + a_2\beta_2 + \dots + a_n\beta_n + (-a'_1)\beta'_1 + (-a'_2)\beta'_2 + \dots + (-a'_m)\beta'_m \in I \cdot J$$

και για κάθε $a \in A$,

$$xa = (a_1\beta_1 + a_2\beta_2 + \dots + a_n\beta_n)a = a_1(\beta_1a) + \dots + a_n(\beta_na) \in I \cdot J,$$

γιατί $\beta_ja \in J$. Προφανώς το συνολοθεωρητικό γινόμενο $I \cdot J = \{a\beta; a \in I, \beta \in J\} \subseteq I \cdot J$ και συνεπώς $(IJ)_\delta \subseteq I \cdot J$. Αλλά και $I \cdot J \subseteq (IJ)_\delta$, γιατί το άθροισμα $a_1\beta_1 + \dots + a_n\beta_n \in (IJ)_\delta$, όταν $a_i \in I$ και $\beta_j \in J$. Άρα $I \cdot J = (IJ)_\delta$. $\square$

Παράδειγμα 2. Έστω $A = \mathbb{Z}[\omega]$ ο υποδακτύλιος του $\mathbb{R}$ με στοιχεία $a + \beta\omega$, όπου $a, \beta \in \mathbb{Z}$ και $\omega^2 = 10$. Ο A είναι αντιμεταθετικός.

i) Έστω $I = (2, \omega) = 2A + \omega A$. Έχουμε $I^2 = 2A$.

Πραγματικά, κάθε στοιχείο του I έχει τη μορφή $2a + \omega\beta$ με $a, \beta \in A$. Συνεπώς το γινόμενο δύο στοιχείων του I είναι

$$\begin{aligned} (2a + \omega\beta)(2a' + \omega\beta') &= 4aa' + 2\omega\beta a' + 2\omega a\beta' + \omega^2\beta\beta' \\ &\in 4A + 2\omega A + 2\omega A + 10A \\ &\subseteq 2A + 2A + 2A + 2A \\ &= 2A \end{aligned}$$

άρα $I^2 \subseteq 2A$. Επειδή $2 = 10 - 2 \cdot 4 = \omega^2 - 2m \in I^2$, έχουμε $I^2 = 2A$.

ii) Έστω $I = (3, 4 + \omega)$, $J = (3, 4 - \omega)$. Τότε $I \cdot J = 3A$.

Πραγματικά, κάθε στοιχείο του I είναι της μορφής $3a + (4 + \omega)\beta$ και του J της μορφής $3a' + (4 - \omega)\beta'$. Το γινόμενο τους είναι

$$(3a + (4 + \omega)\beta)(3a' + (4 - \omega)\beta') = 9aa' + 3(4 + \omega)a'\beta + 3(4 - \omega)a\beta' + (16 - \omega^2)\beta\beta' \in 3A + 3A + 6A \subseteq 3A$$

συνεπώς $I \cdot J \subseteq 3A$. Επειδή $3 \in I \cdot J$, έπεται ότι $I \cdot J = 3A$.

Οι παρακάτω ιδιότητες του αθροίσματος και του γινομένου ιδεωδών προτείνονται σαν ασκήσεις :

$$I + J = J + I$$

$$I + (J + K) = (I + J) + K$$

$$I \cdot J = J \cdot I$$

$$I \cdot (J \cdot K) = (I \cdot J) \cdot K$$

$$I \cdot (J + K) = I \cdot J + I \cdot K$$

$$I \cdot J \subseteq I \cap J. \text{ Αν } I + J = A, \text{ ισχύει η ισότητα.}$$

$$(a) \cdot (\beta) = (a\beta)$$

$$(a) + (\beta) \neq (a + \beta). \text{ Π.χ. στο } \mathbb{Z}, (a) + (\beta) = (\mu.κ.δ.(a, \beta))$$

3. ΜΕΓΙΣΤΑ ΙΔΕΩΔΗ

Ορισμός 1. Ένα ιδεώδες I του δακτυλίου A λέγεται **μέγιστο** (maximal), αν $I \neq A$ και δεν υπάρχει ιδεώδες J τέτοιο, ώστε $I \subset J$.

Παράδειγμα 1. Το ιδεώδες $I = m\mathbb{Z}$ του $\mathbb{Z}$ είναι μέγιστο τότε και μόνο, όταν ο m είναι πρώτος αριθμός.

Πραγματικά, $m\mathbb{Z} \subseteq a\mathbb{Z}$ τότε και μόνο, όταν $m = a\beta$ με $\beta \in \mathbb{Z}$. Αν ο m είναι πρώτος και $m\mathbb{Z} \subset a\mathbb{Z}$, θα πρέπει $a = 1$ ή $a\mathbb{Z} = \mathbb{Z}$. Άρα το $m\mathbb{Z}$ θα είναι μέγιστο ιδεώδες. Αν ο m δεν είναι πρώτος, τότε $m = a\beta$ με $a \neq 1, m$ και συνεπώς $m\mathbb{Z} \subset a\mathbb{Z} \subset \mathbb{Z}$, δηλαδή το $m\mathbb{Z}$ δεν είναι μέγιστο ιδεώδες.

Παρατηρούμε ότι το πηλίκο $\mathbb{Z}/p\mathbb{Z}$, όπου p πρώτος αριθμός ή $p\mathbb{Z}$ μέγιστο ιδεώδες του $\mathbb{Z}$, είναι σώμα, το σώμα $\mathbb{Z}_p$. Αυτό όμως δεν ισχύει πάντοτε, όπως αποδεικνύεται με το επόμενο

Παράδειγμα 2. Έστω η προσθετική ομάδα των ακεραίων $(\mathbb{Z}, +)$. Ορίζουμε τον πολλαπλασιασμό $*$ θέτοντας $a * \beta = 0$. Τότε $(\mathbb{Z}, +, *)$ είναι δακτύλιος. Το σύνολο $I = 3\mathbb{Z}$ είναι ιδεώδες μέγιστο.

Πραγματικά, κάθε ιδεώδες J του $(\mathbb{Z}, +, *)$ είναι υποομάδα της $(\mathbb{Z}, +)$, συνεπώς $J = m\mathbb{Z}$ (βλ. §2, Κεφ. 4). Έτσι $3\mathbb{Z} \subset J$ τότε και μόνο, όταν $m/3$ ή $m = 1$, δηλαδή $J = \mathbb{Z}$.

Το πηλίκο $\mathbb{Z}/3\mathbb{Z}$ είναι ο δακτύλιος $(\mathbb{Z}_3, +, *)$, ο οποίος δεν είναι σώμα. Είναι μηδενικός δακτύλιος, δηλαδή $ab = 0$, με τάξη $|\mathbb{Z}_3| = 3$ πρώτο αριθμό.

Θεώρημα 1. Έστω A ένας μοναδιαίος και αντιμεταθετικός δακτύλιος. Ένα ιδεώδες I αυτού είναι μέγιστο τότε και μόνο, όταν το πηλίκο A/I είναι σώμα.

Απόδειξη. Έστω ότι το I είναι μέγιστο ιδεώδες του A . Θ' αποδείξουμε ότι για κάθε $a \notin I$, το $a+I$ έχει αντίστροφο στο A/I . Το Aa είναι ιδεώδες $\neq (0)$ του A . Το άθροισμα $Aa+I$ είναι επίσης ιδεώδες, που περιέχει το I . Αφού το I είναι μέγιστο ιδεώδες, $Aa+I = A$. Επειδή $1 \in A$, υπάρχουν $x \in A$ και $z \in I$ τέτοια, ώστε $xa + z = 1$. Τότε $(x+I)(a+I) = xa+I = (1-z)+I = 1+I$, δηλαδή $x+I$ είναι αντίστροφο του $a+I$.

Ας υποθέσουμε τώρα ότι το πηλίκο A/I είναι σώμα και ότι J είναι ένα ιδεώδες του A με $I \subset J$. Θεωρούμε ένα $x \in J - I$ και $y \in A$. Υπάρχει $z \in A$, τέτοιο, ώστε $(x+I)(z+I) = y+I$ ή $xz+I = y+I$ ή $y \in x \cdot z + I \subseteq JA + I \subseteq J + I \subseteq J$. Δηλαδή $A \subseteq J$ και $J = A$. $\square$

Εφαρμογή 1. Βάσει του θεωρήματος βρίσκουμε εύκολα τα μέγιστα ιδεώδη του δακτυλίου $\mathbb{Z}$. Κάθε ιδεώδες είναι της μορφής $m\mathbb{Z}$. Το πηλίκο $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ είναι σώμα τότε και μόνο, όταν ο m είναι πρώτος. Άρα το $m\mathbb{Z}$ είναι μέγιστο τότε και μόνο, όταν ο m είναι πρώτος.

Εφαρμογή 2. Έστω $A = \mathbb{Q}^{\mathbb{N}}$ ο δακτύλιος των ακολουθιών Cauchy των ρητών αριθμών. Το σύνολο των μηδενικών ακολουθιών M του A (μηδενικές ως προς τη συνήθη απόλυτη τιμή του $\mathbb{Q}$) είναι ένα ιδεώδες του A . Είναι μέγιστο γιατί, αν $(a_n) \in J - I$ τότε $a_n \rightarrow a \neq 0$, $\frac{1}{a_n} \rightarrow \frac{1}{a} \neq 0$ και συνεπώς $(a_n) \cdot \left(\frac{1}{a_n}\right) = (1) \in J$, οπότε $J = A$. Το πηλίκο $\mathbb{Q}^{\mathbb{N}}/M$ είναι το σώμα των πραγματικών αριθμών $\mathbb{R}$.

4. ΠΡΩΤΑ ΙΔΕΩΔΗ

Ένα ιδεώδες P του δακτυλίου A λέγεται πρώτο ιδεώδες, αν

- (i) $P \neq A$
- (ii) $xy \in P, x \notin P \Rightarrow y \in P$.

Π.χ. τα πρώτα ιδεώδη του $\mathbb{Z}$ είναι

- (α) το ιδεώδες (0) , γιατί $xy \in (0), x \notin (0)$ ισοδυναμούν με $xy = 0, x \neq 0$, οπότε $y = 0$ ή $y \in (0)$.
- (β) Τα ιδεώδη $m\mathbb{Z}$ με m πρώτο. Πραγματικά, αν ο m είναι πρώτος, τότε $xy \in m\mathbb{Z}, x \notin m\mathbb{Z}$ ισοδυναμούν με m/xy και $m \nmid x$, οπότε m/y , δηλαδή $y \in m\mathbb{Z}$ και το $m\mathbb{Z}$ είναι πρώτο ιδεώδες. Αν ο m δεν είναι πρώτος, τότε $m = a\beta$ με $a \neq 1, m$ και $a\beta \in m\mathbb{Z}, a \notin m\mathbb{Z}, \beta \notin m\mathbb{Z}$.

Θεώρημα 1. Το ιδεώδες P του δακτυλίου A είναι πρώτο τότε και μόνο, όταν ο δακτύλιος A/P είναι ακέραιο περιοχή.

Απόδειξη. Έστω $x, y \in A$. Έχουμε τις ισοδύναμες προτάσεις:

- Ο δακτύλιος A/P είναι ακέραιο περιοχή
- $(x + P)(y + P) = 0_{A/P}, x + P \neq 0_{A/P} \Rightarrow y + P = 0_{A/P}$
- $xy + P = P, x + P \neq P \Rightarrow y + P = P$
- $xy \in P, x \notin P \Rightarrow y \in P$
- Το ιδεώδες P είναι πρώτο.

Πόρισμα. Κάθε μέγιστο ιδεώδες I του A είναι πρώτο.

Γιατί το πηλίκο A/I είναι σώμα, άρα ακέραιο περιοχή.

ΑΣΚΗΣΕΙΣ

1. Δείξτε ότι το $I = \{0, 2, 4\}$ είναι ιδεώδες του $\mathbb{Z}_6$ και βρείτε το δακτύλιο πηλίκο $\mathbb{Z}_6/I$.

2. Έστω $I = \{\bar{0}, \bar{3}\} \subseteq \mathbb{Z}_6$. Δείξτε ότι το I είναι ιδεώδες του δακτυλίου $\mathbb{Z}_6$ και βρείτε το δακτύλιο πηλίκο $\mathbb{Z}_6/I$. Γράψτε τους πίνακες των πράξεων.

3. Βρείτε τα ιδεώδη του δακτυλίου $\mathbb{Z}_{12}$.

4. Δείξτε ότι $(\bar{a}) = (\bar{\beta})$ στο $\mathbb{Z}_m$ τότε και μόνο, όταν $(a, m) = (\beta, m)$.

5. Έστω K ένα σώμα και $M_2(K)$ ο δακτύλιος των πινάκων 2×2 με στοιχεία από το K . Δείξτε ότι το σύνολο των πινάκων $\begin{pmatrix} a & \beta \\ 0 & 0 \end{pmatrix} \in M_2(K)$ είναι δεξιό ιδεώδες του $M_2(K)$ όχι όμως ιδεώδες αυτού.

6. Έστω A ένας δακτύλιος και $X \subseteq A$. Έστω $N(X) = \{a \in A; (\forall x \in X) ax = 0\}$. Δείξτε ότι $N(X)$ είναι αριστερό ιδεώδες του A . Αν το X είναι αριστερό ιδεώδες του A , δείξτε ότι το $N(X)$ είναι αμφίπλευρο ιδεώδες του A .

7. Έστω A ο δακτύλιος των πινάκων 2×2 με στοιχεία ακεραίου αριθμούς. Βρείτε το ιδεώδες που παράγεται από τον πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

8. Έστω $(A, +, \cdot)$ ένας δακτύλιος. Ένα στοιχείο $a \in A$ λέγεται μηδενοδύναμο, αν $a^n = 0$ για κάποιο φυσικό n .

- Αν ο A είναι μοναδιαίος με μονάδα το 1 και το στοιχείο a μηδενοδύναμο, το $1 - a$ αντιστρέφεται.
- Αν a, β είναι μηδενοδύναμα και αντιμετατίθενται, τα στοιχεία $a\beta, a + \beta$ είναι μηδενοδύναμα.
- Αν $n \geq 3$, βρείτε την ικανή και αναγκαία συνθήκη ώστε κάθε στοιχείο του δακτυλίου $\mathbb{Z}_n$ που είναι διαιρέτης του μηδενός να είναι μηδενοδύναμο.

9. Έστω A ένας μοναδιαίος δακτύλιος. Δείξτε ότι, αν ο δακτύλιος A έχει δύο μόνο ιδεώδη, είναι σώμα. Δείξτε την ίδια πρόταση, υποθέτοντας ότι $A^2 \neq (0)$ αντί να υποθέσετε ότι ο A είναι μοναδιαίος δακτύλιος.

10. Δείξτε ότι η προσθετική ομάδα $(\mathbb{Q}, +)/(\mathbb{Z}, +)$ δεν δέχεται δομή δακτυλίου.

11. Έστω p ένας πρώτος αριθμός. Δείξτε ότι τα μόνα ιδεώδη του δακτυλίου $\mathbb{Z}$ που περιέχουν το ιδεώδες $p^n \mathbb{Z}$ είναι της μορφής $p^k \mathbb{Z}$ ($1 \leq k \leq n$). Βάσει αυτού βρείτε τα ιδεώδη του δακτυλίου πηλίκου $\mathbb{Z}^n/p\mathbb{Z}$.

12. Έστω R ένας δακτύλιος και A υποδακτύλιος αυτού. Αν I ιδεώδες του R , δείξτε ότι

- $A + I$ είναι υποδακτύλιος του R
- I ιδεώδες του $A + I$.

13. Αν I, J ιδεώδη του δακτυλίου $\mathbb{Z}$ δείξτε ότι $(I + J) \cdot (I \cap J) = I \cdot J$.

14. Αν I, J, K ιδεώδη ακεραίας περιοχής, δείξτε ότι

$$(I + J + K)(IJ + JK + KI) = (I + J)(J + K)(K + I)$$

15. Έστω p ένας πρώτος αριθμός. Κάθε ρητός $x \neq 0$ γράφεται κατά ένα τρόπο υπό τη μορφή $x = p^a \frac{m}{n}$ με m, n ακεραίους $\neq 0$ και μη διαιρετούς με p . Ορίζουμε $|x|_p = p^{-a}$, $|0|_p = 0$, $A_p = \{x \in \mathbb{Q}; |x|_p \leq 1\}$ και $I = \{x \in \mathbb{Q}; |x|_p < 1\}$. Ν' αποδειχτεί ότι

i) $|xy|_p = |x|_p |y|_p$, $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

ii) A_p είναι δακτύλιος.

iii) I είναι ιδεώδες του A_p .

iv) I είναι το μοναδικό maximal ιδεώδες του A_p .

Σημείωση: Η συνάρτηση $x \mapsto |x|_p$ λέγεται p -αδίκη διατίμηση και το σώμα $A_p/I = K_p$ p -αδίκη επέκταση του συνόλου των ρητών.

16. Έστω $K(\mathbb{Q})$ το σύνολο των πινάκων 2×2 με στοιχεία ρητούς αριθμούς, οι οποίοι αντιμετατίθενται με τον πίνακα $\begin{pmatrix} 0 & -2 \\ 1 & 1 \end{pmatrix}$. Δείξτε ότι είναι σώμα αντιμεταθετικό.

Έστω A το σύνολο των πινάκων του $K(\mathbb{Q})$ με στοιχεία ακεραίους αριθμούς. Δείξτε ότι το A είναι δακτύλιος και ότι $3A$ είναι ιδεώδες maximal αυτού.

17. Έστω A ένας δακτύλιος στον οποίο $x^3 = x$ για κάθε $x \in A$. Ν' αποδειχτεί ότι ο A είναι αντιμεταθετικός. Προς τούτο:

1) Δείξτε ότι $6A = \{0\}$, αφού υπολογίσετε το $(x + y)^3$. Στη συνέχεια δείξτε ότι $2A, 3A$ είναι ιδεώδη αμφίπλευρα τέτοια, ώστε $2A + 3A = A$ και $2A \cap 3A = \{0\}$.

2) Δείξτε ότι στο δακτύλιο πηλίκου $C = A/2A$ έχουμε $u^3 = u$ για κάθε $u \in C$ και $2C = \{0\}$.

3) Στον C δείξτε ότι $u^2 = u$ και ότι ο C είναι αντιμεταθετικός.

4) Δείξτε ότι στο δακτύλιο $B = A/3A$ έχουμε $s^3 = s$ για κάθε $s \in B$ και ότι $3B = \{0\}$.

5) Υπολογίστε για $s, t \in B$ τα $(s + t)^3, (s - t)^3$ και βρείτε ότι $s^2t + sts + ts^2 = 0$. Να συμπεράνετε ότι ο B είναι αντιμεταθετικός.

6) Δείξτε τώρα ότι ο A είναι αντιμεταθετικός.

9 | Δακτύλιοι πολυωνύμων

1. ΟΡΙΣΜΟΣ ΔΑΚΤΥΛΙΟΥ ΠΟΛΥΩΝΥΜΩΝ

Το πρόβλημα που θα μας απασχολήσει είναι η κατασκευή ενός δακτυλίου από ένα μοναδιαίο δακτύλιο A και ένα στοιχείο s ενός συνόλου, ο οποίος

να είναι ο ελάχιστος μοναδιαίος
δακτύλιος, που περιέχει το s και
ένα υποδακτύλιο ισόμορφο του A

Είναι προφανές ότι ένας τέτοιος δακτύλιος θα περιέχει τις δυνάμεις του s :

$$s^0 = 1, s, s^2, \dots, s^n, \dots$$

καθώς και εκφράσεις (στοιχεία) της μορφής

$$a_0 + a_1s + a_2s^2 + \dots + a_ns^n \tag{1}$$

όπου $a_i \in A$. Είναι φυσικό οι εκφράσεις (1) να ταυτίζονται με τις εκφράσεις

$$a_0 + a_1s + a_2s^2 + \dots + a_ns^n + 0 \cdot s^{n+1} + \dots \tag{2}$$

Η έκφραση (2) καθορίζεται από την ακολουθία

$$(a_0, a_1, a_2, \dots, a_n, 0, \dots) \quad (3)$$

στοιχείων του A . Έστω $A^{(N)}$ το σύνολο των ακολουθιών στοιχείων του A των οποίων όλοι οι όροι $a_k = 0$ εκτός από ένα πεπερασμένο πλήθος.

Αν A και s περιέχονται σ' ένα δακτύλιο B και το στοιχείο s αντιμετατίθεται με όλα τα στοιχεία του A , τα στοιχεία (1) αποτελούν υποδακτύλιο του B . Έστω $A[s]$ ο δακτύλιος με στοιχεία της μορφής (1). Λέμε ότι ο δακτύλιος $A[s]$ είναι απλή επέκταση του A με την προσθήκη ενός στοιχείου s . Π.χ. ο $\mathbb{C} = \mathbb{R}[i]$ είναι απλή επέκταση του δακτυλίου $\mathbb{R}$ με την προσθήκη του στοιχείου $s = i$.

Έστω ότι το s αντιμετατίθεται με κάθε στοιχείο του A . Τότε $A[s]$ είναι δακτύλιος. Η συνάρτηση $\phi: A^{(N)} \rightarrow A[s]$ με τιμή

$$(a_0, a_1, a_2, \dots, a_n, 0, \dots) \mapsto a_0 + a_1 s + a_2 s^2 + \dots + a_n s^n$$

είναι επί. Θα ορίσουμε στο σύνολο $A^{(N)}$ δύο εσωτερικούς νόμους, ώστε να γίνει δακτύλιος και η συνάρτηση ϕ να είναι ομομορφισμός δακτυλίων.

Κατασκευή του δακτυλίου $A^{(N)}$

Έστω λοιπόν $A^{(N)}$ το σύνολο των ακολουθιών

$$a = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$$

με $a_i \in A$. Ορίζουμε το άθροισμα $a + \beta$ και το γινόμενο $a \cdot \beta$ δύο στοιχείων του $A^{(N)}$ ως εξής:

$$\begin{aligned} a + \beta &= (a_0 + \beta_0, a_1 + \beta_1, a_2 + \beta_2, \dots, a_n + \beta_n, \dots) \\ a \cdot \beta &= (\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_n, \dots) \end{aligned}$$

$$\text{όπου } \gamma_m = \sum_{i=0}^m a_i \beta_{m-i} = \sum_{i+j=m} a_i \beta_j.$$

Εύκολα επαληθεύουμε ότι $(A^{(N)}, +, \cdot)$ είναι μοναδιαίος και αντιμεταθετικός δακτύλιος με

$$\text{μηδέν } \theta = (0, 0, \dots)$$

$$\text{αντίθετο } -a = (-a_0, -a_1, \dots, -a_n, \dots)$$

$$\text{μονάδα } 1 = (1, 0, \dots)$$

Η συνάρτηση $a_0 \mapsto (a_0, 0, 0, \dots)$ του A στο δακτύλιο $A^{(\mathbb{N})}$ είναι ισομορφισμός δακτυλίων. Συνεπώς ο A είναι ισόμορφος με υποδακτύλιο του $A^{(\mathbb{N})}$. Θα γράφουμε λόγω του ισομορφισμού αυτού

$$a_0 = (a_0, 0, \dots)$$

Σπουδαίο ρόλο στην όλη θεωρία που θα αναπτύξουμε παίζει το στοιχείο

$$x = (0, 1, 0, \dots)$$

Παρατηρούμε ότι

$$x^2 = (0, 0, 1, 0, \dots)$$

$$x^3 = (0, 0, 0, 1, 0, \dots)$$

.....

$$x^n = (0, \dots, 0, 1, 0, \dots)$$

↑ _____ $n + 1$ θέση

Παρατηρούμε ακόμη ότι για κάθε $\lambda = (\lambda, 0, \dots)$ έχουμε

$$\lambda x^n = (\lambda, 0, \dots) \cdot (0, 0, \dots, 0, 1, 0, \dots)$$

$$= (0, 0, \dots, 0, \lambda, 0, \dots)$$

↑ _____ $n + 1$ θέση

Ένα οποιοδήποτε στοιχείο a του $A^{(\mathbb{N})}$ γράφεται

$$a = (a_0, a_1, \dots, a_n, 0, \dots)$$

$$= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, 0, a_n, 0, \dots)$$

$$= a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

Έτσι $A^{(\mathbb{N})} = A[x]$. Η συνάρτηση $f : A[x] \rightarrow A[s]$ με τιμή

$$f(a_0 + a_1 x + \dots + a_n x^n) = a_0 + a_1 s + \dots + a_n s^n$$

είναι ομομορφισμός δακτυλίων με τις ιδιότητες

$$1) f(a) = a \text{ για κάθε } a \in A$$

$$2) f(x) = s$$

Η πρώτη ιδιότητα σημαίνει ότι ο f είναι **επέκταση** του ταυτοτικού ομομορφισμού του A . Η εικόνα ενός πολυωνύμου $P \in A[x]$ με τον ομομορφισμό f συμβολίζεται με $P(s)$. Έτσι, αν

$$P = a_0 + a_1 x + \dots + a_n x^n, \text{ τότε } P(s) = a_0 + a_1 s + \dots + a_n s^n$$

Λέμε ότι αντικαταστήσαμε το x με το s . Το $P(s)$ λέγεται τιμή του πολυώνυμου P γὰι $x = s$.

Προφανώς για δύο πολυώνυμα $P, Q \in A[x]$,

$$(P + Q)(s) = P(s) + Q(s)$$

$$(P \cdot Q)(s) = P(s) \cdot Q(s)$$

Αν ο δακτύλιος A είναι αντιμεταθετικός και μοναδιαίος, μπορούμε να πάρουμε σαν s ένα οποιοδήποτε στοιχείο $c \in A$. Παίρνοντας ένα πολυώνυμο $P \in A[x]$, ορίζουμε μια συνάρτηση

$$\tilde{P} : c \mapsto P(c)$$

του A στον εαυτό του. Είναι η πολυωνυμική συνάρτηση, που ορίζεται από το πολυώνυμο P . Η συνάρτηση $P \mapsto \tilde{P}$ είναι ομομορφισμός του δακτυλίου $A[x]$ στο δακτύλιο των συναρτήσεων A^A . Όταν $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, ο ομομορφισμός είναι αμφιμονοσήμαντος και μπορούμε τότε να "ταυτίσουμε" το πολυώνυμο P με την πολυωνυμική συνάρτηση $\tilde{P}$ (οπότε δύο πολυώνυμα P, Q είναι ίσα, όταν οι πολυωνυμικές συναρτήσεις $\tilde{P}, \tilde{Q}$ είναι ίσες και αντίστροφα). Όμως δεν συμβαίνει αυτό πάντοτε. Π.χ. έστω $A = \mathbb{Z}_3$. Τα πολυώνυμα $P = x^3$, $Q = x$ είναι διάφορα, το πρώτο τρίτου βαθμού και το δεύτερο πρώτου. Οι συναρτήσεις όμως $\tilde{P}, \tilde{Q}$ είναι ίσες, γιατί $P(c) = Q(c)$ για κάθε $c \in \mathbb{Z}_3$.

$$\text{Πραγματικά : } \bar{0}^3 = \bar{0}, \bar{1}^3 = \bar{1}, \bar{2}^3 = \bar{2}$$

Ορισμοί - Λεξιλόγιο

Ο δακτύλιος $A[x]$ παράγεται από το σύνολο $A \cup \{x\}$. Κάθε στοιχείο του P έχει τη μορφή

$$P = a_0 + a_1x + \cdots + a_nx^n, \quad a_i \in A$$

και λέγεται πολυώνυμο της μεταβλητής x με συντελεστές a_i από το δακτύλιο A . Ο a_m λέγεται συντελεστής του x_m στο πολυώνυμο P . Γράφουμε $(P)_m = a_m$. Αν $Q = \beta_0 + \beta_1x + \cdots + \beta_kx_k \in A[x]$, έχουμε

$$P = Q \Leftrightarrow (P)_i = (Q)_i, \quad i = 0, 1, 2, \dots$$

Το πολυώνυμο $(0, 0, \dots, 0, \dots)$ λέγεται μηδενικό πολυώνυμο και συμβολίζεται με θ . Έτσι

$$a_0 + a_1x + \cdots + a_nx^n = \theta \Leftrightarrow a_0 = a_1 = \cdots = a_n = 0 \in A$$

Αν P είναι ένα μη μηδενικό πολυώνυμο, υπάρχει συντελεστής $a_n \neq 0$ τέτοιος, ώστε $a_k = 0$ για $k > n$. Ο φυσικός n λέγεται **βαθμός** του πολυωνύμου P και γράφουμε

$$d^o(P) = n.$$

Δεν ορίζουμε λοιπόν βαθμό του μηδενικού πολυωνύμου.

Ο συντελεστής a_0 λέγεται **σταθερός όρος** του πολυωνύμου P . Αν $d^o(P) = n$, ο συντελεστής a_n λέγεται **κύριος συντελεστής** του P . Ένα πολυώνυμο λέγεται **εναδικό**, αν ο κύριος συντελεστής του είναι 1, π.χ. το $-1 + 2x^2 + x^3$ είναι εναδικό με σταθερό όρο -1 και βαθμό 3.

Είναι γνωστή η χρησιμότητα και οι εφαρμογές του δακτυλίου $\mathbb{R}[x]$ των πολυωνύμων με συντελεστές πραγματικούς αριθμούς στη θεωρία συναρτήσεων. Δυστυχώς οι διαφορές του δακτυλίου αυτού με το δακτύλιο $A[x]$, όπου A ένας τυχαίος δακτύλιος, είναι τόσο μεγάλες, που εμφανίζονται ως "ανωμαλίες".

Αναφέρουμε μερικές από τις διαφορές αυτές, που θα μας απασχολήσουν αργότερα:

- Υπάρχουν πολυώνυμα που αντιστρέφονται

Π.χ. στο δακτύλιο $\mathbb{Z}_4[x]$ έχουμε

$$1 = (1 + 2x)(1 - 2x)$$

- Ένα πολυώνυμο είναι γινόμενο πολυωνύμων μεγαλύτερου ή ίσου βαθμού

Π.χ. στο δακτύλιο $\mathbb{Z}_6[x]$ έχουμε

$$x = (2 + 3x)(3 + 2x)$$

- Ο βαθμός του γινομένου δύο πολυωνύμων δεν ισούται με το άθροισμα των βαθμών αυτών πάντοτε

Π.χ. στο δακτύλιο $\mathbb{Z}_4[x]$ έχουμε

$$(x + 2x^2)(2x^2) = 2x^3$$

- Το πολυώνυμο $1 + x^2 + x^3 \in \mathbb{Z}_2[x]$ δεν έχει ρίζες στο σώμα $\mathbb{Z}_2$, γιατί για $x = \bar{0}, \bar{1}$ παίρνει την τιμή $\bar{1} \neq \bar{0}$ (αν και είναι περιττού βαθμού).

Δακτύλιος πολωνύμων δύο μεταβλητών

Έστω A ένας δακτύλιος και $A[x]$ ο δακτύλιος των πολωνύμων μιας μεταβλητής x του A . Ορίζουμε

$$A[x, y] = A[x][y]$$

Ο δακτύλιος $A[x, y]$ λέγεται δακτύλιος πολωνύμων δύο μεταβλητών, των μεταβλητών x, y .

Κάθε στοιχείο P του $A[x, y] = A[x][y]$ έχει τη μορφή

$$P = a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n$$

όπου $a_i \in A[x]$. Αν θέσουμε $a_i = \sum_{j=0}^{n_i} a_{ij} x^j$, έχουμε

$$P = \sum_{i=0}^n a_i y^i = \sum_{i=0}^n \left(\sum_{j=0}^{n_i} a_{ij} x^j \right) y^i = \sum_{i=0, j=0}^{n, n_i} a_{ij} x^j y^i$$

Π.χ. δύο πολυώνυμα του $\mathbb{Z}[x, y]$ είναι τα

$$1 + xy - x^2 y \quad , \quad 2 + xy^2 - x^3 + xy^4.$$

Δακτύλιος πολωνύμων περισσότερων μεταβλητών

Δακτύλιος των πολωνύμων n μεταβλητών $x_1, x_2, \dots, x_n$ με συντελεστές από το δακτύλιο A λέγεται ο δακτύλιος $S = A[x_1, x_2, \dots, x_n]$ που ορίζεται ως εξής:

$$A[x_1, x_2, \dots, x_n] = A[x_1, x_2, \dots, x_{n-1}][x_n].$$

Κάθε στοιχείο του S έχει τη μορφή πεπερασμένου αθροίσματος

$$\sum a_{i_1 i_2 \dots i_k} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$$

με συντελεστές $a_{i_1 i_2 \dots i_k} \in A$.

2. ΑΛΓΟΡΙΘΜΟΣ ΤΗΣ ΔΙΑΙΡΕΣΗΣ ΠΟΛΥΩΝΥΜΩΝ

Ιδιότητες του βαθμού

Αν τα πολυώνυμα P, Q είναι βαθμού m, n αντίστοιχα, τότε $(PQ)_i = 0$ για $i > m + n$. Γιατί, αν $P = (a_0, a_1, \dots, a_m, 0, \dots)$, $Q = (\beta_0, \beta_1, \dots, \beta_n, 0, \dots)$

$$\begin{aligned}(PQ)_i &= a_0\beta_i + a_1\beta_{i-1} + \dots + a_m\beta_{i-m} + a_{m+1}\beta_{i-m-1} + \dots + a_i\beta_0 \\ &= a_0 \cdot 0 + \dots + a_m \cdot 0 + 0 \cdot \beta_{i-m-1} + \dots + 0 \cdot \beta_0 = 0\end{aligned}$$

$$\begin{aligned}(PQ)_{m+n} &= a_0\beta_{m+n} + \dots + a_m\beta_n + a_{m+1}\beta_{n-1} + \dots + a_{m+n}\beta_0 = a_m\beta_n \\ &= (P)_m(Q)_n\end{aligned}$$

Άρα

$$d^o(PQ) \leq d^o(P) + d^o(Q)$$

$$d^o(PQ) = d^o(P) + d^o(Q) \Leftrightarrow (P)_m \cdot (Q)_n \neq 0$$

Έτσι, αν A είναι ακέραια περιοχή, ο δακτύλιος $A[x]$ θα είναι επίσης ακέραια περιοχή και ο βαθμός του γινομένου δύο πολυωνύμων θα ισούται με το άθροισμα των βαθμών αυτών.

Μια άλλη περίπτωση που ισχύει η ισότητα

$$d^o(PQ) = d^o(P) + d^o(Q)$$

είναι ο κύριος συντελεστής του ενός τουλάχιστον πολυωνύμου να αντιστρέφεται, γιατί τότε $(P)_m \cdot (Q)_n \neq 0$, αφού $(P)_m(Q)_n = 0$ και $(P)_m$ αντιστρέψιμος συνεπάγονται $(Q)_n = 0$, πράγμα άτοπο.

Υπενθυμίζουμε ότι όταν μιλάμε για βαθμό ενός πολυωνύμου P , υποθέτουμε αυτόματα ότι $P \neq \theta$. Είναι δυνατόν τα πολυώνυμα P, Q να είναι $\neq \theta$ και το $PQ = \theta$. Π.χ. στο δακτύλιο $\mathbb{Z}_4[x]$ έχουμε $P = Q = 2x^2 \neq \theta$, ενώ $P \cdot Q = 4x^4 = \theta$. Αν θέλουμε να ισχύουν οι παραπάνω ιδιότητες του βαθμού, ορίζουμε ως βαθμό του μηδενικού πολυωνύμου

$$d^o(\theta) = -\infty$$

Για το άθροισμα $P + Q$ προφανώς έχουμε

$$d^o(P) \neq d^o(Q) \Leftrightarrow d^o(P + Q) = \sup(d^o(P), d^o(Q))$$

$$d^o(P) = d^o(Q), (P)_n = -(Q)_n \Rightarrow d^o(P + Q) < d^o(P)$$

$$d^o(P) = d^o(Q), (P)_n \neq -(Q)_n \Rightarrow d^o(P + Q) = d^o(P)$$

Άρα

$$d^o(P + Q) \leq \sup(d^o(P), d^o(Q))$$

Αν ο δακτύλιος A είναι μοναδιαίος και ακέραια περιοχή, θα είναι και ο $A[x]$. Το δε γινόμενο δύο πολυωνύμων P, Q είναι $PQ = 1$ τότε και μόνο, όταν $d^o(P) + d^o(Q) = 0$ όταν δηλαδή $P, Q \in A$ και $PQ = 1$.

Άρα

Τα αντιστρέψιμα στοιχεία του δακτυλίου $A[x]$, όταν ο A είναι μοναδιαίος και ακέραια περιοχή, είναι τα αντιστρέψιμα στοιχεία του A .

Αλγόριθμος της διαίρεσης στο δακτύλιο $A[x]$

Θεώρημα 1. Έστω A ένας μοναδιαίος δακτύλιος και $f, g \in A[x]$. Αν ο κύριος συντελεστής του g αντιστρέφεται στο δακτύλιο A , υπάρχουν πολυώνυμα $q, v \in A[x]$ τέτοια, ώστε

$$f(x) = g(x)q(x) + v(x) \quad (1)$$

και $v(x) = \theta$ ή $d^o(v) < d^o(g)$.

Απόδειξη. Αν $f = \theta$ ή $d^o(f) < d^o(g)$, έχουμε $f(x) = 0 \cdot g(x) + f(x)$, συνεπώς $q = \theta, v = f$. Αν $d^o(f) = d^o(g) = 0$, τότε f, g είναι δύο μη μηδενικά στοιχεία a_0, u του A , οπότε $f(x) = a_0 u^{-1} \cdot g(x)$ και η ισότητα (1) ισχύει. Για τις άλλες περιπτώσεις των f, g θεωρούμε το πολυώνυμο $q \in A[x]$, ώστε το $f - gq$ να έχει τον ελάχιστο δυνατό βαθμό. Τότε $d^o(f - gq) < d^o(g)$ και αρκεί να πάρουμε $v(x) = f(x) - g(x)q(x)$.

Η επιλογή του q γίνεται ως εξής: Έστω

$$\begin{aligned} f(x) &= a_k x^k + \dots + a_0 \\ g(x) &= \beta_m x^m + \dots + \beta_0, \quad k \geq m. \end{aligned}$$

Θεωρούμε το πολυώνυμο

$$f_1(x) = f(x) - a_k \beta_m^{-1} x^{k-m} g(x)$$

βαθμού $\leq k - 1$. Συνεχίζουμε με τον ίδιο τρόπο: Αφαιρούμε από το $f_1(x)$ ένα πολλαπλάσιο του $g(x)$ και βρίσκουμε ένα πολυώνυμο βαθμού $\leq k - 2$ κ.ο.κ.

Η μοναδικότητα των q, v προκύπτει ως εξής: Έστω q_1, v_1 δύο άλλα πολυώνυμα που πληρούν την (1) και ότι π.χ. $d^o(v_1) \leq d^o(v)$. Τότε

$$f(x) = q_1(x)g(x) + v_1(x) = q(x)g(x) + v(x)$$

οπότε $(q_1(x) - q(x)) \cdot g(x) = v(x) - v_1(x)$

Αν $q_1 - q \neq \theta$, θα έχουμε $d^o(q_1 - q)g = d^o(q_1 - q) + d^o(g)$, γιατί ο κύριος συντελεστής β_m του g αντιστρέφεται. Συνεπώς $d^o(v - v_1) = d^o(q_1 - q)g > d^o(g)$, πράγμα άτοπο, γιατί $d^o(v - v_1) < d^o(g)$. Άρα $q_1 = q$, οπότε και $v_1 = v$. $\square$

Πόρισμα. Αν K είναι σώμα, η διαίρεση στο δακτύλιο $K[x]$ είναι πάντοτε δυνατή.

Παράδειγμα. Έστω $f(x) = x^3 + x^2 + x$, $g(x) = x^2 + 2 \in \mathbb{Z}_3[x]$. Βρείτε το πηλίκο και το υπόλοιπο της διαίρεσης του f με το g .

$$\begin{aligned} \text{Λύση. Έστω } f_1(x) &= f(x) - x^{3-2}g(x) = x^3 + x^2 + x - x(x^2 + 2) \\ &= x^2 - x = x^2 + 2x \end{aligned} \quad (1)$$

$$\begin{aligned} f_2(x) &= f_1(x) - x^{2-2}g(x) = f_1(x) - g(x) \\ &= x^2 + 2x - x^2 - 2 = 2x + 1 \end{aligned} \quad (2)$$

Από τις (2) και (1) παίρνουμε

$$\begin{aligned} 2x + 1 &= f_1(x) - g(x) = f(x) - xg(x) - g(x) \\ \text{ή} \quad f(x) &= (x + 1)g(x) + (2x + 1) \end{aligned}$$

δηλαδή $q(x) = x + 1$ και $v(x) = 2x + 1$, αφού $d^o(v) = 1 < d^o(g) = 2$. Η παραπάνω διαδικασία περιγράφεται με το παρακάτω σχήμα

$\begin{array}{r} x^3 + x^2 + x \\ x^2 - x = x^2 + 2x \\ \hline 2x - 2 = \\ 2x + 1 \end{array}$	$\begin{array}{r} x^2 + 2 \\ x + 1 \end{array}$	$\begin{array}{r l} f & g \\ \hline f_1 = f - xg & x + 1 = q \\ f_2 = f_1 - g & \\ v & \end{array}$
---	---	---

Ιδεώδη του δακτυλίου $A[x]$

Θεώρημα 1. Κάθε ιδεώδες του δακτυλίου $A[x]$, όταν ο A είναι σώμα αντιμεταθετικό, είναι κύριο, δηλαδή παράγεται από ένα στοιχείο.

Απόδειξη. Έστω I ένα ιδεώδες του $A[x]$, $I \neq (0)$. Θεωρούμε το πολυώνυμο με το μικρότερο βαθμό μέσα στο I , έστω το f . Για κάθε $p(x) \in A[x]$, έχουμε $f(x)p(x) \in I$. Αν $h(x) \in I$, κάνοντας τη διαίρεση αυτού με το f , παίρνουμε $h(x) = f(x)q(x) + v(x)$, όπου $v = \theta$ ή $d^o(v) < d^o(f)$. Αλλά $v(x) = h(x) - f(x)q(x) \in I - I = I$. Συνεπώς $v = \theta$ και $h(x) = f(x)q(x)$. Άρα $I = (f)$. $\square$

ΑΣΚΗΣΕΙΣ

1. Γράψτε όλα τα πολυώνυμα $1^{\text{ου}}$ και $2^{\text{ου}}$ βαθμού του δακτυλίου $\mathbb{Z}_2[x]$. Για ποιά πολυώνυμα $f \in \mathbb{Z}_2[x]$ βαθμού ≤ 2 υπάρχει $a \in \mathbb{Z}_2$ με $f(a) = 0$;

2. Βρείτε το άθροισμα και το γινόμενο των πολυωνύμων $g, f \in \mathbb{Z}_7[x]$, αν

$$f = 2x^3 + 6x^2 + 3x + 2, \quad g = x^4 + 5$$

3. Έστω δύο πολυώνυμα $a = x^6 + 2x^5 - 2x, \beta = x^2 \in \mathbb{Z}_5[x]$. Τα πολυώνυμα αυτά είναι ίσα; Οι συναρτήσεις $a^*, \beta^* : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ με $a^*(x) = x^6 + 2x^5 - 2x, \beta^*(x) = x^2$ είναι ίσες;

4. Έστω ένας ομομορφισμός $\varphi : \mathbb{Z}_5[x] \rightarrow \mathbb{Z}_5$ με $\varphi(x) = \bar{3}$. Βρείτε την τιμή $\varphi(x^{231} + 3x^{117} - 2x^{53} + 1)$.

5. Βρείτε τα πολυώνυμα $x + \bar{a}, x + \bar{\beta} \in \mathbb{Z}_5[x]$ ώστε $x^2 + x - \bar{1} = (x + \bar{a})(x + \bar{\beta})$.

6. Έστω $a = x^3 + \bar{3}, \beta = 2x^2 + 3x + \bar{4} \in \mathbb{Z}_5[x]$. Να βρείτε το ηλίκο και το υπόλοιπο της διαίρεσης του a με το β .

7. Ποιά είναι το ιδεώδες I του δακτυλίου $\mathbb{Z}_2[x]$ που παράγεται από το πολυώνυμο $x^2 + x + 1$; Γράψτε τα στοιχεία του δακτυλίου ηλίκου $\mathbb{Z}_2[x]/I$ και τους πίνακες των πράξεων στο δακτύλιο αυτό.

8. Έστω I το ιδεώδες του δακτυλίου $\mathbb{Z}[x]$ που παράγεται από το πολυώνυμο $x^2 + 1$. Ν' αποδείξετε ότι ο δακτύλιος ηλίκο $\mathbb{Z}[x]/I$ είναι ισόμορφος του δακτυλίου του Gauss $\mathbb{Z}[i]$.

9. Έστω I το ιδεώδες του δακτυλίου $\mathbb{Q}[x]$ που παράγεται από το πολυώνυμο $x^2 - 2$. Ν' αποδείξετε ότι το ηλίκο $\mathbb{Q}[x]/I$ είναι σώμα ισόμορφο του $\mathbb{Q}(\sqrt{2}) = \{a + \beta\sqrt{2}; a, \beta \in \mathbb{Q}\}$.

10. Έστω $K = \mathbb{Q}[x]/(x^3 - 1)$ ο δακτύλιος ηλίκο του $\mathbb{Q}[x]$ με το ιδεώδες $I = (x^3 - 1)$. Να εξετάσετε, αν το στοιχείο $(x - 1) + I$ του δακτυλίου K αντιστρέφεται.

11. Βρείτε το ηλίκο της διαίρεσης του πολυωνύμου $nx^{n+1} - (n+1)x^n + 1 \in \mathbb{R}[x]$ με το πολυώνυμο $(x - 1)^2$.

12. Βρείτε το υπόλοιπο της διαίρεσης ενός πολυωνύμου $f \in \mathbb{R}[x]$ με $(x - a)(x - \beta)$, όταν $a \neq \beta$ και όταν $a = \beta$.

13. Έστω K ένα σώμα. Δείξτε ότι κάθε πολυώνυμο $f(x) \in K[x]$ γράφεται υπό τη μορφή $h(x^2) + xg(x^2)$, όπου $h(x), g(x) \in K[x]$. Βρείτε το υπόλοιπο της διαίρεσης του f με το $x^2 - a \in K[x]$.

14. Ν' αποδείξετε ότι το υπόλοιπο της διαίρεσης του πολυωνύμου $nx^{n+1} - (n+1)x^n + 1$ με $(x - 1)^2$ είναι μηδέν.

15. Πόσα πολυώνυμα της μορφής $(x + \bar{a})^3$ με $\bar{a} \in \mathbb{Z}_{31}$ υπάρχουν στο δακτύλιο $\mathbb{Z}_{31}[x]$;

16. Βρείτε τους συντελεστές του πολυωνύμου $(1+x)^{m+n}$ με δύο τρόπους και δείξτε ότι
$$\sum_{\rho=0}^k \binom{m}{\rho} \binom{n}{k-\rho} = \binom{m+n}{k}.$$

17. Δείξτε ότι ο αριθμός των μονωνύμων βαθμού k ως προς $x_0, x_1, \dots, x_n$ είναι $\binom{n+k}{n}$.

10 | Κύριοι δακτύλιοι διααιρετότητα

1. ΚΥΡΙΟΙ ΔΑΚΤΥΛΙΟΙ

Είδαμε ότι ένα οποιοδήποτε ιδεώδες του δακτυλίου $\mathbb{Z}$ παράγεται από ένα στοιχείο του και καλέσαμε το ιδεώδες αυτό κύριο. Δεν συμβαίνει όμως το ίδιο στο δακτύλιο $\mathbb{Z}[x]$.

Παράδειγμα. Έστω I το σύνολο των πολυωνύμων $f = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ με a_0 τέτοιο, ώστε $7/a_0$. Το I είναι ένα ιδεώδες του $\mathbb{Z}[x]$, όχι κύριο.

Πραγματικά, είναι εύκολο να δούμε ότι το I είναι ιδεώδες: Προφανώς $f \in \mathbb{Z}[x]$ τότε και μόνο, όταν $f = xg + 7h$ με $g, h \in \mathbb{Z}[x]$, οπότε $I = (x, 7)$. Έστω ότι το I είναι κύριο ιδεώδες, $I = (a)$. Επειδή $x, 7 \in I$, έχουμε $a/7, a/x$. Αλλά $a/7$ συνεπάγεται $d^\circ(7) \geq d^\circ(a)$ ή $0 \geq d^\circ(a) \geq 0$, δηλαδή $d^\circ(a) = 0$. Έτσι $I = (7)$. Επειδή $x \in I$, θα πρέπει $7/x$, πράγμα αδύνατο στο δακτύλιο $\mathbb{Z}[x]$.

Γενικά

Ορισμός 1. Ένας δακτύλιος R λέγεται κύριος, αν είναι ακέραια περιοχή και κάθε ιδεώδες του είναι κύριο, δηλαδή της μορφής (a) .

Έτσι οι δακτύλιοι $\mathbb{Z}$ και $K[x]$, όταν ο K είναι σώμα αντιμεταθετικό, είναι

κύριοι.

Μια άλλη κατηγορία δακτυλίων, οι οποίοι είναι κύριοι δακτύλιοι, είναι οι καλούμενοι Ευκλείδεια δακτύλιοι:

Ορισμός 2. Ένας δακτύλιος μοναδιαίος A χωρίς διαιρέτες του μηδενός, λέγεται **Ευκλείδειος δακτύλιος**, αν υπάρχει μια συνάρτηση $d : A^* \rightarrow \mathbb{N}$, τέτοια, ώστε

- i) $d(x) \leq d(xy)$ για όλα τα $x, y \in A^* = A - \{0\}$
- ii) Για οποιαδήποτε $a, \beta \in A^*$, υπάρχουν $q, v \in A$ τέτοια, ώστε

$$a = \beta q + v \quad \text{με } v = 0 \quad \text{ή} \quad d(v) < d(\beta)$$

Η συνάρτηση d λέγεται **Ευκλείδεια στάθμη** επί του A .

Παράδειγμα 1. Ο δακτύλιος $\mathbb{Z}$ είναι Ευκλείδειος με Ευκλείδεια στάθμη $d(a) = |a|$.

Παράδειγμα 2. Αν K είναι σώμα, ο δακτύλιος των πολυωνύμων $K[x]$ είναι ευκλείδειος με ευκλείδεια στάθμη $d(f) = d^o(f) = \text{βαθμός του } f$.

Παράδειγμα 3. Έστω $\mathbb{Z}[i] = \{a + \beta i ; a, \beta \in \mathbb{Z}\}$ ο δακτύλιος των ακεραίων του Gauss. Ορίζουμε τη συνάρτηση $d : \mathbb{Z}[i] \rightarrow \mathbb{Z}$ θέτοντας $d(a + \beta i) = a^2 + \beta^2$. Έτσι, αν $x = a + \beta i$,

$$d(x) = x\bar{x}$$

Η συνάρτηση d είναι ευκλείδεια στάθμη επί του $\mathbb{Z}[i]$. Πραγματικά, έστω $x, y \neq 0$ στο δακτύλιο $\mathbb{Z}[i]$. Έχουμε

- 1) $d(xy) = xy\bar{x}\bar{y} = xy\bar{x}\bar{y} = |x|^2 d(y) \geq d(y)$, αφού $|x|^2 = |a + \beta i|^2 = a^2 + \beta^2 \geq 1$.
- 2) Έστω $\frac{x}{y} = u + iv (u, v \in \mathbb{Q})$. Υπάρχει $q = m + in \in \mathbb{Z}[i]$ με m, n ακεραίους τέτοιους, ώστε

$$|u - m| < \frac{1}{2}, \quad |v - n| < \frac{1}{2}$$

Θα έχουμε

$$\frac{x}{y} - q = (u - m) + i(v - n)$$

Αν θέσουμε $v = x - qy$ έχουμε

$$\begin{aligned} d(v) &= d\left(y\left(\frac{x}{y} - q\right)\right) = d(y)d\left(\frac{x}{y} - q\right) \\ &= d(y)d((u-m) + i(v-n)) \\ &= d(y)[(u-m)^2 + (v-n)^2] \leq d(y) \cdot \left(\frac{1}{4} + \frac{1}{4}\right) \\ &< d(y) \end{aligned}$$

Άρα η d είναι ευκλείδεια στάθμη επί του $\mathbb{Z}[i]$.

Θεώρημα 1. Έστω A ένας ευκλείδειος δακτύλιος με στάθμη d . Τότε

- i) $d(1) = \min\{d(a) ; a \in A\}$
- ii) Το u είναι ενάδα τότε και μόνο, όταν $d(u) = d(1)$.

Απόδειξη. i) Αν $a \neq 0$, έχουμε $d(1) \leq d(1 \cdot a) = d(a)$.

- ii) Αν το u είναι ενάδα, $d(u) \leq d(u \cdot u^{-1}) = d(1)$, συνεπώς $d(u) = d(1)$.

Αντίστροφα, έστω $u \in A - \{0\}$ με $d(u) = d(1)$. Έστω $q, v \in A$ με $1 = uq + v$, όπου $v = \theta$ ή $d(v) < d(u)$. Αφού όμως $d(u) = d(1)$ είναι το ελάχιστο των $d(a)$ με $a \in A - \{0\}$, δεν ισχύει η σχέση $d(v) < d(u)$.

Άρα $v = 0, 1 = uq$ και το u είναι ενάδα. $\square$

Εφαρμογή. Τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}[i]$ είναι $\pm 1, \pm i$. Πραγματικά, έστω x ένα αντιστρέψιμο στοιχείο του $\mathbb{Z}[i]$. Πρέπει $d(x) = 1$. Αν $x = a + \beta i$ με $a, \beta \in \mathbb{Z}$, έχουμε $d(x) = a^2 + \beta^2 = 1$. Άρα $\beta^2 = 0$ και $a^2 = 1$ ή $a^2 = 1$ και $\beta^2 = 0$, δηλαδή $x = \pm 1$ ή $x = \pm i$.

Θεώρημα 2. Κάθε ευκλείδειος δακτύλιος R είναι κύριος.

Απόδειξη. Έστω d η στάθμη του R και I ένα ιδεώδες του R . Για κάθε $y \in I, d(y) \in \mathbb{N}$. Έστω $a \in I$ με $d(a) = \min\{d(y) ; y \in I\}$. Κάθε $x \in I$ γράφεται υπό την μορφή $x = aq + v$ με $q, v \in R$ και $v = 0$ ή $d(v) < d(a)$. Άρα $v = 0$ και $x = aq \in aR$, δηλαδή $I = aR$. $\square$

2. ΔΙΑΙΡΕΤΟΤΗΤΑ

Θα επεκτείνουμε τον ορισμό της διαιρετότητας των ακεραίων σε μια αντιμεταθετική ακέραια περιοχή με μοναδιαίο στοιχείο.

Ορισμός 1. Έστω A μια αντιμεταθετική ακέραια περιοχή με μοναδιαίο στοιχείο και δύο στοιχεία αυτής $a, \beta \neq 0$. Λέμε ότι το " a διαιρεί το β στον A " και γράφουμε $a \mid_A \beta$, αν υπάρχει $\gamma \in A$ τέτοιο, ώστε $\beta = a\gamma$. Το a

λέγεται **διαιρέτης** του β και το β **πολλαπλάσιο** του a . Όταν ο δακτύλιος A είναι καθορισμένος, γράφουμε a/β αντί $a/{}_A\beta$.

Οι ιδιότητες που αναφέρονται παρακάτω είναι άμεση συνέπεια του ορισμού:

- i) $a/\beta, \beta/\gamma \Rightarrow a/\gamma$
- ii) $a/\beta \Rightarrow a/\beta\gamma$ για κάθε γ
- iii) $a/\beta, a/\gamma \Rightarrow a/(\beta + \gamma), a/(\beta x + \gamma y)$ για όλα τα x, y .

Παράδειγμα 1. Στο δακτύλιο $\mathbb{Z}[i]$, $4+3i/25$, γιατί $25 = (4+3i)(4-3i)$.

Παράδειγμα 2. Στο δακτύλιο $\mathbb{Z}_6[x]$, έστω $a = x + \bar{5}$, $\beta = \bar{5}x + \bar{1}$. Έχουμε ότι a/β και β/a , γιατί

$$\beta = \bar{5}a \quad \text{και} \quad a = \bar{5}\beta.$$

Παράδειγμα 3. Στο δακτύλιο $\mathbb{Z}_6[x]$, έστω $a = \bar{2}x + \bar{1}$, $\beta = x + \bar{5}$. Έχουμε ότι a/β , αλλά $\beta \neq a$.

Πραγματικά, $(\bar{3}x + \bar{5}) \cdot (\bar{2}x + \bar{1}) = x + \bar{5}$, δηλαδή $(\bar{3}x + \bar{5})a = \beta$ συνεπώς a/β . Έστω ότι β/a . Τότε $a = \gamma\beta$ με $\gamma \in \mathbb{Z}_6[x]$. Επειδή ο κύριος συντελεστής του β αντιστρέφεται, έχουμε $d^\circ(\gamma\beta) = d^\circ(\gamma) + d^\circ(\beta) = d^\circ(\gamma) + 1$ και η σχέση $a = \gamma\beta$ συνεπάγεται $d^\circ(a) = d^\circ(\gamma) + 1$ ή $d^\circ(\gamma) = 0$. Τα μόνα πολυώνυμα στο $\mathbb{Z}_6[x]$ βαθμού μηδέν, είναι τα στοιχεία του $\mathbb{Z}_6 - \{0\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Όμως

$$a \neq \bar{1} \cdot \beta, a \neq \bar{2}\beta = \bar{4}x + \bar{2}, a \neq \bar{3}\beta = \bar{3}, a \neq \bar{4}\beta = \bar{2}x + \bar{2}$$

και $a \neq \bar{5}\beta = \bar{x} + \bar{5}$. Άρα $\beta \neq a$.

Στη συνέχεια A θα είναι μια αντιμεταθετική ακέραια περιοχή με μοναδιαίο στοιχείο 1, εκτός αν ορίζεται διαφορετικά.

Ορισμός 2. Δύο στοιχεία a, β του A θα λέγονται **συνδεδεμένα**, αν a/β και β/a .

Π.χ. τα a, β στο παράδειγμα 2 είναι συνδεδεμένα. Τα συνδεδεμένα στοιχεία του $\mathbb{Z}$ είναι n και $-n$. Τα στοιχεία a, β του παραδείγματος 3 δεν είναι συνδεδεμένα.

Πρόταση 1. Οι παρακάτω προτάσεις είναι ισοδύναμες στο δακτύλιο A (αντιμεταθετική ακέραια περιοχή με μονάδα)

- i) a, β είναι συνδεδεμένα
- ii) $a = u\beta$ με u αντιστρέψιμο στοιχείο του A (ενάδα)
- iii) $(a) = (\beta)$, δηλαδή τα a, β παράγουν το ίδιο κύριο ιδεώδες.

Απόδειξη. i) $\Rightarrow$ ii) Υπάρχουν $u, v \in A$ τέτοια, ώστε $\beta = au$, $a = \beta v$. Τότε

$a = auv$ και συνεπώς για $a \neq 0$, $uv = 1$. Αν $a = 0$, θα έχουμε $\beta = a\gamma = 0$ και συνεπώς $a = 1 \cdot \beta$, $\beta = 1 \cdot a$, δηλαδή τα a, β είναι και πάλι συνδεδεμένα.

- ii) $\Rightarrow$ iii) Έχουμε $aA = u\beta A = \beta(uA) = \beta A$, γιατί $uA = A$, αφού $uA \subseteq A$ και κάθε $x \in A$, γράφεται και $x = u(u^{-1}x) \in uA$.
 iii) $\Rightarrow$ i) $(a) = (\beta)$ σημαίνει $aA = \beta A$. Καθώς $\beta \in \beta A$, έχουμε $\beta \in aA$, συνεπώς $\beta = a\gamma$ με $\gamma \in A$, δηλαδή a/β . Όμοια β/a . $\square$

Πόρισμα 1. Δύο πολυώνυμα a, β του $A[x]$ είναι συνδεδεμένα, αν $a = u\beta$ με u αντιστρέψιμο στοιχείο του A . Τότε $d^\circ(a) = d^\circ(\beta)$.

Πόρισμα 2. Έστω $U(a)$ το σύνολο των αντιστρέψιμων στοιχείων του A , η ομάδα των ενάδων του A (βλ. §5 Κεφ.2). Η σχέση " a είναι συνδεδεμένο του β " είναι μια σχέση ισοδυναμίας με κλάσεις $aU(A)$.

Ορισμός 3. Ένα στοιχείο $a \neq 0$ του δακτυλίου A λέγεται **ανάγωγο**, αν οι μόνοι διαιρέτες του είναι τα αντιστρέψιμα στοιχεία και τα στοιχεία του $aU(A) = \{au ; u \text{ αντιστρέψιμο} \}$.

Παράδειγμα. Ο 5 είναι ανάγωγο στοιχείο του $\mathbb{Z}$. Δεν είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$, γιατί $5 = (1 + 2i)(1 - 2i)$ και τα στοιχεία $1 + 2i$, $1 - 2i$ δεν αντιστρέφονται στο δακτύλιο $\mathbb{Z}[i]$, αφού τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[i]$ είναι ± 1 , $\pm i$.

Θεώρημα 1. Σ' ένα κύριο δακτύλιο A , ένα στοιχείο $p \neq 0$ είναι ανάγωγο τότε και μόνο, όταν το ιδεώδες pA είναι πρώτο.

Απόδειξη. Έστω ότι το ιδεώδες pA είναι πρώτο και ότι β/p . Αν $p = \beta\gamma$, τότε $\beta\gamma \in pA$. Ας υποθέσουμε ότι $\gamma \notin pA$, οπότε $\beta \in pA$. Συνεπώς υπάρχει $a \in A$ τέτοιο, ώστε $\beta = pa$ και επομένως $p = \beta\gamma = pa\gamma$. Αφού ο A είναι ακέραια περιοχή, $a\gamma = 1$, δηλαδή τα a, γ είναι αντιστρέψιμα. Έτσι $\beta = pa$ και άρα το p είναι ανάγωγο.

Αντίστροφα, έστω ότι το p είναι ανάγωγο. Το ιδεώδες pA είναι μέγιστο, γιατί, αν $pA \subseteq aA$, θα είναι $p = a\beta$. Τα a, β είναι δηλαδή διαιρέτες του p . Αν το a είναι αντιστρέψιμο, το ιδεώδες $aA = A$. Αν το a δεν είναι αντιστρέψιμο, θα πρέπει $a = pu$ με $p = pu\beta$ ή $u\beta = 1$ και συνεπώς $aA = p(uA) = pA$, γιατί το u είναι αντιστρέψιμο, οπότε $uA = A$. Άρα $aA = A$ ή pA , που σημαίνει ότι το pA είναι μέγιστο, οπότε είναι και πρώτο. $\square$

Πόρισμα. Σ' ένα κύριο δακτύλιο κάθε πρώτο ιδεώδες $\neq (0)$ είναι μέγιστο.

Εφαρμογή. Έστω ο δακτύλιος $\mathbb{R}[x]$ και το πολυώνυμο $p = x^2 + 1$. Εύκολα φαίνεται ότι είναι ανάγωγο. Το πηλίκο $\mathbb{R}[x]/(x^2 + 1)$ είναι σώμα. Έστω $I = (x^2 + 1)$. Τα στοιχεία $\mathbb{R}[x]/I$ είναι της μορφής $f(x) + I$, όπου $f(x) \in \mathbb{R}[x]$. Κάνοντας τη διαίρεση του $f(x)$ με το $x^2 + 1$ βρίσκουμε υπόλοιπο $a + \beta x$, οπότε $f(x) + I = (a + \beta x) + f(x) \cdot q(x) + I = (a + \beta x) + I$. Η συνάρτηση $F : \mathbb{R}[x]/I \rightarrow \mathbb{C}$ με τιμή $F((a + \beta x) + I) = a + \beta i$ είναι ισομορφισμός σωμάτων. Πραγματικά, αν θέσουμε $(a + \beta x) + I = a$, $(\gamma + \delta x) + I = b$, έχουμε

$$F(a + b) = (a + \gamma) + (\beta + \delta)i = (a + \beta i) + (\gamma + \delta i) = F(a) + F(b)$$

$$\begin{aligned} \text{και } ab &= (a + \beta x)(\gamma + \delta x) + I = a\gamma + \beta\delta x^2 + (\beta\gamma + a\delta)x + I \\ &= a\gamma - \beta\delta + (\beta\gamma + a\delta)x + I, \text{ αφού } \beta\delta(x^2 + 1) \in I \end{aligned}$$

οπότε

$$F(ab) = (a\gamma - \beta\delta) + (\beta\gamma + a\delta)i = (a + \beta i)(\gamma + \delta i) = F(a)F(b)$$

Τέλος $F(a) = 0$ συνεπάγεται $a + \beta i = 0$ ή $a = \beta = 0$ και $a = I$. Άρα

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$$

Ας δεχτούμε στο σημείο αυτό ότι ρίζα ενός πολυωνύμου $p(x)$ λέγεται ένα στοιχείο a για το οποίο $p(a) = 0$. Τότε το σώμα $\mathbb{R}[x]/(x^2 + 1)$ περιέχει μια ρίζα του $p(x) = x^2 + 1$. Η ρίζα είναι $x + (x^2 + 1) = x + I$, γιατί

$$p(x + I) = (x + I)^2 + 1 = (x^2 + I) + 1 = I$$

και I είναι του μηδέν του $\mathbb{R}[x]/I$.

Θεώρημα 2. Σε κάθε κύριο δακτύλιο A μια αύξουσα ακολουθία ιδεωδών

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots \subseteq I_n \subseteq \dots$$

είναι τελικά σταθερή, δηλαδή $I_k = I_n$ για $k \geq n$.

Απόδειξη. Έστω $I = \cup I_n$. Το I είναι ιδεώδες του A , γιατί, αν $a, \beta \in I$, έχουμε $a \in I_n$, $\beta \in I_k$ ($k \geq n$) οπότε $a, \beta \in I_k$ και $a - \beta \in I_k$, δηλαδή $a - \beta \in I$. Αν επιπλέον $\gamma \in A$, έχουμε $a\gamma \in I_n$, δηλαδή $a\gamma \in I$. Συνεπώς I είναι ιδεώδες του A . Έστω $I = dA$. Πρέπει το d να ανήκει σε κάποιο από τα ιδεώδη I_k . Τότε $I \subseteq I_k$, συνεπώς $I = I_k$ και άρα $I_m \subseteq I_k$ για $m \geq k$, δηλαδή $I_m = I_k$. $\square$

3. ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ

Ορισμός 1. Έστω $a_1, a_2, \dots, a_n$ στοιχεία $\neq 0$ ενός μοναδιαίου αντιμεταθετικού δακτυλίου A . Ένα στοιχείο d λέγεται **κοινός διαιρέτης** των $a_1, a_2, \dots, a_n$, αν $d/a_i (i = 1, 2, \dots, n)$. Λέγεται **μέγιστος κοινός διαιρέτης** των $a_1, a_2, \dots, a_n$, αν

- 1) $d/a_i (i = 1, 2, \dots, n)$, είναι δηλαδή κοινός διαιρέτης και
- 2) $d'/a_i (i = 1, 2, \dots, n) \Rightarrow d'/d$.

Γράφουμε τότε $d = \mu.κ.δ. (a_1, a_2, \dots, a_n)$ ή απλούστερα $d = (a_1, a_2, \dots, a_n)$.

Θεώρημα 1. Έστω A ένας κύριος δακτύλιος και $a_1, a_2, \dots, a_n \in A$, $a_i \neq 0$. Υπάρχει μέγιστος κοινός διαιρέτης d των $a_1, a_2, \dots, a_n$ και μάλιστα της μορφής

$$d = a_1 x_1 + a_2 x_2 + \dots + a_n x_n \quad \text{με } x_i \in A$$

Απόδειξη. Θεωρούμε τα ιδεώδη $a_i A$. Το άθροισμά τους είναι ιδεώδες του A . Έστω

$$dA = a_1 A + a_2 A + \dots + a_n A$$

Επειδή $a_i A \subseteq dA$ έχουμε $a_i \in dA$, δηλαδή $d/a_i (i = 1, 2, \dots, n)$. Αν $d'/a_i (i = 1, 2, \dots, n)$, τότε $d' \in a_i A \subseteq a_1 A + a_2 A + \dots + a_n A = dA$, δηλαδή $d' \in dA$ και d'/d . $\square$

Παρατήρηση. Δεν υπάρχει πάντοτε $\mu.κ.δ.$ δύο στοιχείων a, β .

Παράδειγμα. Έστω $\mathbb{Z}[\omega] = \{a + b\omega ; a, \beta \in \mathbb{Z}\}$ και $\omega = i\sqrt{5}$. Εύκολα διαπιστώνουμε ότι $\mathbb{Z}[\omega]$ είναι υποδακτύλιος του $\mathbb{C}$. Θεωρούμε τα στοιχεία $a = 9$ και $\beta = 3(2 + \omega)$. Οι κοινοί διαιρέτες είναι τα στοιχεία $1, 3, 2 + \omega$. Πραγματικά, έστω $9 = (x + y\omega)(u + v\omega)$. Τότε $9 = (x - y\omega)(u - v\omega)$, $81 = (x^2 + 5y^2)(u^2 + 5v^2)$. Πρέπει $x^2 + 5y^2 = 1, 3, 9, 27$ ή 81 με $x, y \in \mathbb{Z}$. Βρίσκουμε τελικά ότι οι διαιρέτες του 9 είναι $\pm 1, \pm 3, \pm(2 + \omega), \pm(2 - \omega)$. Όμοια βρίσκουμε ότι οι διαιρέτες του $3(2 + \omega)$ είναι $\pm 1, \pm 3, \pm(2 + \omega)$. Οι κοινοί διαιρέτες των a, β είναι χωρίς τον παράγοντα ± 1 τα στοιχεία $1, 3, 2 + \omega$. Επειδή $3 \neq 1$, ο 1 δεν είναι $\mu.κ.δ.$ των a, β . Επειδή $2 + \omega \neq 3$, ο 3 δεν είναι $\mu.κ.δ.$ των a, β . Τέλος ο $2 + \omega$ δεν είναι $\mu.κ.δ.$ των a, β γιατί $3 \neq 2 + \omega$.

Πόρισμα. Δύο $\mu.κ.δ.$ d, d' των $a_1, a_2, \dots, a_n$ είναι συνδεδεμένα στοιχεία.

Γιατί, αφού $d = \mu.κ.δ.(a_1, a_2, \dots, a_n)$, d'/d . Αντιστρέφοντας το ρόλο των d, d' έχουμε d/d' . Άρα το συμπέρασμα. $\square$

Ορισμός 2. Τα στοιχεία $a_1, a_2, \dots, a_n$ του δακτυλίου $A - \{0\}$ λέγονται **ξένα** μεταξύ τους, αν $\mu.κ.δ.(a_1, a_2, \dots, a_n) = 1$.

Βάσει του παραπάνω θεωρήματος προκύπτει άμεσα το

Πόρισμα. Σ' ένα κύριο δακτύλιο A τα στοιχεία $a_1, a_2, \dots, a_n$ με $a_i \neq 0$ είναι ξένα μεταξύ τους τότε και μόνο, όταν υπάρχουν $x_i \in A (i = 1, 2, \dots, n)$ τέτοια, ώστε

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = 1$$

Η σχέση αυτή είναι γνωστή σαν **ταυτότητα του Bezout**.

Θεώρημα 2. Έστω A ένας κύριος δακτύλιος και $a, \beta \in A$. Αν p είναι ένα ανάγωγο στοιχείο του A τέτοιο, ώστε $p/a\beta$, τότε p/a ή p/β .

Απόδειξη. Έστω ότι $p \neq a$. Αφού το p είναι ανάγωγο είναι $\neq 0$. Υπάρχει $\mu.κ.δ.(p, a) = d$. Επειδή d/p , το d είναι συνδεδεμένο με το p ή είναι μια ενάδα του A . Στην πρώτη περίπτωση p/d , d/a , συνεπώς p/a , πράγμα άτοπο. Έτσι το d είναι μια ενάδα και $dd^{-1} = 1 = \mu.κ.δ.(p, a)$, αφού d^{-1} είναι ενάδα. Τότε βάσει της ταυτότητας του Bezout έχουμε $px + ay = 1$ ή $p(\beta x) + (a\beta)y = \beta$, οπότε p/β , αφού $p/a\beta$. $\square$

Πόρισμα. Αν A είναι κύριος δακτύλιος, $a_1, a_2, \dots, a_n \in A$ και p ανάγωγο στοιχείο του A , τότε

$$p/a_1a_2 \dots a_n \Rightarrow p/a_i \text{ για κάποιο } i$$

Το παραπάνω θεώρημα δεν προσφέρεται για την εύρεση του $\mu.κ.δ.$ Στην πράξη για το σκοπό αυτό εφαρμόζεται ένας **αλγόριθμος του Ευκλείδη**, που περιγράφεται στο παρακάτω θεώρημα.

Θεώρημα 3. Έστω A ένας Ευκλείδειος δακτύλιος με στάθμη d και $a, \beta \in A - \{0\}$. Έστω

$$(1) \quad a = \beta q_1 + v_1 \quad \text{με} \quad v_1 = 0 \text{ ή } d(v_1) < d(\beta).$$

Αν $v_1 \neq 0$, θεωρούμε τα q_2, v_2

$$\beta = v_1 q_2 + v_2 \quad \text{με} \quad v_2 = 0 \text{ ή } d(v_2) < d(v_1).$$

Γενικά έστω q_{k+1}, v_{k+1} τέτοια, ώστε

$$v_{k-1} = v_k q_{k+1} + v_{k+1} \quad \text{με} \quad v_{k+1} = 0 \text{ ή } d(v_{k+1}) < d(v_k).$$

Επειδή $d(v_1) > d(v_2) > d(v_3) > \dots$ για κάποιο k θα είναι $v_k = 0$. Αν $v_j \neq 0$ για $j < k$, τότε

$$\mu.χ.δ.(a, \beta) = v_{k-1}$$

Απόδειξη. Αν $v_1 = 0$, τότε β/a και $\mu.χ.δ.(a, \beta) = \beta$. Έστω $v_1 \neq 0$, οπότε $v_1 = a - \beta q_1$. Κάθε διαιρέτης των a, β είναι διαιρέτης του v_1 , συνεπώς των β, v_1 και αντίστροφα λόγω της (1). Έτσι

$$\begin{aligned} & \mu.χ.δ.(a, \beta) = \mu.χ.δ.(\beta, v_1) \\ \text{όμοια} \quad & \mu.χ.δ.(\beta, v_1) = \mu.χ.δ.(v_1, v_2) \\ & \dots\dots\dots = \dots\dots\dots \\ & \mu.χ.δ.(v_{k-2}, v_{k-1}) = v_{k-1} \quad , \quad \text{γιατί} \quad v_{k-2} = v_{k-1}q_{k-1} + 0. \quad \square \end{aligned}$$

Παράδειγμα 1. Έστω ο Ευκλείδειος δακτύλιος των ακεραίων $\mathbb{Z}$ με στάθμη $|\cdot|$. Να βρεθεί ο $\mu.χ.δ.$ των ακεραίων 1085 και 490. Ο Ευκλείδειος αλγόριθμος είναι

$$\begin{aligned} 1085 &= 490 \cdot 2 + 105 \\ 490 &= 105 \cdot 4 + 70 \\ 105 &= 70 \cdot 1 + 35 \\ 70 &= 35 \cdot 2 + 0, \quad \text{άρα } \mu.χ.δ.(1085, 490) = 35. \end{aligned}$$

Παράδειγμα 2. Στο δακτύλιο $\mathbb{Q}[x]$ δίνονται τα πολυώνυμα $a(x) = x^5 + x^4 - x^3 - x^2 - x + 1$, $\beta(x) = x^3 + x^2 + x + 1$. Βρείτε το $\mu.χ.δ.$ των $a(x), \beta(x)$. Ο Ευκλείδειος αλγόριθμος είναι

$$\begin{aligned} a(x) &= \beta(x) \cdot (x^2 - 2) + (x + 1) \\ \beta(x) &= (x + 1) \cdot (x^2 + 1) + 0, \quad \text{άρα } \mu.χ.δ.(a(x), \beta(x)) = x + 1. \end{aligned}$$

Παράδειγμα 3. Βρείτε το $\mu.χ.δ.$ των $a = 11 + 7i$, $\beta = 3 + 7i$ στο δακτύλιο του Gauss $\mathbb{Z}[i]$. Έχουμε

$$\begin{aligned} a &= \beta(1 - i) + (1 + 3i) \quad , \quad d(1 + 3i) = 10 < d(\beta) = 58 \\ \beta &= (1 + 3i) \cdot 2 + (1 + i) \quad , \quad d(1 + i) = 2 < d(1 + 3i) = 10 \\ 1 + 3i &= (1 + i)(2 + i) \end{aligned}$$

Άρα $\mu.χ.δ.(11 + 7i, 3 + 7i) = 1 + i$. Εξ'άλλου $1 + i = 2a + (3 - 2i)\beta$.

4. ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ

Ορισμός 1. Έστω $a_1, a_2, \dots, a_n$ στοιχεία $\neq 0$ ενός μοναδιαίου αντιμεταθετικού δακτυλίου A . Ένα στοιχείο m θα λέγεται **κοινό πολλαπλάσιο** των a_i , αν

$$a_i/m, \quad i = 1, 2, \dots, n$$

Θα λέγεται **ελάχιστο κοινό πολλαπλάσιο**, αν

i) $a_i/m, (i = 1, 2, \dots, n)$

ii) $a_i/m', (i = 1, 2, \dots, n) \Rightarrow m/m'$

Γράφουμε τότε $m = \text{ε.κ.π.} (a_1, a_2, \dots, a_n)$ ή $m = [a_1, a_2, \dots, a_n]$.

Θεώρημα 1. Έστω A ένας κύριος δακτύλιος και $a_1, a_2, \dots, a_n \in A$, $a_i \neq 0$. Υπάρχει ένα ελάχιστο κοινό πολλαπλάσιο m των a_i και μάλιστα

$$mA = a_1A \cap a_2A \cap \dots \cap a_nA$$

Απόδειξη. Προφανώς $mA \subseteq a_iA$, συνεπώς $m = a_i x_i$ με $x_i \in A$. Δηλαδή το m είναι κοινό πολλαπλάσιο των a_i . Έστω $m' \in A$ τέτοιο, ώστε a_i/m' . Τότε

$$m' = a_i y_i \text{ με } y_i \in A, \text{ συνεπώς } m' \in \cap_1^n a_i A \text{ και}$$

$$m'A \subseteq \cap_1^n a_i A, \text{ δηλαδή } m'A \subseteq mA, \text{ άρα } m/m'.$$

□

Το παρακάτω θεώρημα μας δίνει τη σχέση ενός ε.κ.π. και ενός μ.κ.δ. δύο στοιχείων.

Θεώρημα 2. Έστω a, β δύο στοιχεία $\neq 0$ μιας αθέριμης περιοχής A και m ένα ελάχιστο κοινό πολλαπλάσιο των a, β . Τότε υπάρχει ένας μ.κ.δ. d των a, β τέτοιος, ώστε

$$md = a\beta$$

Απόδειξη. Προφανώς $m/a\beta$. Θ' αποδείξουμε ότι $\frac{a\beta}{m}$ είναι ένας μ.κ.δ. (a, β) .

Έστω $d = \frac{a\beta}{m}$. Έχουμε $\beta/m, a\beta/am, dm/am$, συνεπώς d/a . Όμοια d/β . Έστω $d'/a, d'/\beta$. Τότε $a = xd', \beta = yd'$ με $x, y \in A$. Συνεπώς a/xyd' και β/xyd' , οπότε m/xyd' και

$$d' \left(\frac{xyd'}{m} \right) = \frac{d'x d'y}{m} = \frac{a\beta}{m} = d$$

δηλαδή d'/d . Άρα d είναι ένας μ.κ.δ. των a, β .

□

ΑΣΚΗΣΕΙΣ

1. Ν' αποδείξετε ότι οι παρακάτω δακτύλιοι είναι κύριοι δακτύλιοι:

- α) $\mathbb{Z}_m$
 β) $\{\frac{m}{2^n}; m \in \mathbb{Z}, n \in \mathbb{N}\}$, υποδακτύλιος του $(\mathbb{Q}, +, \cdot)$
 γ) $\mathbb{Z}[\frac{1}{p}] = \{a_0 + \frac{a_1}{p} + \dots + \frac{a_n}{p^n}; a_i \in \mathbb{Z}\}$, p πρώτος.

2. Δείξτε ότι το ιδεώδες του δακτυλίου $\mathbb{Z}[\sqrt{-5}] = \{a + \beta\sqrt{-5}; a, \beta \in \mathbb{Z}\}$ που παράγεται από τα στοιχεία $2, 1 + \sqrt{-5}$ δεν είναι κύριο.

3. Ν' αποδειχτεί ότι το ιδεώδες J του $\mathbb{Z}[x]$ που περιέχει τα πολυώνυμα $f \in \mathbb{Z}[x]$ με σταθερό όρο άρτιο ακέραιο, δεν είναι κύριο. (Να παρατηρήσετε ότι $\pm 1 \notin J, J \neq \langle 2 \rangle, \pm 2 \neq x + 2$).

4. Δείξτε ότι $2 + \sqrt{3}$ είναι μια ενάδα του δακτυλίου $\mathbb{Z}[\sqrt{3}] = \{a + \beta\sqrt{3}; a, \beta \in \mathbb{Z}\}$ και να συμπεράνετε ότι ο δακτύλιος έχει άπειρες ενάδες.

5. Έστω $j = \frac{-1 + \sqrt{3}i}{2}$, $\mathbb{Z}[j] = \{a + \beta j; a, \beta \in \mathbb{Z}\}$. Δείξτε ότι

- i) $\mathbb{Z}[j]$ είναι υποδακτύλιος του $\mathbb{Z}$.
 ii) Είναι μάλιστα Ευκλείδειος δακτύλιος.
 iii) Οι ενάδες του $\mathbb{Z}[j]$ είναι $\pm 1, \pm j, \pm j^2$.
 iv) Το στοιχείο $1 - j/3$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}[j]$.

6. Δείξτε ότι οι παρακάτω δακτύλιοι είναι Ευκλείδαιοι και βρείτε τις ενάδες.

$$i) \quad \mathbb{Z}[\sqrt{-2}] \qquad ii) \quad \mathbb{Z}\left[\frac{-1 + \sqrt{3}}{2}\right]$$

Το 43 είναι πρώτο στοιχείο των δακτυλίων αυτών;

7. Βρείτε τα συνδεδεμένα στοιχεία του $a = 2x^3 + x$ στο δακτύλιο $\mathbb{Z}_5[x]$.

8. Βρείτε του διαιρέτες του πολυωνύμου

- 1) $f = x^4 - 4 \in \mathbb{Q}[x]$
 2) $g = x^4 - 5x^2 + 6$ στους δακτυλίους $\mathbb{Q}[x]$ και $\mathbb{R}[x]$.

9. Βρείτε τους διαιρέτες στο δακτύλιο $\mathbb{Z}_3[x]$ των πολυωνύμων

$$i) \quad x^3 + x + 1, \qquad ii) \quad x^3 + x + 2$$

10. Έστω A ένας δακτύλιος. Για κάθε στοιχείο $a \in A$ ορίζουμε ένα εσωτερικό νόμο $\langle a \rangle$ ως εξής: $x \langle a \rangle y = xay$.

- i) Δείξτε ότι $(A, +, \langle a \rangle)$ είναι δακτύλιος.

- ii) Έστω ότι ο A είναι αντιμεταθετικός και μοναδιαίος. Αν τα a, β είναι συνδεδεμένα, δείξτε ότι οι δακτύλιοι $(A, +, < a >)$, $(A, +, < \beta >)$ είναι ισόμορφοι.
 iii) $(\mathbb{Z}_m, +, < \bar{a} >) \cong (\mathbb{Z}_m, +, < \bar{\beta} >)$ τότε και μόνο, όταν τα $\bar{a}, \bar{\beta}$ είναι συνδεδεμένα.

11. Σε κάθε αντιμεταθετικό δακτύλιο R το άθροισμα δύο κυρίων ιδεωδών $(a), (\beta)$ είναι $(a) + (\beta) = (a, \beta)$.

12. Έστω K ένα σώμα αντιμεταθετικό και A ο δακτύλιος πηλίκο $K[x, y]/(x^2, xy, y^2)$.

- i) Δείξτε ότι κάθε στοιχείο του A είναι της μορφής $a = a + \beta x + \gamma y$ με $a, \beta, \gamma \in K$.
 Αν $a, b \in A$, βρείτε το άθροισμα $a + b$ και το γινόμενο $a \cdot b$.
 ii) Δείξτε ότι το στοιχείο a με $a \neq 0$ αντιστρέφεται και βρείτε το αντίστροφό του.
 iii) Δείξτε ότι τα ιδεώδη που παράγονται από τα στοιχεία $\beta x + \gamma y$ (β, γ όχι και τα δύο μηδέν) είναι κύρια ιδεώδη.

13. Βρείτε το μ.κ.δ των ακεραίων αριθμών

- i) $a = 1505, \beta = 2520$ ii) $a = 4148, \beta = 7684$
 iii) των ακεραίων Gauss $15 + 12i, 3 - 9i$ στο $\mathbb{Z}[i]$.

14. Βρείτε το μ.κ.δ των πολυωνύμων

- i) $x^4 - 1, x^5 - x^4 + x^3 - x^2$
 ii) $nx^{n+1} - (n+1)x^n + 1, x^n - nx + n - 1$

15. Έστω $a = x^5 + x^4 + i, \beta = x^5 + x + i \in \mathbb{Z}_2[x]$. Βρείτε το μ.κ.δ(a, β) και γράψτε τον υπό τη μορφή $fa + g\beta$ με $f, g \in \mathbb{Z}_2[x]$ και $d^\circ(g) \leq 2$.

16. Έστω p ένας πρώτος ακέραιος. Δείξτε ότι

- α) Αν $p \equiv 3 \pmod{4}$, ο p είναι ανάγωγο στοιχείο του $\mathbb{Z}[i]$.
 β) Αν $p \equiv 1 \pmod{4}$, ο p είναι γινόμενο δύο διαφόρων στοιχείων του $\mathbb{Z}[i]$.
 γ) Αν $p = 2$, τότε $p = ia^2$, όπου a ανάγωγο στοιχείο του $\mathbb{Z}[i]$.

17. Δείξτε ότι τα πολυώνυμα $P = x^7 - x - 1, Q = x^5 + 1$ του δακτυλίου $\mathbb{Z}[x]$ είναι σχετικά πρώτα.

18. Δείξτε ότι: i) $(x^m - 1, x^n - 1) = x^d - 1$, όπου $d = (m, n)$.
 ii) $(x^m, (1 - x)^n) = 1$.

19. Έστω δύο πολυώνυμα $f = x^5 + x^4 + \bar{1}, g = x^5 + x + \bar{1}$ του $\mathbb{Z}_2[x]$. Βρείτε το μ.κ.δ(f, g) και $a, \beta \in \mathbb{Z}_2[x]$, ώστε $\mu.κ.δ(f, g) = af + \beta g$.

20. Ν' αποδείξετε ότι οι αριθμοί $\sqrt[3]{4}, \sqrt{2}/\sqrt[3]{5}$ είναι άρρητοι.

21. Ν' αποδείξετε ότι το πολυώνυμο $x^3 + x + 1$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_2[x]$ και δείξτε ότι το πηλίκο $\mathbb{Z}_2[x]/(x^3 + x + 1)$ είναι ένα σώμα με 2^6 στοιχεία.

22. Βρείτε όλους τους υποδακτυλίου του $\mathbb{Q}$. Προς τούτο

- 1) Δείξτε ότι κάθε υποδακτύλιος, που περιέχει το ανάγωγο κλάσμα $\frac{p}{q}$, περιέχει το κλάσμα $\frac{1}{q}$.
- 2) Θεωρείστε ένα σύνολο P πρώτων αριθμών και τον υποδακτύλιο $A(P)$ του $\mathbb{Q}$ που αποτελείται από τα ανάγωγα κλάσματα των οποίων ο παρονομαστής έχει τους πρώτους παράγοντες στο P .
- 3) Θεωρείστε ένα υποδακτύλιο A του $\mathbb{Q}$ και το σύνολο $P(A)$ των πρώτων παραγόντων των παρονομαστών των αναγώγων κλασμάτων του A και δείξτε ότι $A(P(A)) = A$.

11

Πεδία μονοσήμαντης παραγοντοποίησης

Η μονοσήμαντη ανάλυση ενός στοιχείου δακτυλίου σε γινόμενο αναγώγων στοιχείων είναι μια έννοια χρήσιμη και λεπτή. Δεν είναι δυνατή σε οποιοδήποτε δακτύλιο. Υπάρχει η εικασία ότι ο Fermat κατά την απόδειξη του περίφημου θεωρήματός του, η οποία δεν βρέθηκε, είχε χρησιμοποιήσει δακτυλίους στους οποίους υπέθεσε ότι ισχύει η ανάλυση αυτή, πλάνη στην οποία υπέπεσαν π.χ. οι Kummer και Euler.

1. ΔΑΚΤΥΛΙΟΙ ΜΟΝΟΣΗΜΑΝΤΗΣ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗΣ

Ορισμός 1. Ένας δακτύλιος A θα λέγεται δακτύλιος μονοσήμαντης παραγοντοποίησης, αν είναι αχέραια περιοχή και ισχύουν οι παρακάτω προτάσεις (α) , (β) :

α) Κάθε στοιχείο $x \neq 0$ του A γράφεται σαν γινόμενο της μορφής

$$x = u p_1 p_2 \cdots p_n \quad (n \geq 0) \quad (1)$$

όπου u ένα αντιστρέψιμο στοιχείο του A και p_j ανάγωγα στοιχεία του A .

β) Αν το x γράφεται σαν γινόμενο της μορφής (1) και της μορφής

$$x = vq_1q_2 \cdots q_m \quad (2)$$

όπου v αντιστρέψιμο στοιχείο του A και q_i ανάγωγα στοιχεία αυτού, τότε $n = m$ και με αλλαγή σειράς των q_i στην (2) το x γράφεται

$$x = vq'_1q'_2 \cdots q'_n$$

έτσι, ώστε τα p_j, q'_j να είναι συνδεδεμένα ($j = 1, 2, \dots, n$).

Ο δακτύλιος των ακεραίων είναι δακτύλιος μονοσήμαντης παραγοντοποίησης. Ο Kummer το 1835 υπέθεσε ότι ο δακτύλιος

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_r\zeta^r ; a_i \in \mathbb{Z}, r \geq 1\}$$

όπου ζ γεννήτορας της ομάδας των ριζών της εξίσωσης $x^p = 1$ ($p =$ περιττός πρώτος) είναι δακτύλιος μονοσήμαντης παραγοντοποίησης και απέδειξε το θεώρημα του Fermat, ότι $x^p + y^p = z^p$ δεν έχει ακέραιες λύσεις. Αλλά ο Dirichlet απέδειξε ότι αυτή η υπόθεση του Kummer ήταν λάθος. Στην προσπάθεια τους οι Kummer και Dedekind να καλύψουν το κενό της απόδειξης του θεωρήματος του Fermat εισήγαγαν την έννοια του ιδεώδους, ανοίγοντας το δρόμο στη σύγχρονη θεωρία δακτυλίων.

Αναφέρουμε στη συνέχεια παράδειγμα δακτυλίου, ο οποίος δεν είναι δακτύλιος μονοσήμαντης παραγοντοποίησης οφειλόμενο στο Dedekind.

Παράδειγμα 1. Έστω $\mathbb{Z}[\omega] = \{a + b\omega ; a, b \in \mathbb{Z}, \omega = \sqrt{-5}\}$. Είναι εύκολο να επαληθεύσουμε ότι $\mathbb{Z}[\omega]$ είναι υποδακτύλιος του $\mathbb{C}$. Στο δακτύλιο $\mathbb{Z}[\omega]$ έχουμε $6 = 2 \cdot 3 = (1 - \omega)(1 + \omega)$. Θ' αποδείξουμε ότι τα στοιχεία $2, 3, 1 - \omega, 1 + \omega$ είναι ανάγωγα, οπότε ο $\mathbb{Z}[\omega]$ δεν είναι δακτύλιος μονοσήμαντης παραγοντοποίησης, αφού ο 6 θα γράφεται κατά δύο τρόπους σαν γινόμενο αναγώγων στοιχείων. Έστω

$$2 = (x + y\omega)(u + v\omega) \quad , \quad x, y, u, v \in \mathbb{Z}.$$

Τότε $4 = 2 \cdot 2 = (x^2 + y^2 \cdot 5)(u^2 + v^2 \cdot 5)$. Αν $x^2 + y^2 \cdot 5 = 1$, θα είχαμε $y = 0$ και $x = \pm 1$, οπότε $u^2 + 5v^2 = 4$, $v = 0$ και $u = \pm 2$, δηλαδή οι διαιρέτες του 2 θα είναι ή ενάδες ή $2u$ με u ενάδα. Άρα το 2 θα είναι ανάγωγο στοιχείο.

Όμοια και ο 3. Αν $1 + \omega = (x + y\omega)(u + v\omega)$, θα είχαμε $6 = 1 - \omega^2 = (x^2 + 5 \cdot y^2)(u^2 + 5v^2)$. Εύκολα φαίνεται ότι ο ένας παράγοντας πρέπει να

είναι ο 2 και ο άλλος 3, πράγμα αδύνατο. 'Αρα $1 + \omega$ είναι ανάγωγο. 'Ομοια και το $1 - \omega$.

Παρατήρηση. Ο δακτύλιος $\mathbb{Z}[\omega]$ δεν είναι κύριος σύμφωνα με το θεώρημα που ακολουθεί.

Θεώρημα 1. Σε κάθε κύριο δακτύλιο A κάθε στοιχείο $x \neq 0$, το οποίο δεν αντιστρέφεται στον A , είναι γινόμενο αναγώγων στοιχείων.

Απόδειξη. Θ' αποδείξουμε κατ' αρχήν ότι το x έχει ένα ανάγωγο παράγοντα. Αν το x είναι ανάγωγο, ισχύει. Έστω ότι το x δεν είναι ανάγωγο. Τότε $x = a_1\beta_1$ με a_1, β_1 μη αντιστρέψιμα. Συνεπώς $(x) \subseteq (a_1)$. Θ' αποδείξουμε ότι

$$(x) \subset (a_1) \quad (1)$$

Αν $(x) = (a_1)$, θα είχαμε $a_1 = vx$ με $v \in A$, οπότε

$$x = a_1\beta_1 = vx\beta_1 = v\beta_1x$$

ή $1 = v\beta_1$, πράγμα άτοπο, αφού το β_1 δεν είναι αντιστρέψιμο. Παίρνοντας το a_1 και επαναλαμβάνοντας την ίδια εργασία βρίσκουμε μια γνήσια αύξουσα ακολουθία ιδεωδών

$$(x) \subset (a_1) \subset (a_2) \subset \dots$$

Σύμφωνα με το θεώρ.2§2, Κεφ.10, πρέπει να είναι σταθερή. 'Αρα υπάρχει κάποιο a_m , το οποίο είναι ανάγωγο. Το a_m προφανώς είναι παράγοντας του x .

Έτσι το x είναι ανάγωγο ή $x = p_1d_1$, όπου p_1 είναι ανάγωγο και d_1 μη αντιστρέψιμο. Έχουμε την ανάλογη σχέση της (1):

$$(x) \subset (d_1).$$

Αν το d_1 δεν είναι ανάγωγο, τότε $d_1 = p_2d_2$ για ένα ανάγωγο στοιχείο p_2 και ένα μη αντιστρέψιμο στοιχείο d_2 . Συνεχίζοντας βρίσκουμε μια γνήσια αύξουσα ακολουθία ιδεωδών

$$(x) \subset (d_1) \subset (d_2) \subset \dots$$

Σύμφωνα πάλι με το θεώρ.2§2, Κεφ.10 πρέπει η ακολουθία να τερματίζεται. 'Αρα κάποιο d_k είναι ανάγωγο, δηλαδή $x = p_1p_2 \dots p_kd_k$. $\square$

Θεώρημα 2. Κάθε κύριος δακτύλιος είναι δακτύλιος μόνοςήμαντης παραγοντοποίησης.

Απόδειξη. Έστω A ένας κύριος δακτύλιος. Σύμφωνα με το προηγούμενο θεώρημα κάθε $x \in A - \{0\}$ θα αντιστρέφεται ή θα γράφεται σαν γινόμενο αναγώνων στοιχείων. Μένει ν' αποδείξουμε τη μοναδικότητα, όπως στον ορισμό 1. Έστω ότι $x = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ με p_i, q_j ανάγωγα στοιχεία. Τότε $p_1/q_1 q_2 \cdots q_m$, οπότε p_1/q_i για κάποιο $i \in \{1, 2, \dots, m\}$. Αλλάζοντας την αρίθμηση των $q_1, q_2, \dots, q_m$ μπορούμε να υποθέσουμε ότι p_1/q_1 . Έστω $q_1 = p_1 u_1$. Αφού το q_1 είναι ανάγωγο, το u_1 είναι αντιστρέψιμο. Έτσι τα p_1, q_1 είναι συνδεδεμένα. Έχουμε συνεπώς $x = p_1 p_2 \cdots p_n = p_1 u_1 q_2 \cdots q_m$, απ' όπου

$$p_2 \cdots p_n = u_1 q_2 \cdots q_m$$

Συνεχίζοντας με το p_2 κ.λ.π. φθάνουμε σε μια σχέση

$$1 = u_1 u_2 \cdots u_n q_{n+1} \cdots q_m$$

Αφού τα q_j είναι ανάγωγα, έχουμε $n = m$. Γιατί στην αντίθετη περίπτωση ανάγωγο στοιχείο θα ήταν αντιστρέψιμο. $\square$

Το θεώρημα ισχύει και στους Ευκλείδειους δακτύλιους:

Θεώρημα 3. Κάθε Ευκλείδειος δακτύλιος είναι δακτύλιος μονοσήμαντης παραγοντοποίησης.

Απόδειξη. Έστω A ένας Ευκλείδειος δακτύλιος με στάθμη d . Κάνουμε επαγωγή επί του $d(a)$, $a \in A$. Η ελάχιστη τιμή του $d(a)$ είναι $d(1)$. Έστω $d(a) = d(1)$. Σύμφωνα με το θεώρ.1§1, Κεφ.10, το a αντιστρέφεται. Η υπόθεση της επαγωγής είναι ότι κάθε x με $d(x) < d(a)$ είναι αντιστρέψιμο ή γινόμενο αναγώνων στοιχείων του A . Θ' αποδείξουμε το ίδιο για το a . Αν το a δεν είναι ανάγωγο, θα έχουμε $a = \beta\gamma$, όπου β, γ μη αντιστρέψιμα. Τότε $d(\beta) < d(a)$, $d(\gamma) < d(a)$, συνεπώς τα β, γ είναι γινόμενα αναγώνων στοιχείων του A . Άρα και το a .

Η μοναδικότητα προκύπτει, όπως στο προηγούμενο θεώρημα. $\square$

Παράδειγμα 2. Ο δακτύλιος $\mathbb{Z}[\omega]$ με $\omega = i\sqrt{5}$ δεν είναι Ευκλείδειος. Γιατί δεν είναι δακτύλιος μονοσήμαντης παραγοντοποίησης (παράδ.1§3).

2. ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΣΤΟΥΣ ΔΑΚΤΥΛΙΟΥΣ $\mathbb{Q}[x], \mathbb{Z}[x]$

Λήμμα Gauss. Αν ένα πολυώνυμο $P \in \mathbb{Q}[x]$ αναλύεται σε γινόμενο δύο πολυωνύμων του $\mathbb{Q}[x]$, θα αναλύεται και σε γινόμενο δύο πολυωνύμων του $\mathbb{Z}[x]$.

Απόδειξη. Έστω $P(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$ και ότι $P(x) = p(x)q(x)$ με $p(x), q(x) \in \mathbb{Q}[x]$. Θεωρούμε τους ρητούς συντελεστές του $p(x)$ και το ε.κ.π. των παρονομαστών, έστω m . Τότε $p(x) = \frac{1}{m}\bar{p}(x)$, όπου $\bar{p}(x) \in \mathbb{Z}[x]$.

Έστω d ο μ.κ.δ. των συντελεστών του $\bar{p}(x)$. Τότε $p(x) = \frac{d}{m}B(x)$, όπου $B(x) \in \mathbb{Z}[x]$ και ο μ.κ.δ. των συντελεστών του A είναι 1. Γράφουμε το $q(x)$ με τον ίδιο τρόπο, $q(x) = \frac{t}{s}\Gamma(x)$. Τότε

$$P(x) = \frac{dt}{ms}B(x)\Gamma(x) \quad \text{και} \quad msP(x) = dtB(x)\Gamma(x).$$

Έστω $B(x) = \beta_0 + \dots + \beta_k x^k$, $\Gamma(x) = \gamma_0 + \dots + \gamma_p x^p$. Έστω p ένας πρώτος αριθμός ακέραιος. Επειδή $\mu.κ.δ.(\beta_0, \dots, \beta_k) = 1$, ο p δεν διαιρεί όλους τους συντελεστές. Έστω ότι $p/\beta_0, \dots, \beta_i, p \nmid \beta_{i+1}$. Όμοια, έστω $p/\gamma_0, \dots, \gamma_j, p \nmid \gamma_{j+1}$. Ο συντελεστής του x^{i+j} στο γινόμενο $B(x)\Gamma(x)$ είναι

$$\beta_{i+j}\gamma_0 + \beta_{i+j-1}\gamma_1 + \dots + \beta_{i+1}\gamma_{j-1} + \beta_i\gamma_j + \dots + \beta_0\gamma_{j+i}$$

Επειδή $p/\gamma_0, \dots, \gamma_{j-1}, p/\beta_i, \dots, \beta_0$ και $p/\beta_i\gamma_j$ ο συντελεστής του x^{i+j} δεν διαιρείται με p . Συνεπώς ο μ.κ.δ. των συντελεστών του $B(x)\Gamma(x)$ είναι 1.

Άρα ms/dt και το πολυώνυμο $\frac{dt}{ms}B(x) \in \mathbb{Z}[x]$, δηλαδή το $P(x)$ αναλύεται σε γινόμενο δύο πολυωνύμων στο δακτύλιο $\mathbb{Z}[x]$. $\square$

Κριτήριο Eisenstein. Έστω $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{Z}[x]$. Αν υπάρχει πρώτος p τέτοιος, ώστε

- i) $p/a_0, a_1, \dots, a_{n-1}$
- ii) $p \nmid a_n$
- iii) $p^2 \nmid a_0$

το πολυώνυμο $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Απόδειξη. Έστω ότι το $f(x)$ δεν είναι ανάγωγο. Κατά το λήμμα Gauss θα είναι γινόμενο δύο πολυωνύμων του $\mathbb{Z}[x]$,

$$f(x) = (\beta_0 + \beta_1x + \dots + \beta_kx^k)(\gamma_0 + \gamma_1x + \dots + \gamma_px^p)$$

με $\beta_i, \gamma_j \in \mathbb{Z}$, $k+p=n$. Προφανώς $a_0 = \beta_0\gamma_0$. Το p δεν διαιρεί και τους δύο συντελεστές β_0, γ_0 , γιατί τότε p^2/a_0 . Έστω ότι $p/\beta_0, p \nmid \gamma_0$. Το p δεν διαιρεί επίσης όλους τους συντελεστές $\beta_0, \beta_1, \dots, \beta_k$, γιατί θα διαιρούσε και τον a_n . Έστω i ο μικρότερος ακέραιος για τον οποίο $p \nmid \beta_i$ ($1 \leq i \leq k < n$). Τότε

$$a_i = \beta_i\gamma_0 + \beta_{i-1}\gamma_1 + \dots + \beta_1\gamma_{i-1} + \beta_0\gamma_i$$

όπου $p/a_i, p/\beta_0, \beta_1, \dots, \beta_{i-1}$. Συνεπώς $p/\beta_i \gamma_0$. Αλλά $p \neq \beta_i, p \neq \gamma_0$ και άρα $p \neq \beta_i \gamma_0$, δηλαδή καταλήξαμε σε άτοπο. $\square$

Παράδειγμα 1. Το πολυώνυμο $f(x) = x^5 - 2$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Γιατί, $f(x) = -2 + x^5$, ο 2 είναι πρώτος και διαιρεί όλους τους συντελεστές εκτός του συντελεστή του x^5 , καθώς ο $2^2 \nmid (-2)$. Κατά το κριτήριο Eisenstein, το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

Παράδειγμα 2. Για κάθε πρώτο p το πολυώνυμο $\phi(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Το πολυώνυμο αυτό λέγεται κυκλοτομικό πολυώνυμο.

Πραγματικά, έχουμε $\phi(x) = \frac{x^p - 1}{x - 1}$ και

$$\phi(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \dots + \frac{p(p-1)}{2!}y + p$$

Έτσι ο p διαιρεί όλους τους συντελεστές του $\phi(y+1)$ εκτός του κύριου συντελεστή, και ο p^2 δεν διαιρεί το σταθερό όρο. Ισχύει συνεπώς το κριτήριο Eisenstein και το $\phi(y+1)$ είναι ανάγωγο επί του $\mathbb{Q}[y]$, άρα και το $\phi(x)$ επί του $\mathbb{Q}[x]$.

3. ΜΟΝΟΣΗΜΑΝΤΗ ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ ΣΤΟΝ $A[x]$.

Θεώρημα 1. Αν A είναι ένας δακτύλιος μονοσήμαντης παραγοντοποίησης, ο δακτύλιος των πολυωνύμων $A[x]$ είναι επίσης δακτύλιος μονοσήμαντης παραγοντοποίησης

Απόδειξη. Θ' αποδείξουμε ότι κάθε $f \in A[x]$ δέχεται μια ανάλυση σε γινόμενο ανάγωγων στοιχείων μονοσήμαντη. Αν $d^\circ(f) = 0$, αυτό ισχύει, γιατί $f \in A$. Έστω $d^\circ(f) \geq 1$. Έστω K το σώμα κλασμάτων του A . Ο δακτύλιος $K[x]$ είναι κύριος, συνεπώς είναι δακτύλιος μονοσήμαντης παραγοντοποίησης. Το $f \in K[x]$. Συνεπώς δέχεται μια μοναδική ανάλυση σε γινόμενο ανάγωγων στοιχείων του $K[x]$.

$$f = a \prod g^{n(g)}$$

όπου $a \in K - \{0\}$, $n(g)$ ακέραιοι ≥ 0 , $g \in K[x]$. Υπάρχει $m(g) \in A - \{0\}$, τέτοιο, ώστε $m(g)g = q \in A[x]$. Το $m(g)$ είναι αντιστρέψιμο στο K , συνεπώς το q είναι ανάγωγο στο $K[x]$, άρα και στο $A[x]$. Θέτουμε $q = c(q)q'$, όπου q' πολυώνυμο του $A[x]$ με μ.κ.δ. των συντελεστών 1.

Έστω $m = \prod m(g)$. Έχουμε

$$f \cdot m = a \prod c(q) \prod q' n(q')$$

και θέτοντας $f = c(f)f'$, παίρνουμε

$$c(f)mf' = \left(a \prod c(q)\right) \prod q' n(q')$$

οπότε

$$c(f)m = a \prod c(q)$$

και $f = c(f) \prod q' n(q')$.

Αφού ο A είναι δακτύλιος μονοσήμαντης παραγοντοποίησης, $c(f) = u \prod p^{m(p)}$ με u ανάγωγο και p επίσης ανάγωγο στοιχείο του A και $m(p) \neq 0$ για πεπερασμένο πλήθος στοιχείων p . Έχουμε συνεπώς την ανάλυση του f σε γινόμενο ανάγωγων στοιχείων

$$f = u \prod p^{m(p)} \prod g^{n(g)}$$

Η μοναδικότητα προκύπτει από τη μοναδικότητα της ανάλυσης στους δακτύλιους $A, K[x]$, που συνεπάγεται τη μοναδικότητα των $m(p), n(g)$. $\square$

Πόρισμα. Αν A είναι δακτύλιος μονοσήμαντης παραγοντοποίησης και ο δακτύλιος $A[x_1, x_2, \dots, x_n]$ θα είναι δακτύλιος μονοσήμαντης παραγοντοποίησης.

Γιατί $A[x_1]$ είναι δακτύλιος μονοσήμαντης παραγοντοποίησης, συνεπώς και ο $A[x_1][x_2] = A[x_1, x_2]$, καθώς και ο $A[x_1, x_2][x_3] = A[x_1, x_2, x_3]$ κ.ο.κ. $\square$

ΑΣΚΗΣΕΙΣ

1. Ν' αναλύσετε τα στοιχεία $12 + i$, $6 + 2i$, $3 + 5i$ του δακτυλίου $\mathbb{Z}[i]$ σε γινόμενο πρώτων παραγόντων.

2. Το πολυώνυμο $x + \bar{3} \in \mathbb{Z}_{10}[x]$ αναλύεται σε γινόμενο δυο πρωτοβάθμιων πολυωνύμων του $\mathbb{Z}_{10}[x]$;

3. Έστω K, K' δύο σώματα. Ο δακτύλιος $K \times K'$ είναι δακτύλιος μονοσήμαντης παραγοντοποίησης;

4. Ν' αποδείξετε ότι ο δακτύλιος $\mathbb{Z}[\sqrt{3}]$ δεν είναι δακτύλιος μονοσήμαντης παραγοντοποίησης ($4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$).

5. Δείξτε ότι το πολυώνυμο $x^4 + 15x^3 + 7$ είναι ανάγωγο στο $\mathbb{Z}_5[x]$. Είναι ανάγωγο στους δακτυλίους $\mathbb{Z}[x], \mathbb{Q}[x]$;

6. Ν' αποδείξετε ότι: i) κάθε στοιχείο του $\mathbb{Z}[\sqrt{-5}]$ είναι γινόμενο ανάγωγων στοιχείων.

ii) Τα ιδεώδη $I = (2, 1 + \sqrt{-5})$, $J = (3, 1 + \sqrt{-5})$, $K = (3, 1 - \sqrt{-5})$ είναι πρώτα και όχι κύρια.

iii) $(6) = I^2 JK$.

7. Δείξτε ότι το πολυώνυμο $x^3 - 4x + 6$ είναι ανάγωγο στο δακτύλιο $\mathbb{Q}[x]$.

8. Δείξτε ότι τα παρακάτω πολυώνυμα είναι ανάγωγα στο δακτύλιο $\mathbb{Q}[x]$. i) $x^4 + 5x^3 + 10x^2 + 10x + 5$ ii) $x^4 + x^3 + x^2 + x + 1$

9. Όμοια το πολυώνυμο $25x^5 - 9x^4 + 3x^2 - 12 \in \mathbb{Q}[x]$ είναι ανάγωγο.

10. Αν το 2 είναι ανάγωγο στοιχείο του δακτυλίου $\mathbb{Z}[\sqrt{n}]$, ν' αποδείξετε ότι ο δακτύλιος αυτός δεν είναι πεδίο μονοσήμαντης παραγοντοποίησης.

12 | Ρίζες πολυωνύμου

Μια από τις πλέον ενδιαφέρουσες ιδιότητες των πολυωνύμων του δακτυλίου $A[x]$ είναι η "αντικατάσταση" του x με κάποιο στοιχείο ρ του A ή ενός αντιμεταθετικού μοναδιαίου δακτυλίου S που περιέχει τον A . Έτσι, αν $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ και $\rho \in S$, θέτουμε

$$f(\rho) = a_0 + a_1\rho + \cdots + a_n\rho^n \in A[\rho]$$

Η συνάρτηση $\phi : A[x] \rightarrow A[\rho]$ με τιμή

$$f \mapsto f(\rho) \tag{1}$$

είναι ομομορφισμός των δακτυλίων $A[x]$, $A[\rho]$ και συνεπώς

$$(f + g)(\rho) = f(\rho) + g(\rho) \quad , \quad (f \cdot g)(\rho) = f(\rho) \cdot g(\rho).$$

Προφανώς $\phi(x) = \rho$ και $\phi(a) = a$ για κάθε $a \in A$, δηλαδή ο ομομορφισμός ϕ είναι επέκταση του ταυτοτικού ομομορφισμού $i : a \mapsto a$ του A στον δακτύλιο $A[x]$ έτσι, ώστε $\phi(x) = \rho$. Η ισότητα $\phi(f) = f(\rho)$ γίνεται $\phi(f) = f(\phi(x))$. Παραλείπουμε συνήθως τον ομομορφισμό ϕ και γράφουμε

καταχρηστικά $f = f(x)$. Ο ομομορφισμός ϕ λέγεται ομομορφισμός **εκτίμησης** στο ρ .

1. ΡΙΖΕΣ ΠΟΛΥΩΝΥΜΩΝ

Ορισμός 1. Έστω A ένας μοναδιαίος αντιμεταθετικός δακτύλιος και $f \in A[x]$. Ένα στοιχείο ρ του A λέγεται **ρίζα** του f , αν $f(\rho) = 0$.

Π.χ., αν $f = x^2 + 1 \in \mathbb{Z}_2[x]$, το $\bar{1} \in \mathbb{Z}_2$ είναι ρίζα του f , γιατί $f(\bar{1}) = \bar{1}^2 + \bar{1} = \bar{0}$. Αν $f = x^2 + 1 \in \mathbb{C}[x]$, το $i \in \mathbb{C}$ είναι ρίζα του f , γιατί $i^2 + 1 = (-1) + 1 = 0$.

Θεώρημα 1. Έστω A ένας μοναδιαίος αντιμεταθετικός δακτύλιος, $a \in A$ και $f \in A[x]$.

- i) Το υπόλοιπο της διαίρεσης του $f(x)$ με $x - a$ είναι $f(a)$.
- ii) Το a είναι ρίζα του $f \Leftrightarrow x - a \mid f(x)$.

Απόδειξη. Έστω $q(x)$ και $v(x)$ το πηλίκο και το υπόλοιπο της διαίρεσης του $f(x)$ με $x - a$ στο δακτύλιο $A[x]$. Επειδή $v(x) = 0$ ή $d^0(v) < 1 = d^0(x - a)$, έχουμε $v \in A$. Έτσι $f(x) = (x - a)q(x) + v$. Θέτοντας $x = a$ παίρνουμε $f(a) = 0 \cdot q(a) + v$ ή $f(a) = v$. Αν το a είναι ρίζα του f , έχουμε $v = f(a) = 0$, οπότε $f(x) = (x - a)q(x)$, δηλαδή $x - a \mid f(x)$. Αν $x - a \nmid f(x)$, τότε $f(x) = (x - a)q(x)$ και συνεπώς $f(a) = 0$. $\square$

Ορισμός 2. Έστω A μοναδιαίος αντιμεταθετικός δακτύλιος. Το $a \in A$ λέγεται ρίζα **πολλαπλότητας** $m \geq 1$ του $f \in A[x]$, αν υπάρχει $q \in A[x]$ τέτοιο, ώστε

$$f(x) = (x - a)^m q(x) \quad \text{και} \quad q(a) \neq 0.$$

Προφανώς $(x - a)^m \mid f(x)$, ενώ $(x - a)^{m+1} \nmid f(x)$.

Πραγματικά, αν $(x - a)^{m+1} \mid f(x)$, θα είχαμε $f(x) = (x - a)^{m+1} g(x) = (x - a)^m [(x - a)g(x)]$. Επειδή $q(x), (x - a)g(x) \in A[x]$ και το πηλίκο της διαίρεσης του f με $(x - a)^m$ ορίζεται μονοσήμαντα στο $A[x]$, έχουμε $q(x) = (x - a)g(x)$, συνεπώς $q(a) = 0$, πράγμα άτοπο.

Αντίστροφα, αν $(x - a)^m \mid f(x)$ και $(x - a)^{m+1} \nmid f(x)$, το a είναι ρίζα του f πολλαπλότητας m . Γιατί $f(x) = (x - a)^m q(x)$ με $q(a) \neq 0$, αφού $q(a) = 0$ συνεπάγεται $x - a \mid q(x)$ ή $q(x) = (x - a)\phi(x)$ και $f(x) = (x - a)^{m+1}\phi(x)$, δηλαδή το $(x - a)^{m+1}$ θα διαιρούσε το $f(x)$. Έτσι έχουμε τον ισοδύναμο

Ορισμός 3. Το a λέγεται ρίζα **πολλαπλότητας** $m \geq 1$ του $f(x)$, αν

$$(x - a)^m \mid f(x) \quad \text{και} \quad (x - a)^{m+1} \nmid f(x).$$

Πρόταση 1. Έστω A μια ακέραια περιοχή. Αν $a, \beta \in A$ είναι ρίζες του $f \in A[x]$ πολλαπλότητας m, n και $a \neq \beta$, τότε

$$f(x) = (x - a)^m (x - \beta)^n \pi(x) \quad \text{με} \quad \pi \in A[x].$$

Απόδειξη. Έχουμε $f(x) = (x - a)^m q(x)$ με $q \in A[x]$. Το $(x - a)^m$ δεν διαιρείται με $x - \beta$, γιατί για $x = \beta$ παίρνουμε το υπόλοιπο $(\beta - a)^m \neq 0$, αφού A ακέραια περιοχή. Επειδή $(x - \beta)^n / f(x) = (x - a)^m q(x)$ και $(x - \beta)^k \nmid (x - a)^m$ για $k = 1, 2, \dots, n$ έπεται ότι $(x - \beta)^n / q(x)$. Θέτοντας $q(x) = (x - \beta)^n \pi(x)$ έχουμε $f(x) = (x - a)^m (x - \beta)^n \pi(x)$. $\square$

Πόρισμα 1. Αν A ακέραια περιοχή, $\lambda_1, \lambda_2, \dots, \lambda_k \in A$ ρίζες του $f \in A[x]$ πολλαπλότητας $m_1, m_2, \dots, m_k$, τότε

$$f(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_k)^{m_k} q(x)$$

$$\text{και} \quad d^o(f) \geq m_1 + m_2 + \cdots + m_k \geq k$$

Πόρισμα 2. Το πλήθος των ριζών ενός πολυωνύμου $f \in A[x]$ στην ακέραια περιοχή A είναι $\leq d^o(f)$.

Παράδειγμα 1. Το $f = x^2 + \bar{1} \in \mathbb{Z}_2[x]$, έχει μια μόνο ρίζα στο $\mathbb{Z}_2$, την $a = \bar{1}$, γιατί $f(\bar{1}) = 0$ και $f(\bar{0}) = \bar{1} \neq \bar{0}$. Συνεπώς $x - \bar{1} / x^2 + \bar{1}$, στο δακτύλιο $\mathbb{Z}_2[x]$. Πραγματικά $x^2 + \bar{1} = x^2 - \bar{1} = x^2 - \bar{1}^2 = (x - \bar{1})(x + \bar{1}) = (x - \bar{1})^2$. Παρατηρούμε ότι το $\mathbb{Z}_2$ είναι σώμα και ότι $d^o(f) = 2 = m_1$.

Παράδειγμα 2. Έστω $f = x^2 - 6x \in \mathbb{Z}_8[x]$. Το f δέχεται ως ρίζες τα στοιχεία $\bar{0}, \bar{2}, \bar{4}, \bar{6} \in \mathbb{Z}_8$. Παρατηρούμε ότι $d^o(f) = 2 < k = \text{πλήθος ριζών του } f \text{ στο } \mathbb{Z}_8$ και ότι $\mathbb{Z}_8$ δεν είναι ακέραια περιοχή.

Παράδειγμα 3. Βρείτε τις ρίζες του πολυωνύμου $f = 2x^{210} + 3x^{74} + 2x^{57} + 3x^{44} \in \mathbb{Z}_5[x]$ στο $\mathbb{Z}_5$.

Το πολυώνυμο γράφεται $f(x) = x^{44}(2x^{166} + 3x^{30} + 2x^{13} + 3)$. Το $a = \bar{0} \in \mathbb{Z}_5$ είναι ρίζα πολλαπλότητας 44. Έστω β μια ρίζα του $g(x) = 2x^{166} + 3x^{30} + 2x^{13} + 3$ στο $\mathbb{Z}_5$. Έχουμε $\beta^5 = \beta$ (θεώρημα Fermat). Συνεπώς

$$\beta^{166} = (\beta^5)^{33} \cdot \beta = \beta^{35} = \beta^7 = \beta^2$$

$$\beta^{30} = (\beta^5)^6 = \beta^6 = \beta^2$$

$$\beta^{13} = (\beta^5)^2 \cdot \beta^3 = \beta^2 \cdot \beta^3 = \beta.$$

$$g(\beta) = 2\beta^2 + 3\beta^2 + 2\beta + 3 = 2\beta + 3 = 2(\beta + 4) = 2(\beta - 1)$$

Άρα $g(\beta) = 0$ για $\beta = 1$. Έτσι οι ρίζες του f στο $\mathbb{Z}_5$ είναι το $\bar{0}$ πολλαπλότητας 44 και το $\bar{1}$.

Παράδειγμα 4. Το πολυώνυμο $f = x^2 + 1 \in \mathbb{R}[x]$ δεν έχει ρίζα στο $\mathbb{R}$.

Γιατί, αν $a \in \mathbb{R}$ με $a^2 + 1 = 0$, θα είχαμε $a^2 = -1 < 0$, πράγμα αδύνατο στο $\mathbb{R}$. Όμως υπάρχει σώμα στο οποίο το πολυώνυμο $f(x) = x^2 + 1$ έχει ρίζα, είναι το σώμα των μιγαδικών αριθμών $\mathbb{C}$, το οποίο περιέχει το $\mathbb{R}$.

Το ερώτημα που προκύπτει είναι προφανές: Αν ένα πολυώνυμο $f \in K[x]$ δεν έχει ρίζα στο σώμα K , υπάρχει σώμα το οποίο να περιέχει μια τουλάχιστον ρίζα του f και το σώμα K ;

Η απάντηση στο ερώτημα αυτό είναι καταφατική (βλ. Κεφ.13)

2. ΠΑΡΑΓΩΓΟΣ ΠΟΛΥΩΝΥΜΟΥ

Για τη μελέτη της πολλαπλότητας των ριζών εισάγουμε την έννοια της παραγώγου ενός πολυωνύμου.

Ορισμός 1. Έστω A μια αθέραια περιοχή και $f = a_n x^n + \dots + a_1 x + a_0 \in A[x]$. Παράγωγος του f λέγεται το πολυώνυμο

$$f' = n a_n x^{n-1} + \dots + a_1$$

Αν $f \in A$, ορίζουμε $f' = 0$.

Πρόταση 1. Ισχύουν οι ιδιότητες

$$\alpha) (f + g)' = f' + g'$$

$$\beta) (af)' = af', \quad a \in A$$

$$\gamma) (f \cdot g)' = f' \cdot g + f \cdot g'$$

Απόδειξη. (α) Διευκολύνει η γραφή του πολυωνύμου $f(x)$ υπό τη μορφή
"τυπικής σειράς"

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

όπου πεπερασμένο πλήθος συντελεστών a_i είναι $\neq 0$ και $x^0 = 1$. Τότε

$$f'(x) = \sum_{i=0}^{\infty} i a_i x^{i-1}$$

και συνεπώς για $g(x) = \sum_0^\infty \beta_i x^i$ έχουμε

$$\begin{aligned}
 (f(x) + g(x))' &= \left(\sum_0^\infty (a_i + \beta_i) x^i \right)' = \sum_1^\infty i(a_i + \beta_i) x^{i-1} \\
 &= \sum_1^\infty i a_i x^{i-1} + \sum_1^\infty i \beta_i x^{i-1} \\
 &= f'(x) + g'(x). \\
 (\beta) \quad (af(x))' &= \left(a \sum_0^\infty a_i x^i \right)' = \left(\sum_0^\infty a a_i x^i \right)' = \sum_1^\infty a i a_i x^{i-1} \\
 &= a \sum_1^\infty i a_i x^{i-1} = a f'(x)
 \end{aligned}$$

(γ) Αν η ιδιότητα ισχύει για ένα πολυώνυμο f και για δύο πολυώνυμα $g = g_1$ και $g = g_2$, θα ισχύει για το f και το $g = g_1 + g_2$, γιατί

$$\begin{aligned}
 (f(g_1 + g_2))' &= (f g_1 + f g_2)' = (f g_1)' + (f g_2)' \\
 &= (f' g_1 + f g_1') + (f' g_2 + f g_2') \\
 &= f'(g_1 + g_2) + f(g_1' + g_2') \\
 &= f'(g_1 + g_2) + f(g_1 + g_2)'
 \end{aligned}$$

Αρκεί συνεπώς να αποδειχτεί για τυχόν πολυώνυμο f και τυχόν μονώνυμο $g = \beta x^k$.

Για $k = 0$ είναι η ιδιότητα (β), αφού $(\beta)' = 0$. Έστω $k > 0$. Έχουμε

$$\begin{aligned}
 (f(x)g(x))' &= \left(\sum_{i=0}^\infty a_i \beta x^{i+k} \right)' = (a_0 \beta x^k + a_1 \beta x^{1+k} + \dots)' \\
 &= \sum_{i=0}^\infty (i+k) a_i \beta x^{i+k-1} \\
 &= \sum_{i=0}^\infty i a_i \beta x^{i+k-1} + \sum_{i=0}^\infty k a_i \beta x^{i+k-1} \\
 &= \left(\sum_1^\infty i a_i x^{i-1} \right) \beta x^k + \left(\sum_{i=0}^\infty a_i x^i \right) (k \beta x^{k-1}) \\
 &= f'(x)g(x) + f(x)g'(x)
 \end{aligned}$$

□

Στην περίπτωση του δακτυλίου $\mathbb{R}[x]$, όπου η χαρακτηριστική του $\mathbb{R}$ είναι μηδέν, το μόνο πολυώνυμο με $f'(x) = 0$ είναι το σταθερό πολυώνυμο $f = a \in A$. Αν η χαρακτηριστική p της αθέραιας περιοχής A είναι $p \neq 0$, παύει

να υπάρχει αναλογία. Π.χ., έστω $f = x^2 \in \mathbb{Z}_2[x]$. Προφανώς $f' = 2 \cdot x = 0$ και $f \notin \mathbb{Z}_2$. Σχετική είναι η παρακάτω πρόταση

Πρόταση 2. Έστω A μια αθέραια περιοχή με μονάδα και χαρακτηριστική p . Αν $f \in A[x]$ και $f' = \theta$, τότε

$$\alpha) p = 0 \Rightarrow f \in A$$

$$\beta) p > 0 \Rightarrow f = a_{mp}x^{mp} + \dots + a_px^p + a_0$$

Απόδειξη. Έστω $f(x) = a_nx^n + \dots + a_1x + a_0$ και ότι

$$f'(x) = na_nx^{n-1} + \dots + ka_kx^{k-1} + \dots + a_1 = \theta$$

Τότε $ka_k = 0$ για $k = n, \dots, 1$. Αν $p = 0$, έχουμε $a_k = 0$ για $k = n, \dots, 1$, δηλαδή $f(x) = a_0 \in A$. Έστω $p \neq 0$. Τότε $ka_k = 0$ συνεπάγεται $k \equiv 0 \pmod{p}$ ή $a_k = 0$. Το συμπέρασμα (β) είναι προφανές. $\square$

Πρόταση 3. Αν A αθέραια περιοχή και το $a \in A$ είναι ρίζα του $f \in A[x]$ πολλαπλότητας $m > 1$, τότε το a είναι ρίζα του f' πολλαπλότητας τουλάχιστον $m - 1$. Αν η χαρακτηριστική του A είναι μηδέν, είναι πολλαπλότητας ακριβώς $m - 1$.

Απόδειξη. Έστω $f(x) = (x - a)^m q(x)$ με $q(a) \neq 0$. Έχουμε $f'(x) = m(x - a)^{m-1}q(x) + (x - a)^m q'(x) = (x - a)^{m-1}Q(x)$ με $Q(x) = mq(x) + (x - a)q'(x)$. Συνεπώς $Q(a) = mq(a)$. Αν η χαρακτηριστική p/m , τότε $Q(a) = 0$, $x - a \mid Q(x)$ και $(x - a)^m \mid f'(x)$. Αν $p = 0$, $Q(a) \neq 0$ και η πολλαπλότητα της ρίζας a του f' είναι $m - 1$. $\square$

Ορισμός 2. Η παράγωγος n τάξης ενός πολυωνύμου f συμβολίζεται με $f^{(n)}$ και ορίζεται επαγωγικά ως εξής:

$$f^{(0)} = f, \quad f^{(n)} = \left(f^{(n-1)}\right)' \quad \text{για } n = 1, 2, \dots$$

Παράδειγμα 1. Έστω $f(x) = (x - a)^m$. Τότε

$$f^{(1)} = f'(x) = m(x - a)^{m-1}$$

$$f^{(2)} = f''(x) = m(m - 1)(x - a)^{m-2}$$

.....

$$f^{(k)} = m(m - 1) \dots (m - (k - 1))(x - a)^{m-k} = k! \binom{m}{k} (x - a)^{m-k}$$

Πρόταση 4. (Taylor) Αν K είναι αντιμεταθετικό σώμα χαρακτηριστικής μηδέν, $f \in K[x]$ και $a \in K$, ισχύει ο τύπος του Taylor

$$f(x) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} (x - a)^k, \quad \text{όπου } n = d^{\circ}(f) \quad (1)$$

Απόδειξη. Επειδή $x^k = ((x-a) + a)^k = \sum_{i=0}^k \binom{k}{i} (x-a)^i a^{k-i} = \sum_{i=0}^k \lambda_i (x-a)^i$, έπεται ότι υπάρχουν συντελεστές $\beta_k \in K$ ώστε

$$f(x) = \sum_{k=0}^n \beta_k (x-a)^k \quad (2)$$

Αρκεί συνεπώς ν' αποδείξουμε ότι $\beta_k = \frac{f^{(k)}(a)}{k!}$. Η (2) γράφεται

$$f(x) = \beta_0 + \beta_1(x-a) + \dots + \beta_k(x-a)^k + \dots + \beta_n(x-a)^n$$

Συνεπώς

$$f^{(k)}(x) = k!\beta_k + (k+1)!\beta_{k+1}(x-a) + \dots + n \dots (n-k)\beta_n(x-a)^{n-k}$$

οπότε $f^{(k)}(a) = k!\beta_k$, δηλαδή $\beta_k = \frac{f^{(k)}(a)}{k!}$. Έτσι από την (2) προκύπτει η (1). $\square$

Παρατήρηση 1. Ο τύπος Taylor ισχύει και όταν η χαρακτηριστική p του K είναι $> d^0(f)$, γιατί τότε $p \neq k!$ για $k = 1, 2, \dots, n$, δηλαδή $k! \neq 0$.

Πρόταση 5. Έστω K ένα σώμα και $f \in K[x]$. Ένα στοιχείο a κάποιου σώματος F , του οποίου το K είναι υπόσωμα, είναι ρίζα του f πολλαπλότητας > 1 τότε και μόνο όταν $f(a) = f'(a) = 0$.

Απόδειξη. Το a είναι ρίζα πολλαπλότητας > 1 τότε και μόνο, όταν $(x-a)^2/f$. Έστω $f(x) = (x-a)^2q(x)$. Τότε $f'(x) = 2(x-a)q(x) + (x-a)^2q'(x)$, συνεπώς $f(a) = 0$ και $f'(a) = 0$. Αντίστροφα, έστω $f(x) = (x-a)^2q(x) + v(x)$ με $d^0(v) \leq 1$. Τότε $v(a) = f(a) = 0$, $f'(x) = 2(x-a)q(x) + (x-a)2q'(x) + v'(x)$, οπότε $v'(a) = 0$. Από τις συνθήκες $v(a) = v'(a) = 0$, $v(x) = \lambda a + \mu$ παίρνουμε $v = 0$, δηλαδή $(x-a)^2/f$. $\square$

Παράδειγμα 2. Πότε το πολυώνυμο $f = \lambda x^2 + \mu x + \nu \in \mathbb{R}[x]$ έχει πολλαπλή ρίζα;

Θα πρέπει για κάποιο x να έχουμε $f(x) = f'(x) = 0$. Επειδή $f'(x) = 2\lambda x + \mu$, πρέπει $x = -\frac{\mu}{2\lambda}$, συνεπώς και $f(x) = \frac{\mu^2}{4\lambda} - \frac{\mu^2}{2\lambda} + \nu = 0$ ή $\mu^2 - 4\lambda\nu = 0$. Άρα το f έχει πολλαπλή ρίζα, αν η παράσταση $D(f) = \mu^2 - 4\lambda\nu$ μηδενίζεται.

Παρατήρηση 1. Αν x_1, x_2 είναι οι ρίζες του f , έχουμε

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \frac{\mu^2}{\lambda^2} - \frac{4\nu}{\lambda} = 0 \Leftrightarrow D(f) = 0$$

Η παράσταση $D(f) = (x_1 - x_2)^2$ λέγεται **διακρίνουσα** του f . Είδαμε ότι το f έχει πολλαπλή ρίζα τότε και μόνο, όταν $D(f) = 0$. Το αποτέλεσμα αυτό γενικεύεται για οποιοδήποτε πολυώνυμο.

Παρατήρηση 2. Οι ρίζες πολλαπλότητας > 1 του f είναι ρίζες των f, f' , συνεπώς και του $\mu.κ.δ.(f, f')$, ο οποίος βρίσκεται με τον αλγόριθμο του Ευκλείδη. Βρίσκοντας λοιπόν το $\mu.κ.δ.(f, f')$ εντοπίζουμε τις ρίζες πολλαπλότητας > 1 .

Παράδειγμα 3. Έστω K ένα σώμα χαρακτηριστικής $p = 0$ ή $p \neq n$. Οι ρίζες του $f = x^n - \beta \in K[x]$ στο K είναι απλές (πολλαπλότητας $= 1$). Γιατί $f'(a) = na^{n-1} \neq 0$ για κάθε $a \in K$.

Παρατήρηση 3. Υπάρχουν σώματα στα οποία το πολυώνυμο $f = x^n - \beta$ δεν έχει ρίζα. Π.χ. το $f = x^2 - 2 \in \mathbb{Z}_3[x]$ δεν έχει ρίζα στο $\mathbb{Z}_3$, γιατί $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{2}$, $f(\bar{2}) = \bar{1}$, δηλαδή $\sqrt{2} \notin \mathbb{Z}_3$ (το $\mathbb{Z}_3$ δεν είναι κλειστό ως προς την εξαγωγή ριζών).

Παράδειγμα 4. Βρείτε τις ρίζες πολλαπλότητας > 1 του $f = x^3 + x^2 - x - 1$.

Έχουμε $f' = 3x^2 + 2x - 1$. Εκτελούμε τη διαίρεση f με το f' και βρίσκουμε $f = \left(\frac{1}{3}x + \frac{1}{9}\right)f' + \left(-\frac{8x}{9} - \frac{8}{9}\right) = \left(\frac{1}{3}x + \frac{1}{9}\right)f' - \frac{8}{9}(x+1)$. Επειδή $x+1/f'$, αφού $f'(-1) = 0$, έπεται ότι $\mu.κ.δ.(f, f') = x+1$. Συνεπώς $x = -1$ είναι ρίζα του f πολλαπλότητας > 1 . Κάνοντας την διαίρεση του f με $(x+1)^2$ παίρνουμε $f = (x+1)^2(x-1)$. Άρα το -1 είναι ρίζα πολλαπλότητας 2.

Πρόταση 6. Έστω K ένα σώμα χαρακτηριστικής μηδέν και $f \in K[x]$. Το $a \in K$ είναι ρίζα του f πολλαπλότητας $m > 1$ τότε και μόνο, όταν

$$f(a) = f'(a) = \dots = f^{(m-1)}(a) = 0 \quad \text{και} \quad f^{(m)}(a) \neq 0 \quad (1)$$

Απόδειξη. Έστω ότι το a είναι ρίζα του f πολλαπλότητας $m > 1$. Κατά την πρότ.5 θα είναι $f(a) = f'(a) = 0$. Θέτοντας $f = (x-a)^{m-1}q(x)$, παίρνουμε $f' = x(x-a)^{m-1}q(x) + (x-a)^m q'(x) = (x-a)^{m-1}Q(x)$ με $Q(x) = mq(x) + (x-a)q'(x)$, οπότε $Q(a) = mq(a) \neq 0$. Έτσι το a είναι ρίζα του f' πολλαπλότητας $m-1$. Κατά την πρότ.5 θα είναι $f''(a) = 0$. Συνεχίζοντας με τον ίδιο τρόπο παίρνουμε τις σχέσεις (1).

Αντίστροφα, έστω ότι ισχύουν οι σχέσεις (1). Τότε από τον τύπο του Taylor

παίρνουμε

$$\begin{aligned} f(x) &= \frac{f^{(m)}(a)}{m!}(x-a)^m + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n, \quad n = d^o(f) \\ &= (x-a)^m \left[\frac{f^{(m)}(a)}{m!} + \frac{f^{(m)}(a)}{(m+1)!}(x-a) + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^{n-m} \right] \\ &\equiv (x-a)^m Q(x), \quad \text{όπου } Q(a) = \frac{f^{(m)}(a)}{m!} \neq 0 \end{aligned}$$

Άρα το a είναι ρίζα του f πολλαπλότητας m . □

3. ΑΚΕΡΑΙΕΣ ΚΑΙ ΡΗΤΕΣ ΡΙΖΕΣ

Έστω $f(x) \in \mathbb{Z}[x]$. Θα παρουσιάσουμε μία μέθοδο υπολογισμού των ριζών στο $\mathbb{Z}$ ή $\mathbb{Q}$. Μια ρίζα $\rho \in \mathbb{Z}$ θα λέγεται **ακέραια ρίζα**. Αν μια ρίζα $\rho \in \mathbb{Q}$ και $\rho \notin \mathbb{Z}$ θα λέγεται **ρητή ρίζα**.

Θεώρημα 1. Έστω $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Αν ρ είναι μια ακέραια ρίζα του f , τότε ρ/a_0 . Αν $a_0 = 0$, μια ακέραια ρίζα του είναι το μηδέν. Έστω ότι είναι ρίζα πολλαπλότητας m . Τότε $f(x) = x^m q(x)$ με $q(0) \neq 0$ και οι ακέραιες ρίζες του f είναι οι ακέραιες ρίζες του $q(x)$.

Απόδειξη. Προφανώς $a_n \rho^n + \cdots + a_1 \rho + a_0 = 0$ και $\rho(a_n \rho^{n-1} + \cdots + a_1) = -a_0$. Έτσι ρ/a_0 . □

Παράδειγμα 1. Έστω $f(x) = x^3 - 4x + 3$. Βρείτε τις ακέραιες ρίζες του f .

Αν ρ είναι ακέραια ρίζα του f , πρέπει $\rho/3$. Συνεπώς $\rho = \pm 1, \pm 3$. Με αντικατάσταση βρίσκουμε ότι $f(\rho) = 0$ μόνο για $\rho = 1$.

Παράδειγμα 2. Βρείτε τις ακέραιες ρίζες του $f(x) = x^7 + x^6 - 5x^5 + x^4 - 6x^3$.

Έχουμε $f(x) = x^3 q(x)$ με $q(x) = x^4 + x^3 - 5x^2 + x - 6$. Το μηδέν είναι ακέραια ρίζα πολλαπλότητας 3. Αναζητούμε τις ακέραιες ρίζες του $q(x)$. Έστω ρ ακέραια ρίζα του $q(x)$. Πρέπει $\rho/-6$. Συνεπώς $\rho = \pm 1, \pm 2, \pm 3, \pm 6$. Με αντικατάσταση βρίσκουμε ότι $q(\rho) = 0$ μόνο για $\rho = 2$ και $\rho = 3$. Έτσι οι ακέραιες ρίζες του f είναι $0, 2, -3$.

Θεώρημα 2. Έστω $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ και $\rho = \frac{a}{\beta}$ με $\beta > 0$ και $(a, \beta) = 1$ μια ρητή ρίζα του f . Τότε a/a_0 και β/a_n .

Απόδειξη. Η σχέση $f(\rho) = 0$ γράφεται

$$a_0 \beta^n = -a(a_n a^{n-1} + \dots + a_1 \beta^{n-1})$$

ή
$$a_n a^n = -\beta(a_{n-1} a^{n-1} + \dots + a_1 a \beta^{n-2} + a_0 \beta^{n-1})$$

Από την πρώτη ισότητα προκύπτει ότι $a/a_0 \beta^n$. Επειδή $a \neq \beta$, έπεται ότι a/a_0 . Από τη δεύτερη ισότητα προκύπτει ότι $\beta/a_n a^n$. Επειδή $\beta \neq a$, παίρνουμε ότι β/a_n . $\square$

Παράδειγμα 3. Βρείτε τις ρίζες του $f(x) = 6x^4 - x^3 - 13x^2 + 2x + 2$.

Οι διαιρέτες του σταθερού όρου είναι $\pm 1, \pm 2$ και του χύριου συντελεστή $\pm 1, \pm 2, \pm 3, \pm 6$. Συνεπώς οι ρητές ρίζες είναι μεταξύ των αριθμών

$$\pm 1, \pm 2, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{1}{6}.$$

Μετά από αντικατάσταση βρίσκουμε ότι $f(\rho) = 0$ μόνο για $\rho = \frac{1}{2}, -\frac{1}{3}$.

Παράδειγμα 4. Βρείτε τις ρίζες του πολυωνύμου του προηγούμενου παραδείγματος.

Βρήκαμε ότι το πολυώνυμο έχει τις ρητές ρίζες $\rho_1 = \frac{1}{2}$ και $\rho_2 = -\frac{1}{3}$. Συνεπώς διαιρείται με $\left(x - \frac{1}{2}\right) \left(x + \frac{1}{3}\right) = x^2 - \frac{1}{6}x - \frac{1}{6} = \frac{1}{6}(6x^2 - x - 1)$. Διαιρούμε στη συνέχεια το $f(x)$ με $6x^2 - x - 1$. Βρίσκουμε ότι $f(x) = (6x^2 - x - 1)(x^2 - 2)$. Άρα οι ρίζες του $f(x)$ είναι $\frac{1}{2}, -\frac{1}{3}, \sqrt{2}, -\sqrt{2}$.

ΑΣΚΗΣΕΙΣ

1. Έστω K ένα σώμα αντιμεταθετικό. Ν' αποδειχτεί ότι οι δακτύλιοι πηλίκια $K[x]/(x^2 - 1)$, $K[x]/(x^2 - 4)$ είναι ισόμορφοι.

2. Έστω A ένας αντιμεταθετικός δακτύλιος και $a \in A$. Δείξτε ότι η συνάρτηση $f \mapsto f(x - a)$ είναι αυτομορφισμός του $A[x]$.

3. Βρείτε τις ρίζες του πολυωνύμου $f = x^2 - 1 \in \mathbb{Z}_{15}[x]$ στο δακτύλιο $\mathbb{Z}_{15}$.

4. Το πολυώνυμο $f = x^2 + 1 \in \mathbb{Z}_5[x]$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_5[x]$;

5. Έστω A μια ακεραία περιοχή. Αν το πολυώνυμο $f \in A[x]$ διαιρείται με τα πολυώνυμα $x - a$, $x - \beta \in A[x]$ και $a \neq \beta$, δείξτε ότι διαιρείται και με το πολυώνυμο $(x - a)(x - \beta) \in A[x]$.

6. Δείξτε ότι το πολυώνυμο $f = (x-2)^{2n} + (x-1)^n - 1 \in \mathbb{R}[x]$ διαιρείται με το πολυώνυμο $g = x^2 - 3x + 2$ και βρείτε το ηλίκο της διαίρεσης στο δακτύλιο $\mathbb{R}[x]$.

7. Το πολυώνυμο $f = x^4 + 4 \in \mathbb{Z}_7[x]$ διαιρείται μ' ένα πολυώνυμο $x - \bar{a} \in \mathbb{Z}_7[x]$; Η ίδια ερώτηση για το πολυώνυμο $g = x^4 + 5 \in \mathbb{Z}_7[x]$.

8. Να βρείτε το ηλίκο και το υπόλοιπο της διαίρεσης του $x^n - a^n$ με το $x^m - a^m$ στο δακτύλιο $\mathbb{R}[x]$. Πότε το υπόλοιπο είναι μηδέν;

9. Ν' αποδειχτεί ότι $(x-1)^2$ διαιρεί το πολυώνυμο $f = nx^{n+1} - (n+1)x^n + 1$ στο δακτύλιο $\mathbb{R}[x]$. Βρείτε την πολλαπλότητα της ρίζας $\rho = 1$ του f .

10. Βρείτε τις ρίζες του πολυωνύμου $f = x^6 - 3x^4 + 3x^2 - 1 \in \mathbb{R}[x]$ πολλαπλότητας > 1 .

11. Το πολυώνυμο $f = x^{2n} - nx^{n+1} + nx^{n-1} - 1 \in \mathbb{R}[x]$ με $n > 1$ έχει ρίζα τον αριθμό $\rho = 1$. Βρείτε την πολλαπλότητα της ρίζας αυτής.

12. Έστω P ένα πολυώνυμο του δακτυλίου $\mathbb{R}[x]$. Ν' αποδειχτεί ότι το πολυώνυμο

$$Q = \frac{x-a}{2} [p'(x) + p'(a)] - [p(x) - p(a)], \quad a \in \mathbb{R}$$

έχει το a ρίζα πολλαπλότητας 3.

13. Αν $n \not\equiv 0 \pmod{3}$ δείξτε ότι $x^2 + x + 1/x^{2n} + x^n + 1$ στο δακτύλιο $\mathbb{R}[x]$.

14. Ν' αποδείξετε ότι το πολυώνυμο $f = x^3 + x + 1$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_2[x]$. Βρείτε το σώμα $\mathbb{Z}_2[x]/(f(x))$.

15. Ποιά πολυώνυμα του $\mathbb{Z}_3[x]$ 4^{ου} βαθμού δεν γράφονται γινόμενα άλλων πολυωνύμων του δακτυλίου αυτού;

16. Βρείτε ένα πολυώνυμο $f \in \mathbb{Q}[x]$ με ρίζα $\rho = \sqrt{2} + \sqrt{3}$. Ν' αποδείξετε ότι ο αριθμός $\sqrt{2} + \sqrt{3}$ είναι άρρητος.

17. Ν' αποδείξετε ότι ο αριθμός $\sqrt{2}/\sqrt[3]{5}$ είναι άρρητος.

18. Αν ο φυσικός n δεν διαιρείται με 2 και 3, δείξτε ότι το $xy(x^2 + xy + y^2)/(x+y)^n - x^n - y^n$ στο δακτύλιο $\mathbb{R}[x, y]$.

19. Στο πολυώνυμο $f = x^4 + 3x^3 - 5x^2 + 1$ θέτουμε $y = x - 1$. Βρείτε τον συντελεστή του y^2 .

20. Έστω ένα πολυώνυμο $P \in \mathbb{Z}[x, y]$. Ν' αποδειχτεί ότι $x^2 + xy + y^2/P$ τότε και μόνο, όταν $P(x, jx) = 0$; όπου $j = \text{syn} \frac{2\pi}{3} + i \eta\mu \frac{2\pi}{3}$.

Εφαρμογή: $x^2 + xy + y^2/x^{2n} + x^n y^n + y^{2n} \Leftrightarrow n \not\equiv 0 \pmod{3}$.

21. Έστω A, B, Γ τρία πολυώνυμα 2° βαθμού με συντελεστές πραγματικούς, σχετικά πρώτα και τέτοια, ώστε $A^2 + B^2 = \Gamma^2$. Δείξτε ότι

- i) Το Γ δεν έχει πραγματικές ρίζες.
- ii) Τα A, B έχουν πραγματικές ρίζες διάφορες.
- iii) Τα πολυώνυμα $\Gamma + A, \Gamma + B, \Gamma - B$ έχουν διπλές ρίζες.

22. Δείξτε ότι υπάρχει μια μοναδική ακολουθία πολυωνύμων $B_n(x) \in \mathbb{R}[x]$ τέτοια, ώστε

$$B'_n = nB_{n-1}$$

$$B_n(0) - B_n(1) = 0 \quad \text{για } n \geq 2$$

και $B_0(x) = 1, B_1(x) = x - \frac{1}{2}$. Στη συνέχεια ν' αποδείξετε ότι:

- i) $B_n(1-x) = (-1)^n B_n(x)$ και βρείτε τον συντελεστή του μεγιστοβάθμιου όρου του B_n .
- ii) $B_n(x+1) - B_n(x) = nx^{n-1}$ και βάσει αυτού να υπολογίσετε το άθροισμα

$$S_n = 1 + 2^p + \dots + n^p$$

23. Ν' αποδειχτεί ότι

$$x^{2n} - 2x^n \sin \theta + 1 = \left(x^2 - 2x \sin \frac{\theta}{n} + 1\right) \cdots \left(x^2 - 2x \sin \frac{(2n-2)\pi + \theta}{n} + 1\right)$$

Εφαρμογή: Αν $A_1, A_2, \dots, A_n$ είναι οι κορυφές ενός κανονικού πολυγώνου εγγεγραμμένου στον κύκλο κέντρου O και ακτίνας R , δείξτε ότι για κάθε σημείο M του επιπέδου του

$$(OM)^{2n} - 2(OM)^n + \sin \theta + R^{2n} = (MA_1)^2 \cdots (MA_n)^2$$

όπου $\theta = (\widehat{OM, OA_1})$. Αν $M_1, M_2, \dots$ τα μέσα των πλευρών $A_1A_2, A_2A_3, \dots$, και M σημείο της ακτίνας OA_1 , δείξτε ότι

$$|(OM)^n - R^n| = (MA_1)(MA_2) \cdots (MA_n)$$

$$(OM)^n + R^n = (MM_1)(MM_2) \cdots (MM_n)$$

24. Έστω $z_1, z_2, \dots, z_n$ οι μιγαδικές ρίζες της εξίσωσης $z^n = 1$, $\sigma_m = z_1^n + \dots + z_m^n$. Δείξτε ότι

- i) $m \equiv 0 \pmod{n} \Rightarrow \sigma_m = n$.
- ii) $m \not\equiv 0 \pmod{n} \Rightarrow \sigma_m = 0$.
- iii) $(z_1^2 - 2z_1 \sin \theta + 1) \cdots (z_n^2 - 2z_n \sin \theta + 1) = 2(1 - \sin n\theta)$.

13

Εισαγωγή στις επεκτάσεις σωμάτων

Βασικό συμπέρασμα της ενότητας αυτής είναι ότι κάθε μη σταθερό πολυώνυμο με συντελεστές από ένα σώμα K έχει μια ρίζα σε κάποιο σώμα και μάλιστα ότι υπάρχει σώμα στο οποίο το πολυώνυμο αναλύεται σε γινόμενο πρωτοβάθμιων πολυωνύμων.

Μια μερική περίπτωση, γνωστή από το Λύκειο, είναι το πολυώνυμο $f = x^2 + 1 \in \mathbb{R}[x]$, το οποίο δεν έχει ρίζα στο σώμα $\mathbb{R}$. Κατασκευάστηκε όμως το σώμα των μιγαδικών $\mathbb{C}$, το οποίο περιέχει μια ρίζα i του f και στο οποίο το f αναλύεται σε πρωτοβάθμιους παράγοντες : $f = (x - i)(x + i)$.

1. ΕΠΕΚΤΑΣΗ ΣΩΜΑΤΟΣ, ΑΛΓΕΒΡΙΚΑ ΣΤΟΙΧΕΙΑ

Το σώμα των μιγαδικών $\mathbb{C}$ περιέχει το σώμα των πραγματικών $\mathbb{R}$ σαν υπόσωμα. Λέμε ότι το σώμα $\mathbb{C}$ είναι επέκταση του $\mathbb{R}$. Γενικά:

Ορισμός 1. Ένα σώμα F , που περιέχει σαν υπόσωμα ένα σώμα K , λέγεται **επέκταση** του σώματος K .

Το σώμα F είναι τότε ένας διανυσματικός χώρος επί του K . Η διάσταση του

χώρου αυτού λέγεται **διάσταση** ή **βαθμός** της επέκτασης και συμβολίζεται με $[F : K]$.

Αν η διάσταση $[F : K]$ είναι πεπερασμένη, η επέκταση F του K λέγεται **πεπερασμένη**

Πρόταση 1. Είναι $[F : K] = 1 \Leftrightarrow F = K$.

Απόδειξη. Έστω ότι $[F : K] = 1$ και $\{a\}$ μια βάση του F επί του K . Αν $\beta \in F$, υπάρχει $\lambda \in K$ με $\beta = \lambda a$. Ειδικά για $\beta = 1$, έχουμε $1 = \lambda a$ με $\lambda \in K$. Τότε $a = \lambda^{-1} \in K$ και $\mu a \in K$ για κάθε $\mu \in K$. Άρα $F = K$. Το αντίστροφο είναι προφανές. $\square$

Αν το F παράγεται από ένα σώμα K και ένα στοιχείο $\gamma \in F$, η επέκταση F του K λέγεται **απλή** και συμβολίζεται με $F = K(\gamma)$.

Ορισμός 2. Ένα στοιχείο γ της επέκτασης F του K λέγεται **αλγεβρικό** επί του K , αν είναι ρίζα ενός μη μηδενικού πολυωνύμου με συντελεστές από το K .

Κάθε στοιχείο που δεν είναι αλγεβρικό επί του K λέγεται **υπερβατικό** επί του K .

Παραδείγματα.

1. Το $\mathbb{C}$ είναι πεπερασμένη επέκταση του $\mathbb{R}$, γιατί $[\mathbb{C} : \mathbb{R}] = 2$, αφού το σύνολο $\{1, i\}$ είναι βάση του χώρου $\mathbb{C}$ επί του $\mathbb{R}$. Η επέκταση $\mathbb{C}$ του $\mathbb{R}$ είναι απλή, γιατί $\mathbb{C} = \langle \mathbb{R} \cup \{i\} \rangle$, δηλαδή $\mathbb{C} = \mathbb{R}(i)$.

2. Ένα οποιοδήποτε σώμα F χαρακτηριστικής 0 είναι επέκταση του σώματος των ρητών $\mathbb{Q}$. Αν έχει χαρακτηριστική $p \neq 0$, είναι επέκταση του $\mathbb{Z}_p$.

3. Αναζητούμε το μικρότερο σώμα που είναι επέκταση του σώματος των ρητών $\mathbb{Q}$ και περιέχει το στοιχείο $\sqrt{2}$. Έστω K το σώμα αυτό. Πρέπει να περιέχει τις δυνάμεις του $\sqrt{2}$:

$$\sqrt{2}^0 = 1, \sqrt{2}, \sqrt{2}^2 = 2, \sqrt{2}^3 = 2\sqrt{2}, \dots, \sqrt{2}^n, \dots$$

όπως επίσης τους αριθμούς

$$a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \dots + a_n\sqrt{2}^n \quad \text{με } a_i \in \mathbb{Q}.$$

Οι αριθμοί αυτοί γράφονται $a + \beta\sqrt{2}$ με $a, \beta \in \mathbb{Q}$. Το K πρέπει να περιέχει ακόμη τον αντίστροφο του $a + \beta\sqrt{2}$ με $a, \beta \in \mathbb{Q}$. Αλλά

$$\frac{1}{a + \beta\sqrt{2}} = \frac{a - \beta\sqrt{2}}{a^2 - 2\beta^2} = \frac{a}{a^2 - 2\beta^2} + \frac{(-\beta)}{a^2 - 2\beta^2}\sqrt{2} = x + y\sqrt{2}$$

με $x, y \in \mathbb{Q}$, δηλαδή $\frac{1}{a + \beta\sqrt{2}} \in K$. Επειδή το σύνολο $\{a + \beta\sqrt{2} ; a, \beta \in \mathbb{Q}\}$ είναι σώμα και περιέχει το $\sqrt{2} = 0 + 1 \cdot \sqrt{2}$ και το σώμα $\mathbb{Q}$, έπεται ότι $K = \{a + \beta\sqrt{2} ; a, \beta \in \mathbb{Q}\}$. Η επέκταση K του $\mathbb{Q}$ είναι πεπερασμένη, γιατί $\{1, \sqrt{2}\}$ είναι βάση του K επί του $\mathbb{Q}$, δηλαδή $[K : \mathbb{Q}] = 2$. Τέλος $K = \mathbb{Q}(\sqrt{2})$, δηλαδή K είναι απλή επέκταση του $\mathbb{Q}$.

4. Ο αριθμός $i \in \mathbb{C}$ είναι αλγεβρικός επί του $\mathbb{R}$, γιατί είναι ρίζα του πολωνύμου $f = x^2 + 1 \in \mathbb{R}[x]$.

5. Ο αριθμός $\rho = \sqrt[3]{5 - \sqrt[3]{4}}$ είναι αλγεβρικός επί του $\mathbb{Q}$, γιατί είναι ρίζα πολωνύμου με συντελεστές ρητούς. Το πολυώνυμο αυτό βρίσκεται ως εξής: Έχουμε $\rho^2 = 5 - \sqrt[3]{4}$, $(\rho^2 - 5)^3 = -4$, $\rho^6 - 15\rho^4 + 75\rho^2 - 125 = -4$, δηλαδή το ρ είναι ρίζα του πολωνύμου $f = x^6 - 15x^4 + 75x^2 - 121 \in \mathbb{Q}[x]$.

6. Ο αριθμός $a = \sin \frac{2\pi}{5}$ είναι αλγεβρικός επί του $\mathbb{Q}$;

Λύση. Γνωρίζουμε ότι

$$\left(\sin \frac{2\pi}{5} + i \eta \mu \frac{2\pi}{5} \right)^5 = \sin 2\pi + i \eta \mu 2\pi = 1.$$

Αν $\beta = \eta \mu \frac{2\pi}{5}$, έχουμε $(a + i\beta)^5 = 1$ ή

$$a^5 - 10\beta^2 a^3 + 5\beta^4 a = 1$$

Επειδή $a^2 + \beta^2 = 1$, έχουμε

$$a^5 - 10(1 - a^2)a^3 + 5(1 - a^2)^2 a = 1$$

ή $16a^5 - 20a^3 + 5a - 1 = 0$. Άρα το a είναι αλγεβρικό επί του $\mathbb{Q}$.

7. Το πρώτο παράδειγμα υπερβατικού αριθμού επί του $\mathbb{Q}$ δόθηκε από τον Liouville το 1844. Το 1882 ο Lindemann απέδειξε ότι ο αριθμός $\pi = 3.14159 \dots$ είναι υπερβατικός επί του $\mathbb{Q}$. Η απόδειξη της υπερβατικότητας του π οδήγησε στην αρνητική απάντηση του προβλήματος του "τετραγωνισμού του κύκλου" αντίθετα με την πεποίθηση μεγάλης πλειοψηφίας μαθηματικών της εποχής εκείνης.

Το 1873 ο Hermite απέδειξε την υπερβατικότητα του e :

Θεώρημα 1. Ο αριθμός e είναι υπερβατικός επί του $\mathbb{Q}$.

Απόδειξη. Για κάθε πολυώνυμο $f \in \mathbb{Q}[x]$ βαθμού n θέτουμε $F(x) = \sum_0^n f^{(i)}(x)$ και επαληθεύουμε ότι

$$(e^{-x}F(x))' = -e^{-x}f(x)$$

Εφαρμόζουμε το θεώρημα μέσης τιμής για την συνάρτηση $x \mapsto e^{-x}F(x)$ στο διάστημα $[0, k]$, όπου k ακέραιος θετικός. Έχουμε

$$e^{-k}F(k) - F(0) = -e^{-\theta_k k}f(\theta_k k)k \quad \text{με } 0 < \theta_k < 1$$

απ' όπου

$$F(k) - F(0)e^k = -e^{(1-\theta_k)k}f(\theta_k k)k \equiv \epsilon_k$$

Ας υποθέσουμε ότι ο e είναι αλγεβρικός επί του $\mathbb{Q}$. Τότε υπάρχουν ακέραιοι c_i τέτοιοι, ώστε

$$c_m e^m + c_{m-1} e^{m-1} + \dots + c_0 = 0$$

Συνεπώς

$$\sum_1^m c_k F(k) - F(0) \sum_1^m c_k e^k = \sum_1^m c_k \epsilon_k$$

και

$$\sum_1^m c_k F(k) = \sum_1^m c_k \epsilon_k \equiv A.$$

Παίρνουμε τώρα σαν πολυώνυμο f το πολυώνυμο

$$f(x) = \frac{1}{(p-1)!} x^{p-1} (1-x)^p (2-x)^p \dots (m-x)^p$$

όπου p πρώτος $> \max\{m, c_0\}$.

Για $i \geq p$, $f^{(i)}(x) \in \mathbb{Z}[x]$ είναι το μηδενικό πολυώνυμο του $\mathbb{Z}_p[x]$, συνεπώς $f^{(i)}(j) \equiv 0 \pmod{p}$ για κάθε ακέραιο j . Επειδή το f έχει ρίζες $1, 2, \dots, m$ τάξης p , για $1 \leq j \leq m$ έχουμε

$$f(j) = f^{(1)}(j) = \dots = f^{(p-1)}(j) = 0$$

Συνεπώς

$$F(j) = \sum_{i=0}^n f^{(i)}(j) \equiv 0 \pmod{p} \quad , \quad 1 \leq j \leq m$$

Έχουμε ακόμη

$$f(0) = f^{(1)}(0) = \dots = f^{(p-2)}(0) = 0$$

Έτσι για $i \geq p$, $f^{(i)}(0) \equiv 0 \pmod{p}$, ενώ $f^{(p-1)}(0) = (m!)^p \not\equiv 0 \pmod{p}$, γιατί ο p είναι πρώτος $> m$. Συνεπώς

$$F(0) = \sum_0^n f^{(i)}(0) \not\equiv 0 \pmod{p}$$

και $A \not\equiv 0 \pmod{p}$. Επειδή $\theta_k \in (0, 1)$,

$$|\epsilon_k| \leq \frac{e^k m^p (m!)^p}{(p-1)!} \rightarrow 0 \quad (\text{για } p \rightarrow +\infty)$$

Για κάποιο $p > \max\{m, c_0\}$ έχουμε

$$\left| \sum_1^m c_k \epsilon_k \right| < 1 \quad \text{ή} \quad |A| < 1 \quad \text{ή} \quad A = 0,$$

αφού ο A είναι ακέραιος. Αυτό είναι άτοπο, γιατί αποδείξαμε ότι $A \not\equiv 0 \pmod{p}$. Άρα ο e , δεν είναι αλγεβρικός επί του $\mathbb{Q}$. $\square$

Σημείωση. Τα προβλήματα που αναφέρονται στην υπερβατικότητα αριθμών είναι εξαιρετικά δύσκολα. Γνωρίζουμε π.χ. ότι ο e^π είναι υπερβατικός επί του $\mathbb{Q}$, αλλά δεν γνωρίζουμε αν είναι ο π^e . Ένα βασικό αποτέλεσμα στη θεωρία αυτή είναι το θεώρημα των Gelfond-Schneider ότι ο a^β είναι υπερβατικός επί του $\mathbb{Q}$, όταν οι a, β είναι αλγεβρικοί επί του $\mathbb{Q}$ και $a \neq 0, 1, \beta \notin \mathbb{Q}$. Το πρόβλημα αυτό τέθηκε από τον Hilbert και περιλαμβάνεται στα περίφημα 23 προβλήματα που έθεσε στο διεθνές συνέδριο των Μαθηματικών στο Παρίσι το 1900. Η απόδειξη των Gelfond και Schneider είναι ανεξάρτητη και έγινε το 1934.

Θεώρημα 2. Έστω $E \subseteq K \subseteq L$ τρία σώματα. Αν οι επεκτάσεις K του E και L του K είναι πεπερασμένες, τότε η επέκταση L του E είναι πεπερασμένη και

$$[L : E] = [L : K] \cdot [K : E]$$

Απόδειξη. Έστω $\{e_1, e_2, \dots, e_m\}$ βάση του L επί του K και $\{v_1, v_2, \dots, v_n\}$ βάση του K επί του E . Θ' αποδείξουμε ότι

$$B = \{v_j e_i; i = 1, 2, \dots, m, j = 1, 2, \dots, n\}$$

είναι βάση του L επί του E . Έστω $x \in L$. Τότε $x = \sum_1^m x_i e_i$ με $x_i \in K$. Κάθε $x_i \in K$ γράφεται υπό τη μορφή $x_i = \sum_{j=1}^n \lambda_{ij} v_j$ με $\lambda_{ij} \in E$. Συνεπώς

$$x = \sum_{i=1}^m \left(\sum_{j=1}^n \lambda_{ij} v_j \right) e_i = \sum \lambda_{ij} v_j e_i$$

και το B παράγει το χώρο L επί του E . Έστω τώρα ότι

$$\sum_{i=1}^m \sum_{j=1}^n \lambda_{ij} v_j e_i = 0 \quad \text{με } \lambda_{ij} \in E.$$

Αφού τα e_i είναι γραμμικά ανεξάρτητα,

$$\sum_{j=1}^n \lambda_{ij} v_j = 0 \quad (i = 1, 2, \dots, m)$$

Αλλά και τα v_j είναι γραμμικά ανεξάρτητα επί του E . Συνεπώς $\lambda_{ij} = 0$ για κάθε i και κάθε j . Άρα το B είναι βάση του L επί του E και $[L : E] = mn = [L : K] \cdot [K : E]$. $\square$

Εφαρμογή. Δείξτε ότι δεν υπάρχουν σώματα μεταξύ του $\mathbb{Q}$ και του $L = \mathbb{Q}[x]/(x^3 - 2)$.

Απάντηση. Τα σταθερά πολυώνυμα στο L είναι τα στοιχεία του $\mathbb{Q}$. Έστω ότι υπάρχει σώμα K με $\mathbb{Q} \subseteq K \subseteq L$. Τότε από το θεώρημα προκύπτει ότι $[L : \mathbb{Q}] = [L : K] \cdot [K : \mathbb{Q}]$. Αλλά κάθε στοιχείο του L γράφεται μονοσήμαντα υπό τη μορφή

$$a_0 + a_1 x + a_2 x^2 + (x^3 - 2) \quad \text{με } a_i \in \mathbb{Q}.$$

Συνεπώς $\{1, x, x^2\}$ είναι βάση του L επί του $\mathbb{Q}$. Έτσι

$$3 = [L : K][K : \mathbb{Q}]$$

δηλαδή $[L : K] = 1$ ή $[K : \mathbb{Q}] = 1$. Στην πρώτη περίπτωση $L = K$ και στη δεύτερη $K = \mathbb{Q}$.

2. ΑΛΓΕΒΡΙΚΗ ΕΠΕΚΤΑΣΗ

Κάθε μιγαδικός αριθμός $z = a + \beta i$ είναι αλγεβρικός επί του $\mathbb{R}$, γιατί είναι ρίζα του πολυωνύμου $f = (x - a)^2 + \beta^2 \in \mathbb{R}[x]$. Λέμε ότι η επέκταση $\mathbb{C}$ του $\mathbb{R}$ είναι αλγεβρική επί του $\mathbb{R}$. Γενικά :

Ορισμός 1. Μια επέκταση F του σώματος K λέγεται **αλγεβρική**, αν κάθε στοιχείο του F είναι αλγεβρικό επί του K .

Θεώρημα 1. Κάθε πεπερασμένη επέκταση ενός σώματος K είναι αλγεβρική.

Απόδειξη. Έστω F μια πεπερασμένη επέκταση του K , $n = [F : K]$ και $a \in F$. Τα στοιχεία $1, a, a^2, \dots, a^n$ πλήθους $n+1$ είναι γραμμικά εξαρτημένα επί του K . Συνεπώς υπάρχουν $\lambda_i \in K$ όχι όλα μηδέν, τέτοια ώστε $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \dots + \lambda_n a^n = 0$, δηλαδή το a είναι ρίζα του μη μεδενικού πολυωνύμου $f = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \dots + \lambda_n x^n$, με συντελεστές $\lambda_i \in K$. Άρα το a είναι αλγεβρικό επί του K . $\square$

Έστω $a \in F$ αλγεβρικό επί του K . Υπάρχει συνεπώς πολυώνυμο $f \in K[x]$ με ρίζα το a .

Ορισμός 2. Το μη μηδενικό πολυώνυμο του $K[x]$ με τον ελάχιστο δυνατό βαθμό, που έχει ρίζα το a και κύριο συντελεστή τη μονάδα, λέγεται **ελάχιστο πολυώνυμο** του a επί του K και συμβολίζεται με $f_{a/K}$.

Πρόταση 1. Το ελάχιστο πολυώνυμο $f_{a/K}$ του a διαιρεί κάθε πολυώνυμο $f \in K[x]$ με ρίζα το a και είναι ανάγωγο στο δακτύλιο $K[x]$. Κάθε ανάγωγο πολυώνυμο του $K[x]$ με ρίζα το a είναι της μορφής $cf_{a/K}$ με $c \in K$.

Απόδειξη. Έστω $f \in K[x]$ με $f(a) = 0$. Έστω $f(x) = f_{a/K}(x) \cdot q(x) + v(x)$ με $d^0(v) < d^0(f_{a/K})$. Για $x = a$ παίρνουμε $0 = v(a)$. Συνεπώς βάσει του ορισμού του $f_{a/K}$ θα πρέπει $v = 0$ και $f_{a/K} \mid f$.

Το $f_{a/K}$ είναι ανάγωγο. Γιατί, αν υποθέσουμε ότι $f_{a/K}(x) = g(x)h(x)$, θα έχουμε $g(a)h(a) = 0$ και συνεπώς $g(a) = 0$ ή $h(a) = 0$. Τότε $f_{a/K}/g$ ή $f_{a/K}/h$. Αφού $g, h/f_{a/K}$, το $f_{a/K}$ είναι ανάγωγο. Αν το g είναι ανάγωγο πολυώνυμο με ρίζα το a , θα πρέπει $f_{a/K}/g$, δηλαδή $g = f_{a/K} \cdot q$ και αφού το g είναι ανάγωγο, $q = c \in K$. $\square$

Παράδειγμα 1. Έστω $a = i \in \mathbb{C}$. Προφανώς $f_{i/\mathbb{R}} = x^2 + 1$.

Παράδειγμα 2. Έστω $F = \mathbb{Q}(\sqrt{2})$. Το $\sqrt{2}$ είναι αλγεβρικό επί του $\mathbb{Q}$, γιατί είναι ρίζα του $f = x^2 - 2$. Δεν υπάρχει πολυώνυμο πρώτου βαθμού στο δακτύλιο $\mathbb{Q}[x]$ με ρίζα $\sqrt{2}$, γιατί $\sqrt{2} \notin \mathbb{Q}$. Συνεπώς $f_{\sqrt{2}/\mathbb{Q}} = x^2 - 2$.

Θεώρημα 2. Έστω K ένα σώμα, a ένα στοιχείο μιας επέκτασης του K αλγεβρικό επί του K και $p \in K[x]$ ένα ανάγωγο πολυώνυμο με ρίζα το a . Τότε

- i) $K(a) \cong K[x]/(p(x))$
- ii) $K(a) = K[a]$
- iii) $[K(a) : K] = d^0(p)$ και μια βάση είναι το σύνολο $\{1, a, a^2, \dots, a^{n-1}\}$, όπου $n = d^0(p)$.
- iv) Αν $|K| = m$, τότε το $K(a)$ έχει m^n στοιχεία.

Απόδειξη. Θεωρούμε τον ομομορφισμό

$$f : K[x] \rightarrow K(a) \quad \text{με τιμή} \quad f(\phi(x)) = \phi(a) :$$

$$\phi(x) = a_0 + a_1x + \cdots + a_nx^n \mapsto a_0 + a_1a + \cdots + a_na^n.$$

Ο πυρήνας του f είναι κύριο ιδεώδες του $K[x]$. Έστω $\text{Ker}(f) = (v(x))$ με $v(x) \in K[x]$. Αφού $p(a) = 0$, $p(x) \in \text{Ker}(f)$ και συνεπώς $p(x) = \lambda v(x)$ με $\lambda \in K$, δηλαδή $\text{Ker } f = (p(x))$. Σύμφωνα με το θεώρημα ισομορφισμού των δακτυλίων

$$K[x]/(p(x)) \cong \text{Im } f \subseteq K(a)$$

Αλλά το $K[x]/(p(x))$ είναι σώμα (θεώρ.1§2, Κεφ.10). Έτσι η εικόνα $\text{Im } f$ του f είναι υπόσωμα του $K(a)$, που περιέχει το K και το a . Άρα $\text{Im } f = K(a)$ και το πρώτο συμπέρασμα αποδείχτηκε ταυτόχρονα με το δεύτερο.

Το τρίτο συμπέρασμα προκύπτει αμέσως από τα συμπεράσματα i, ii.

Τέλος η ιδιότητα (iv) προκύπτει από την (iii) και την παρατήρηση ότι κάθε στοιχείο του $K(a)$ έχει τη μορφή $\lambda_0 \cdot 1 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_{n-1} a^{n-1}$, όπου για κάθε συντελεστή λ_i υπάρχουν m επιλογές. $\square$

Πόρισμα. Αν το a είναι υπερβατικό επί του K , η διάσταση $[K(a):K] = \infty$.

Παράδειγμα 3. Δείξτε ότι ο αριθμός $a = \sqrt[3]{7}i$ είναι αλγεβρικός επί του $\mathbb{Q}$ και βρείτε τη διάσταση $[\mathbb{Q}(a):\mathbb{Q}]$. Βρείτε επίσης μια βάση του χώρου $\mathbb{Q}(a)$ επί του $\mathbb{Q}$.

Προφανώς $a^4 - 7 = 0$. Το πολυώνυμο $f = x^4 - 7$ είναι σύμφωνα με το κριτήριο του Eisenstein ανάγωγο επί του $\mathbb{Q}$. Συνεπώς $f_{a/\mathbb{Q}} = x^4 - 7$ και $[\mathbb{Q}(a):\mathbb{Q}] = \text{βαθμός του } f_{a/\mathbb{Q}} = 4$. Μια βάση αποτελούν τα στοιχεία $1, a, a^2, a^3$.

Ορισμός 3. Έστω F μια επέκταση του K και $S \subseteq F$. Η τομή των υποσωμάτων του F , που περιέχουν το S και το K , είναι το μικρότερο υπόσωμα του F που περιέχει το S και το K και συμβολίζεται με $K(S)$. Αν $S = \{a_1, a_2, \dots, a_n\}$, γράφουμε $K(a_1, a_2, \dots, a_n)$ αντί $K(\{a_1, a_2, \dots, a_n\})$. Λέμε ότι το $K(S)$ προκύπτει από το K με την προσθήκη του S .

Πρόταση 2. Έστω F μια επέκταση του K και $S_1, S_2 \subseteq F$. Τότε

$$K(S_1 \cup S_2) = K(S_1)(S_2)$$

Απόδειξη. Το $K(S_1)(S_2)$ είναι υπόσωμα του F που περιέχει τα K, S_1, S_2 , συνεπώς τα $K, S_1 \cup S_2$, δηλαδή $K(S_1 \cup S_2) \subseteq K(S_1)(S_2)$. Επειδή $S_1 \cup S_2 \supseteq S_1, S_2$, έχουμε $K(S_1 \cup S_2) \supseteq K(S_1)$ και $K(S_1 \cup S_2) \supseteq S_2$. Συνεπώς $K(S_1 \cup S_2) \supseteq K(S_1)(S_2)$, άρα $K(S_1 \cup S_2) = K(S_1)(S_2)$. $\square$

Πόρισμα. $K(a_1, a_2, \dots, a_n)$ προκύπτει με διαδοχικές απλές επεκτάσεις του K : $K(a_1), K(a_1)(a_2) = K(a_1, a_2), \dots$

Πρόταση 3. Αν τα a_1, a_2 είναι αλγεβρικά επί του K , τότε $K(a_1, a_2)$ είναι πεπερασμένη επέκταση του K , συνεπώς αλγεβρική.

Απόδειξη. Σύμφωνα με το θεώρ.2 η $K(a_1)$ είναι πεπερασμένη επέκταση του K . Αφού το a_2 είναι αλγεβρικό επί του K , θα είναι αλγεβρικό και επί του $K(a_1)$. Δηλαδή η επέκταση $K(a_1)(a_2)$ του $K(a_1)$ είναι πεπερασμένη. Επειδή $[K(a_1, a_2) : K] = [K(a_1)(a_2) : K(a_1)][K(a_1) : K]$, η επέκταση $K(a_1, a_2)$ του K είναι πεπερασμένη. $\square$

Πόρισμα 1. Αν τα $a_1, a_2, \dots, a_n$ είναι αλγεβρικά επί του K , τότε $K(a_1, a_2, \dots, a_n)$ είναι πεπερασμένη επέκταση του K και άρα αλγεβρική επέκταση του K .

Πόρισμα 2. Έστω F μια επέκταση του K . Το σύνολο $\bar{K}$ των αλγεβρικών στοιχείων του F επί του K είναι υπόσωμα του F .

Γιατί, αν $a, \beta \in \bar{K}$, η επέκταση $K(a, \beta)$ είναι αλγεβρική και $a \pm \beta, a \cdot \beta, a/\beta$ (με $\beta \neq 0$) $\in K(a, \beta)$ δηλαδή $a \pm \beta, a \cdot \beta, a/\beta \in \bar{K}$. $\square$

3. ΚΑΤΑΣΚΕΥΕΣ ΜΕ ΚΑΝΟΝΑ ΚΑΙ ΔΙΑΒΗΤΗ

Οι Έλληνες γεωμέτρες είχαν ενδιαφερθεί για την κατασκευή γεωμετρικών σχημάτων με κανόνα και διαβήτη. Από την εποχή του Ευκλείδη γνώριζαν να διχοτομούν ένα ευθύγραμμο τμήμα και μια γωνία, να φέρουν κάθετο και παράλληλη ευθεία σε δοσμένη ευθεία και τέλος να κατασκευάζουν κανονικό πεντάγωνο.

Τα προβλήματα της τριχοτόμησης γωνίας, του διπλασιασμού του κύβου και του τετραγωνισμού του κύκλου, είναι γνωστά σαν “τα τρία περίφημα άλυτα προβλήματα της αρχαιότητας”. Αναζητούσαν επί αιώνες μέθοδο λύσης των προβλημάτων αυτών, που δυστυχώς δεν υπήρχε.

Το ότι είναι αδύνατον να λυθούν τα προβλήματα αυτά με κανόνα και διαβήτη αποδείχτηκε μόλις τον περασμένο αιώνα (κατά χρονολογική σειρά: 1837, 1829, 1882). Η απάντηση στα προβλήματα αυτά είναι μια από τις

πολλές εφαρμογές της θεωρίας των επεκτάσεων των σωμάτων.

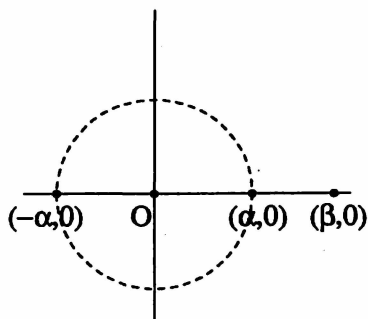
Κατασκευάσιμοι αριθμοί

Έστω E ένα επίπεδο και ένα ορθοκανονικό σύστημα συντεταγμένων με αρχή το σημείο $O(0,0)$.

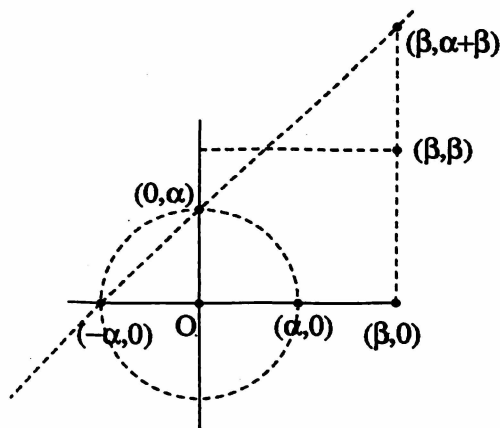
- Ένα σημείο $(a, \beta) \in E$ λέγεται **κατασκευάσιμο**, αν ορίζεται από τα σημεία $(0, 0)$ και $(1, 0)$ με πεπερασμένο πλήθος κατασκευών με τη βοήθεια μόνο του κανόνα και του διαβήτη.
- Ο πραγματικός αριθμός a λέγεται **κατασκευάσιμος**, αν το σημείο $(a, 0)$ είναι κατασκευάσιμο.
- Προφανώς το σημείο (a, β) είναι κατασκευάσιμο, αν οι αριθμοί a, β είναι κατασκευάσιμοι.

Θεώρημα 1. Το σύνολο K των κατασκευάσιμων πραγματικών αριθμών είναι ένα υπόσωμα του $\mathbb{R}$ και συνεπώς μια επέκταση του $\mathbb{Q}$.

Απόδειξη. Έστω $a, \beta \in K$. Προφανώς $-a \in K$ (σχ.1) και $a + \beta \in K$ (σχ.2). Πραγματικά,

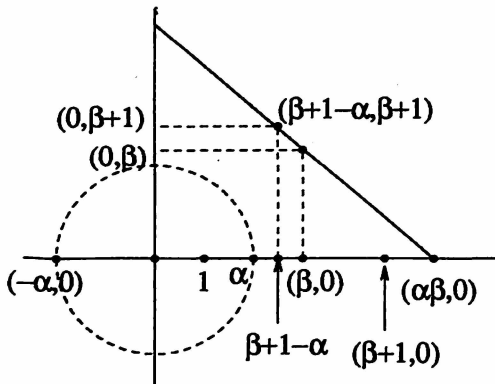


(σχ.1)

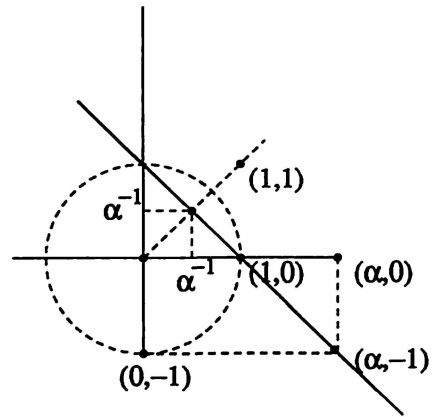


(σχ.2)

το σημείο $(\beta, a + \beta)$ είναι τομή των ευθειών που περνούν από τα κατασκευάσιμα σημεία $(\beta, 0)$, (β, β) και $(-a, 0)$, $(0, a)$. Συνέπεια αυτού είναι ότι $\beta + 1$, $\beta + 1 - a$ είναι κατασκευάσιμοι πραγματικοί αριθμοί. Η ευθεία που περνά από τα σημεία $(\beta + 1 - a, \beta + 1)$ και (β, β) τέμνει τον άξονα των x στο σημείο $(a\beta, 0)$, συνεπώς $a\beta \in K$ (σχ.3)



(σχ.3)

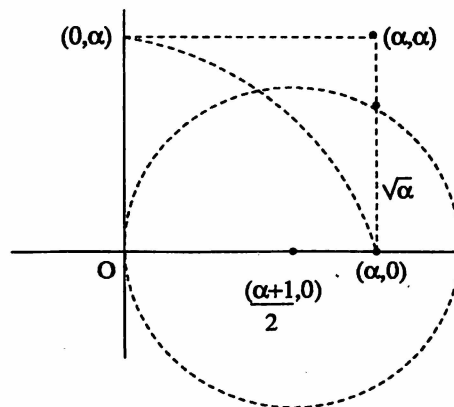


(σχ.4)

Αν $a \neq 0$, η ευθεία που περνά από τα σημεία $(1, 0)$, $(a, -1)$ τέμνει την ευθεία που περνά από τα σημεία $(0, 0)$, $(1, 1)$ στο σημείο (a^{-1}, a^{-1}) , δηλαδή $a^{-1} \in K$ (σχ.4). Άρα το K είναι σώμα, υπόσωμα του $\mathbb{R}$. Επειδή το $\mathbb{Q}$ είναι το μικρότερο υπόσωμα του $\mathbb{R}$, έπεται ότι $\mathbb{Q} \subseteq K$. $\square$

Πρόταση 1. Αν a θετικός πραγματικός αριθμός, ο αριθμός $\sqrt{a}$ είναι κατασκευάσιμος.

Απόδειξη. Ο αριθμός $\frac{a+1}{2}$ είναι κατασκευάσιμος. Ο κύκλος κέντρου $(\frac{a+1}{2}, 0)$ που περνά από το $(0, 0)$ τέμνει την ευθεία που περνά από τα σημεία (a, a) και $(a, 0)$ στα σημεία $(a, \sqrt{a})$, $(a, -\sqrt{a})$, συνεπώς $\sqrt{a} \in K$. $\square$



Πρόταση 2. (i) Η τομή δύο ευθειών με εξισώσεις, των οποίων οι συντελεστές ανήκουν σ' ένα σώμα $\mathcal{K}$, έχει συντεταγμένες στο σώμα $\mathcal{K}$.
(ii) Η τομή μιας ευθείας και ενός κύκλου (ή δύο κύκλων), των οποίων οι εξι-

σώσεις έχουν συντελεστές σ' ένα σώμα $\mathcal{K}$, έχει συντεταγμένες στοιχεία του σώματος $\mathcal{K}$ ή μιας επέκτασης $\mathcal{K}(\sqrt{d})$ του $\mathcal{K}$, όπου $d > 0$.

Απόδειξη. (i) Έστω $ax + \beta y + \gamma = 0$, $a'x + \beta'y + \gamma' = 0$ οι εξισώσεις των δύο ευθειών με συντελεστές $a, \dots, \gamma' \in \mathcal{K}$. Αν οι ευθείες τέμνονται, έχουμε $D = a\beta' - \beta a' \neq 0$ και

$$x = \frac{\beta\gamma' - \gamma\beta'}{D} \in \mathcal{K}, \quad y = \frac{\gamma a' - a\gamma'}{D} \in \mathcal{K}.$$

είναι οι συντεταγμένες του σημείου τομής.

(ii) Έστω οι εξισώσεις μιας ευθείας και ενός κύκλου

$$ax + \beta y + \gamma, \quad x^2 + y^2 + \lambda x + \mu y + \nu = 0$$

με συντελεστές $a, \beta, \dots, \nu$ στο σώμα $\mathcal{K}$. Ένας από τους συντελεστές a, β είναι $\neq 0$, έστω $\beta \neq 0$. Τότε $y = -\frac{a}{\beta}x - \frac{\gamma}{\beta}$ και η δεύτερη εξίσωση (του κύκλου) γίνεται $Ax^2 + Bx + \Gamma = 0$ με $A, B, \Gamma \in \mathcal{K}$. Για να έχει λύση πρέπει $D = B^2 - 4A\Gamma \geq 0$. Οι λύσεις είναι $x = \frac{-B \pm \sqrt{D}}{2A} \in \mathcal{K}(\sqrt{D})$. Αν $\sqrt{D} \in \mathcal{K}$, τότε $\mathcal{K}(\sqrt{D}) = \mathcal{K}$. Αν $\sqrt{D} \notin \mathcal{K}$, τότε $\mathcal{K} \subset \mathcal{K}(\sqrt{D})$ και οι συντεταγμένες του σημείου τομής $x, y \in \mathcal{K}(\sqrt{D})$ με $D > 0$.

Όμοια, αν έχουμε δύο κύκλους με εξισώσεις

$$x^2 + y^2 + ax + \beta y + \gamma = 0, \quad x^2 + y^2 + \lambda x + \mu y + \nu = 0$$

με συντελεστές $a, \dots, \nu \in \mathcal{K}$, τα σημεία τομής επαληθεύουν τις εξισώσεις

$$(a - \lambda)x + (\beta - \mu)y + (\gamma - \nu) = 0, \quad x^2 + y^2 + ax + \beta y + \gamma = 0$$

και κατά το πρώτο μέρος οι συντεταγμένες των σημείων τομής βρίσκονται στο $\mathcal{K}$ ή στο $\mathcal{K}(\sqrt{D})$ με $D > 0$. $\square$

Πρόταση 3. Αν $[K : F] = 2$ και $\mathbb{Q} \subseteq F$, τότε $K = F(\sqrt{\gamma})$ με $\gamma \in F$.

Απόδειξη. Το K είναι ένας διανυσματικός χώρος επί του F διάστασης 2. Έστω μια βάση του K επί του F της μορφής $\{1, a\}$. Τότε $K = \{\lambda + \mu a; \lambda, \mu \in F\}$. Αφού το K είναι σώμα, το $a^2 \in K$, συνεπώς $a^2 = \lambda_0 + \mu_0 a$ με $\lambda_0, \mu_0 \in F$ ή $\left(a - \frac{\mu_0}{2}\right)^2 = \lambda_0 + \left(\frac{\mu_0}{2}\right)^2$. Θέτοντας $\beta = a - \frac{\mu_0}{2}$ έχουμε $\beta^2 = \lambda_0 + \left(\frac{\mu_0}{2}\right)^2 \in F$. Τα στοιχεία $\{1, \beta\}$ είναι γραμμικά ανεξάρτητα

επί του f , γιατί $x \cdot 1 + y\beta = 0$ τότε και μόνο, όταν $x + y\left(a - \frac{\mu_0}{2}\right) = 0$ ή $\left(x - \frac{y\mu_0}{2}\right) + ya = 0$ ή $y = 0$ και $x = 0$. Συνεπώς $K = F(\beta) = F(\sqrt{\gamma})$, όπου $\gamma = \beta^2$. $\square$

Χαρακτηρισμός των κατασκευάσιμων αριθμών

Είδαμε ότι οι ρητοί αριθμοί είναι κατασκευάσιμοι. Συνεπώς όλα τα σημεία του επιπέδου με ρητές συντεταγμένες είναι κατασκευάσιμα με κανόνα και διαβήτη.

Ξεκινώντας από το σώμα των ρητών $\mathbb{Q}$ κατασκευάζουμε σύμφωνα με τις προτάσεις 1 και 2 τα στοιχεία του σώματος $\mathbb{Q}(\sqrt{b_1})$ με $b_1 > 0, b_1 \in \mathbb{Q}$. Αν $\sqrt{b_1} \in \mathbb{Q}$, τότε $\mathbb{Q}(\sqrt{b_1}) = \mathbb{Q}$ και $[\mathbb{Q}(\sqrt{b_1}) : \mathbb{Q}] = 1$. Αν $\sqrt{b_1} \notin \mathbb{Q}$ τότε $[\mathbb{Q}(\sqrt{b_1}) : \mathbb{Q}] = 2$. Η επέκταση $F(\sqrt{b_1})$ ενός σώματος F με βαθμό επέκτασης 2, λέγεται **τετραγωνική επέκταση** του F .

Από το σώμα $K_1 = \mathbb{Q}(\sqrt{b_1})$ κατασκευάζουμε τα στοιχεία του σώματος $K_2 = K_1(\sqrt{b_2}) = \mathbb{Q}(\sqrt{b_1}, \sqrt{b_2})$ με $[K_2 : K_1] = 2$ και $b_2 \in \mathbb{Q}(\sqrt{b_1})$.

Συνεχίζοντας κατασκευάζουμε μια ακολουθία σωμάτων (K_n) τέτοια, ώστε

- i) $\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_n \subset \dots$
- ii) $[K_i : K_{i-1}] = 2$, δηλαδή K_i είναι τετραγωνική επέκταση του K_{i-1}
- iii) $K_n \subset K$, όπου K το σύνολο των κατασκευάσιμων αριθμών.

Θεώρημα 2. Αν a είναι κατασκευάσιμος πραγματικός αριθμός, τότε $[\mathbb{Q}(a) : \mathbb{Q}] = 2^d$ με d ακέραιο ≥ 0 .

Απόδειξη. Αφού ο a είναι κατασκευάσιμος αριθμός, υπάρχει μια επέκταση K_m του $\mathbb{Q}$ τέτοια, ώστε $a \in K_m$ και $K_m = \mathbb{Q}(\sqrt{b_1}, \dots, \sqrt{b_m})$ με $[K_m : K_{m-1}] = 2$. Συνεπώς έχουμε

$$[K_m : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = [K_m : \mathbb{Q}] = [K_m : K_{m-1}] \cdots [K_1 : \mathbb{Q}] = 2^m$$

Άρα $[\mathbb{Q}(a) : \mathbb{Q}]$ διαιρεί τον αριθμό 2^m , δηλαδή $[\mathbb{Q}(a) : \mathbb{Q}] = 2^d$ με $d \geq 0$, $d \in \mathbb{Z}$. $\square$

Παρατήρηση. Η συνθήκη $[\mathbb{Q}(a) : \mathbb{Q}] = 2^d$ δεν είναι ικανή για να είναι ο a κατασκευάσιμος αριθμός (βλ. άσκ.31).

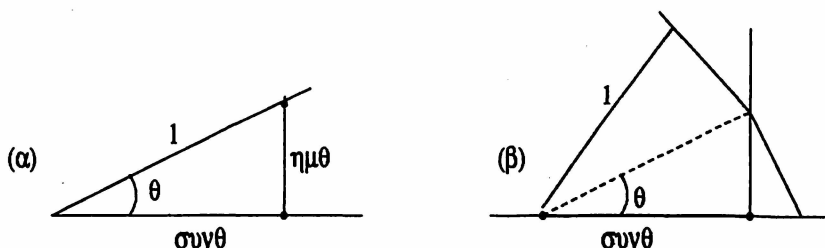
Απάντηση στα άλυτα προβλήματα της αρχαιότητας

Πρόταση 4. Ο διπλασιασμός του κύβου είναι αδύνατος με κανόνα και διαβήτη.

Απόδειξη. Έστω a το μήκος της πλευράς ενός κύβου. Ο όγκος του είναι a^3 . Πρέπει να κατασκευάσουμε κύβο όγκου $2a^3$. Αν x η πλευρά του, πρέπει $x^3 = 2a^3$ ή $x = a\sqrt[3]{2}$. Θ' αποδείξουμε ότι ο αριθμός $\sqrt[3]{2}$ δεν είναι κατασκευάσιμος. Ο αριθμός $\sqrt[3]{2}$ είναι ρίζα του πολυωνύμου $x^3 - 2 \in \mathbb{Q}[x]$. Το πολυώνυμο αυτό είναι ανάγωγο επί του $\mathbb{Q}$, συνεπώς $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^d$. Άρα ο $\sqrt[3]{2}$ δεν είναι κατασκευάσιμος αριθμός, οπότε και η πλευρά x δεν είναι κατασκευάσιμη. $\square$

Πρόταση 5. Η γωνία 60° είναι κατασκευάσιμη, ενώ η γωνία 20° δεν είναι κατασκευάσιμη. Άρα η τριχοτόμηση γωνίας δεν είναι πάντοτε δυνατή.

Απόδειξη. Όταν δίνεται μια γωνία θ κατασκευάζουμε ευθύγραμμο τμήματα μήκους $\sin \theta$ και $\eta\mu \theta$, όπως φαίνεται στο παρακάτω σχήμα (α)



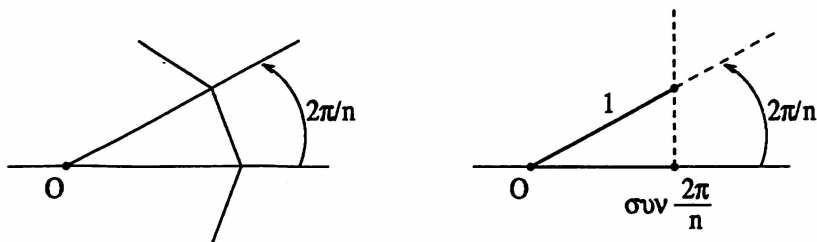
Αντίστροφα, αν ο αριθμός $\sin \theta$ είναι κατασκευάσιμος, η γωνία θ είναι κατασκευάσιμη (σχ.β). Θ' αποδείξουμε τώρα ότι ο αριθμός $x = 2 \sin \theta$ με $\theta = 20^\circ$ δεν είναι κατασκευάσιμος, άρα και ο $\sin \theta$. Έχουμε $\sin 3\theta = 4 \sin^3 \theta - 3 \sin \theta = \frac{1}{2}$, συνεπώς $x^3 - 3x - 1 = 0$. Το πολυώνυμο $x^3 - 3x - 1$ είναι ανάγωγο επί του $\mathbb{Q}$, γιατί δεν δέχεται ρίζα στο $\mathbb{Q}$ (οι μόνες δυνατές ρίζες είναι ± 1). Συνεπώς ο αριθμός x είναι αλγεβρικός επί του $\mathbb{Q}$ με $[\mathbb{Q}(x) : \mathbb{Q}] = 3 \neq 2^d$. Άρα ο x δεν είναι κατασκευάσιμος και η γωνία 20° δεν τριχοτομείται με κανόνα και διαβήτη. $\square$

Ο τετραγωνισμός του κύκλου, η κατασκευή δηλαδή τετραγώνου εμβαδού ίσου με το εμβαδό κύκλου, είναι επίσης αδύνατος, γιατί ο π θα ήταν κατασκευάσιμος αριθμός και συνεπώς αλγεβρικός επί του $\mathbb{Q}$. Αλλά αποδείχτηκε από τον Lindemann το 1882 ότι ο π είναι υπερβατικός. Άρα ο τετραγωνισμός του κύκλου είναι αδύνατος.

Κατασκευή κανονικού πολυγώνου

Η κατασκευή ενός κανονικού n -γώνου με κανόνα και διαβήτη είναι δυνατή τότε και μόνο, όταν η γωνία $\frac{2\pi}{n}$ είναι κατασκευάσιμη ή ο αριθμός $\sin \frac{2\pi}{n}$

είναι κατασκευάσιμος



Έστω $\zeta = \sigmaυν \frac{2\pi}{n} + i \etaμ \frac{2\pi}{n}$. Τότε $\frac{1}{\zeta} = \sigmaυν \frac{2\pi}{n} - i \etaμ \frac{2\pi}{n}$ και συνεπώς

$$\zeta + \frac{1}{\zeta} = 2 \sigmaυν \frac{2\pi}{n}$$

Έτσι το κανονικό n -γωνο είναι κατασκευάσιμο τότε και μόνο, όταν ο αριθμός $\zeta + \frac{1}{\zeta}$ είναι κατασκευάσιμος. Αποδεικνύεται(*) ότι

$$\left[\mathbb{Q} \left(\zeta + \frac{1}{\zeta} \right) : \mathbb{Q} \right] = \frac{\varphi(n)}{2} \quad (1)$$

όπου φ η συνάρτηση “φί” του Euler. Άρα, αν το κανονικό n -γωνο είναι κατασκευάσιμο, θα πρέπει $\varphi(n) = 2^m$ με $m \geq 1$. Ισχύει και το αντίστροφο(*). Από τον πίνακα τιμών της συνάρτησης φ

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	...
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12	...

προκύπτει π.χ ότι το κανονικό 7-γωνο και το 9-γωνο, δεν κατασκευάζονται με κανόνα και διαβήτη.

Για τα συμπεράσματα αυτά δεν είναι απαραίτητη η αναπόδεικτη σχέση (1) (βλ. ασκήσεις).

4. ΣΩΜΑ ΡΙΖΩΝ ΠΟΛΥΩΝΥΜΩΝ

Το σώμα των μιγαδικών αριθμών $\mathbb{C}$ κατασκευάστηκε σαν μια επέκταση του σώματος των πραγματικών αριθμών $\mathbb{R}$, που να περιέχει μια τουλάχιστον ρίζα του πολυωνύμου $f = x^2 + 1$, το οποίο δεν έχει καμιά ρίζα στο $\mathbb{R}$. Το πρόβλημα γενικεύεται αν αντικαταστήσουμε το σώμα $\mathbb{R}$ μ' ένα τυχαίο σώμα K και το πολυώνυμο $x^2 + 1$ μ' ένα πολυώνυμο $f \in K[x]$.

(*) βλ. Τόμο II

Θεώρημα 1. Έστω K ένα σώμα και $p \in K[x]$ ένα ανάγωγο πολυώνυμο στο $K[x]$. Τότε

- i) Υπάρχει πεπερασμένη επέκταση του K στην οποία το p έχει μια ρίζα, είναι η επέκταση

$$L = K[x]/(p(x))$$

- ii) Υπάρχει επέκταση του K , που περιέχει όλες τις ρίζες του $p(x)$, δηλαδή n ρίζες, όπου $n = d^\circ(p)$.

Απόδειξη. i) Έστω $I = (p(x))$. Το πηλίκο $L = K[x]/I$ είναι σώμα. Αν $p(x) = a_0 + a_1x + \dots + a_nx^n$, έχουμε $[L : K] = n$ και

$$\begin{aligned} p(x + I) &= a_0 + a_1(x + I) + a_2(x + I)^2 + \dots + a_n(x + I)^n \\ &= a_0 + (a_1x + I) + (a_2x^2 + I) + \dots + a_n(x^n + I) \\ &= p(x) + I = I \end{aligned}$$

και το I είναι το μηδέν του L .

- ii) Κάνουμε επαγωγή επί του βαθμού του p . Αν $d^\circ(p) = 1$, τότε $L = K$. Έστω ότι το συμπέρασμα ισχύει για πολυώνυμο βαθμού $n - 1$. Έστω f ένα πολυώνυμο βαθμού n . Αν είναι ανάγωγο, υπάρχει επέκταση K , η οποία περιέχει μια ρίζα ρ_1 του f . Τότε $f(x) = (x - \rho_1)q(x)$ με $d^\circ(q) = n - 1$. Κατά την υπόθεση της επαγωγής υπάρχει πεπερασμένη επέκταση K_2 του K_1 , που περιέχει όλες τις ρίζες του $q(x)$. Επειδή $[K_2 : K] = [K_2 : K_1] \cdot [K_1 : K]$, η K_2 είναι πεπερασμένη επέκταση του K και περιέχει όλες τις ρίζες του p .

Αν το f δεν είναι ανάγωγο, γράφεται σαν γινόμενο $f(x) = \phi(x)q(x)$, όπου ϕ ανάγωγο πολυώνυμο. Συνεπώς υπάρχει μια επέκταση K_1 του K που περιέχει μια ρίζα a του ϕ . Τότε $\phi(x) = (x - a)\sigma(x)$ και $f(x) = (x - a)Q(x)$ με $d^\circ(Q) = n - 1$. Συνεχίζοντας όπως παραπάνω βρίσκουμε μια πεπερασμένη επέκταση, που περιέχει όλες τις ρίζες του f . $\square$

Παράδειγμα 1. Βρείτε ένα σώμα με 4 στοιχεία. Γράψτε τους πίνακες των πράξεων.

Θεωρούμε το σώμα $\mathbb{Z}_2$. Αρκεί να βρούμε ένα ανάγωγο πολυώνυμο f του δακτυλίου $\mathbb{Z}_2[x]$ βαθμού 2 και να θεωρήσουμε το σώμα $\mathbb{Z}_2[x]/(f)$.

Τα πολυώνυμα πρώτου βαθμού του $\mathbb{Z}_2[x]$ είναι $x, x + 1$. Τα μη ανάγωγα $2^{\text{ου}}$ βαθμού είναι τα γινόμενα τους, $x^2, x(x + 1) = x^2 + x, (x + 1)^2 = x^2 + 1$. Συνεπώς το πολυώνυμο $f = x^2 + x + 1$ είναι ανάγωγο επί του $\mathbb{Z}_2[x]$.

Πραγματικά, $f(\bar{0}) = \bar{1}, f(\bar{1}) = \bar{1}$. Συνεπώς το πηλίκο $\mathbb{Z}_2[x]/(x^2 + x + 1)$ είναι σώμα με $2^2 = 4$ στοιχεία. Τα στοιχεία του γράφονται υπό τη μορφή

$$(ax + \beta) + I$$

όπου $a, \beta \in \mathbb{Z}_2$ και $I = (x^2 + x + 1)$. Συνεπώς

$$\mathbb{Z}_2[x]/I = \{I, 1 + I, x + I, (1 + x) + I\}.$$

Το I είναι το μηδέν του σώματος και το $1 + I$ η μονάδα. Γράφουμε

$$I = \bar{0}, \quad 1 + I = \bar{1}, \quad x + I = a, \quad (1 + x) + I = 1 + a$$

και παρατηρούμε ότι το a είναι ρίζα του πολυωνύμου $x^2 + x + 1$ στο σώμα $\mathbb{Z}_2[x]/I$, γιατί

$$\begin{aligned} a^2 + a + 1 &= (x + I)^2 + ((1 + x) + I) = (x^2 + I) + ((x + 1) + I) \\ &= (x^2 + x + 1) + I = I \end{aligned}$$

Οι πίνακες των πράξεων είναι

+	0	1	a	1+a
0	0	1	a	1+a
1	1	0	1+a	a
a	a	1+a	0	1
1+a	1+a	a	1	0

	0	1	a	1+a
0	0	0	0	0
1	0	1	a	1+a
a	0	1	1+a	1
1+a	0	1+a	1	a

Μια άλλη ρίζα του πολυωνύμου $x^2 + x + 1$ στο σώμα $L = \mathbb{Z}_2[x]/I$ είναι το $1 + a$, γιατί $(1 + a)^2 + (1 + a) + 1 = 1 + a^2 + a + a + 1 = a^2 + a + 1 = 0$. Άρα η επέκταση L του $\mathbb{Z}_2$ περιλαμβάνει όλες τις ρίζες του $f = x^2 + x + 1$. Γι' αυτό γράφεται στο σώμα αυτό σαν γινόμενο πρωτοβάθμιων πολυωνύμων

$$f = (x - a_1)(x - a_2), \quad a_1 = a, \quad a_2 = a + 1$$

Ορισμός 1. Έστω F μια επέκταση του K στην οποία

$$f = (x - a_1)(x - a_2) \cdots (x - a_n), \quad a_i \in F$$

Το σώμα $K(a_1, a_2, \dots, a_n)$ είναι το μικρότερο υπόσωμα της επέκτασης F του K , που περιέχει τις ρίζες του f . Λέγεται **σώμα ριζών** του f επί του K και συμβολίζεται με $\Sigma_{f/K}$.

Παράδειγμα 2. Βρείτε το σώμα ριζών του πολυωνύμου $f = x^3 - 2$ επί του $\mathbb{Q}$ και τη διάσταση $[\Sigma_{f/\mathbb{Q}} : \mathbb{Q}]$.

Οι ρίζες του f βρίσκονται στο σώμα των μιγαδικών αριθμών και είναι

$$\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$$

όπου $\omega = \frac{-1 + \sqrt{3}i}{2}$ μια πρωτεύουσα ρίζα του 1. Συνεπώς

$$\begin{aligned}\Sigma_{f/K} &= \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) \\ &= \mathbb{Q}(\sqrt[3]{2}, \omega)\end{aligned}$$

Το πολυώνυμο $f = x^3 - 2$ είναι ανάγωγο στο $\mathbb{Q}[x]$, συνεπώς $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Το ω είναι ρίζα του $h = x^2 + x + 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$ και συνεπώς

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] \leq 2$$

οπότε $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 6$

Το πολυώνυμο $h = x^2 + x + 1$ είναι ανάγωγο επί του $\mathbb{Q}$ (βλ. §2, Κεφ.11), συνεπώς $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Επειδή

$$[\mathbb{Q}(\omega) : \mathbb{Q}] / [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$$

και $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] / [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$

έχουμε ότι $2, 3 / [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}]$, οπότε $6 / [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] \leq 6$.

Άρα $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$.

Πρόταση 1. Έστω ένα πολυώνυμο $f \in K[x]$ ανάγωγο επί του K και u, v δύο ρίζες του f σ' ένα σώμα $L \supseteq K$. Τότε υπάρχει ισομορφισμός $\varphi : K(u) \rightarrow K(v)$ τέτοιος, ώστε $\varphi(a) = a$ για κάθε $a \in K$ και $\varphi(u) = v$.

Απόδειξη. Κατά το θεώρημα 2 υπάρχουν ισομορφισμοί

$$\sigma : K(u) \rightarrow K[x]/(f(x)) \text{ και } \psi : K[x]/(f(x)) \rightarrow K(v)$$

τέτοιοι, ώστε

$$u \xrightarrow{\sigma} x + (f(x)) \xrightarrow{\psi} v \text{ και } a \rightarrow a + (f(x)) \rightarrow a, \forall a \in K$$

Ο ισομορφισμός $\psi \circ \sigma = \varphi$ είναι ο ζητούμενος. $\square$

Θεώρημα 2. Έστω $f \in K[x]$ και F, E δύο σώματα ριζών του f επί του K . Τα σώματα F, E είναι ισόμορφα, μάλιστα υπάρχει ισομορφισμός $\phi : F \rightarrow E$ που αφήνει σταθερά τα στοιχεία του K , δηλαδή $\phi(a) = a$ για κάθε $a \in K$.

Ένας τέτοιος ισομορφισμός μεταξύ δύο επεκτάσεων ενός σώματος K , θα λέγεται K -ισομορφισμός.

Το θεώρημα αυτό είναι μερική περίπτωση του θεωρήματος που ακολουθεί, αν θεωρήσουμε $K = K^*$ και h τον ταυτοτικό ισομορφισμό του K στον εαυτό του.

Θεώρημα 3. Έστω K, K^* δύο σώματα, $h : K \rightarrow K^*$ ισομορφισμός, $f \in K[x]$ και $f^* \in K^*[x]$ με συντελεστές τις εικόνες των συντελεστών του f με τον ισομορφισμό h . Αν Σ, Σ^* είναι σώματα ριζών των f, f^* αντίστοιχα, υπάρχει ισομορφισμός $\varphi : \Sigma \rightarrow \Sigma^*$ τέτοιος, ώστε $\varphi(a) = h(a)$ για κάθε $a \in K$.

Απόδειξη. Κάνουμε επαγωγή ως προς $n = [\Sigma : K]$. Αν $n = 1$, έχουμε $\Sigma = K, \Sigma^* = K^*$ και $h = \varphi$. Έστω $n > 1$ και ότι το θεώρημα ισχύει για όλα τα σώματα ριζών βαθμού επέκτασης $< n$ επί του σώματος K . Επειδή $n > 1$, το πολυώνυμο f δεν έχει όλες τις ρίζες στο K , συνεπώς έχει ένα ανάγωγο παράγοντα g βαθμού $d > 1$. Έστω u μια ρίζα του g στο Σ και $g^* \in K^*[x]$ το πολυώνυμο με συντελεστές τις εικόνες των συντελεστών του g με τον h . Το σώμα των ριζών Σ^* περιέχει μια ρίζα v του g^* . Κατά την πρόταση 1 υπάρχει ισομορφισμός $\psi : K(u) \rightarrow K^*(v)$ τέτοιος, ώστε $\psi(a) = a^* (= h(a))$. Τα σώματα Σ, Σ^* είναι σώματα ριζών των f, f^* αντίστοιχα επί των $K(u), K^*(v)$. Αλλά $[\Sigma : K(u)] = \frac{n}{d} < n$. Κατά την υπόθεσή μας ο ψ επεκτείνεται σ' ένα ισομορφισμό $\varphi : \Sigma \rightarrow \Sigma^*$ ο οποίος επεκτείνει τον h . $\square$

Θεώρημα 4. Έστω K, K^* δύο ισόμορφα σώματα, $h : K \rightarrow K^*$ ένας ισομορφισμός, $f \in K[x]$ με ρίζες απλές στο σώμα των ριζών Σ . Υπάρχουν $n = [\Sigma : K]$ ισομορφισμοί $\varphi : \Sigma \rightarrow \Sigma^*$ που επεκτείνουν τον h .

Απόδειξη. Κάνουμε επαγωγή ως προς το βαθμό $n = [\Sigma : K]$. Για $n = 1$ είναι προφανές. Έστω $n > 1$ και ότι το συμπέρασμα ισχύει για κάθε σώμα ριζών Σ με $[\Sigma : K] < n$ επί του K . Αφού $n > 1$, υπάρχει ένας ανάγωγος παράγοντας g του f βαθμού $d > 1$. Έστω a μια ρίζα του g στο Σ και $g^* \in K^*[x]$ με συντελεστές τις εικόνες των συντελεστών του f με τον h . Κάθε επέκταση φ του h απεικονίζει την ρίζα a σε μια ρίζα β του g^* . Αφού το g^* έχει d ρίζες, υπάρχουν d ισομορφισμοί $\psi : K(a) \rightarrow K^*(\beta)$ με $\psi(a) = \beta$.

Κατά την υπόθεση της επαγωγής υπάρχουν $\frac{n}{d} = [\Sigma : K(a)]$ επεκτάσεις του ψ , άρα $d \frac{n}{d} = n$ επεκτάσεις του h στο Σ . $\square$

ΑΣΚΗΣΕΙΣ

1. Ν' αποδειχτεί ότι $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(3 + \sqrt{2})$.
2. Βρείτε τα στοιχεία του σώματος $\mathbb{Q}(\sqrt[3]{5})$.
3. Δείξτε ότι $\mathbb{Q}(\sqrt{2}, \sqrt{6})$ και $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ είναι επεκτάσεις του $\mathbb{Q}(\sqrt{3})$ και βρείτε τους βαθμούς των επεκτάσεων αυτών.
4. Ν' αποδείξετε ότι $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ και γενικά $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ για όλα τα $a, b \in \mathbb{Q}$.
5. Βρείτε μια βάση της επέκτασης $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ επί του $\mathbb{Q}$.
6. Βρείτε το $(1 + \sqrt[3]{2})^{-1}$ στο σώμα $\mathbb{Q}(\sqrt[3]{2})$.
7. Βρείτε τον αριθμό a , ώστε $\mathbb{Q}(\sqrt{2}, \sqrt{-3}) = \mathbb{Q}(a)$.
8. Δείξτε ότι οι παρακάτω αριθμοί είναι αλγεβρικοί επί του $\mathbb{Q}$:
 $(\alpha) \sqrt{2} + 1, \quad (\beta) \sqrt[3]{4} + \sqrt{3}, \quad (\gamma) 1 + i$
9. Ν' αποδείξετε ότι η επέκταση $\mathbb{R}$ του $\mathbb{Q}$ δεν είναι πεπερασμένη.
10. Ν' αποδείξετε ότι ο αριθμός $\sin 36^\circ$ είναι αλγεβρικός επί του $\mathbb{Q}$.
11. Ν' αποδείξετε ότι $[\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}, \dots, \sqrt{n_k}) : \mathbb{Q}] \leq 2^k$.
12. Βρείτε το βαθμό της επέκτασης $\mathbb{Q} \left(\sin \frac{2\pi}{5} \right)$ του $\mathbb{Q}$.
13. Δείξτε ότι το ελάχιστο πολυώνυμο του $\sqrt{7} + i$ είναι
 $\alpha) x^2 - 2\sqrt{7}x + \beta$ επί του $\mathbb{R}$
 $\beta) x^4 - 12x^2 + 64$ επί του $\mathbb{Q}$.
14. Βρείτε το ελάχιστο πολυώνυμο του $\sqrt[3]{2} + \sqrt[3]{4}$ επί του $\mathbb{Q}$ (υπόδειξη: Στο δακτύλιο $\mathbb{C}[x]$, το πολυώνυμο $x + z + w/x^3 - 3zwx + z^3 + w^3$).
15. Βρείτε το ελάχιστο πολυώνυμο του $\sqrt{7} + i$ επί του $\mathbb{Q}(i)$.
16. Έστω μια αλγεβρική επέκταση του σώματος K και ένας δακτύλιος A με $K \subseteq A \subseteq F$. Ν' αποδειχτεί ότι ο A είναι σώμα. Αντίστροφα, αν κάθε δακτύλιος A με $K \subseteq A \subseteq F$ είναι σώμα, η F είναι αλγεβρική επέκταση του K .

17. Βρείτε μια επέκταση $\mathbb{Q}(a, \beta, \gamma)$ του $\mathbb{Q}$, η οποία να περιέχει τις ρίζες του πολυωνύμου $x^4 - 8x^2 + 5$ και $\beta^2 \in \mathbb{Q}(a)$, $\gamma^2 \in \mathbb{Q}(a, \beta)$.

18. Αν ξ είναι αλγεβρικός αριθμός επί του $\mathbb{Q}$, ρίζα του πολυωνύμου $f \in \mathbb{Q}[x]$ βαθμού n για κάθε $\delta > 0$ και $A > 0$ η ανισότητα

$$\left| \xi - \frac{p}{q} \right| < \frac{A}{q^{n+\delta}}$$

ισχύει για πεπερασμένο πλήθος ακεραίων p και q .

Εφαρμογή: Δείξτε ότι ο αριθμός

$$\xi = \frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \dots$$

είναι υπερβατικός.

19. Δείξτε ότι η γωνία 30° είναι κατασκευάσιμη.

20. Το σύνολο A των πραγματικών αριθμών a για τους οποίους το συν a είναι κατασκευάσιμος αριθμός, είναι υποομάδα της $(\mathbb{R}, +)$ και για κάθε $a \in A$, $\frac{1}{2}a \in A$.

21. Αν ο αριθμός συν θ είναι κατασκευάσιμος, δείξτε ότι οι αριθμοί συν $(n\theta)$ και συν $\frac{\theta}{2^n}$ είναι κατασκευάσιμοι για κάθε φυσικό n .

22. Ν' αποδειχτεί ότι η γωνία φ τριχοτομείται τότε και μόνο, όταν το πολυώνυμο $4x^3 - 3x - \text{συν } \varphi$ δεν είναι ανάγωγο επί του $\mathbb{Q}$.

23. Έστω $\zeta = \text{συν } \frac{2\pi}{5} + i \text{ ημ } \frac{2\pi}{5}$. Δείξτε ότι

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1 = 0, \quad \zeta + \zeta^{-1} = \frac{-1 + \sqrt{5}}{2}$$

$$j = \frac{-1 + \sqrt{5}}{2} + i \frac{\sqrt{-2 + 2\sqrt{5}}}{2}.$$

Βάσει του τύπου αυτού να κατασκευάσετε με κανόνα και διαβήτη κανονικό πεντάγωνο.

24. Έστω $\zeta = \text{συν } \frac{2\pi}{7} + i \text{ ημ } \frac{2\pi}{7}$, $\xi = \text{συν } \frac{2\pi}{7}$. Δείξτε ότι

- i) $\zeta^7 - 1 = 0$, $\zeta \neq 1$
- ii) $\zeta^3 + \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} + \zeta^{-3} = 0$
- iii) $\zeta^2 + \zeta^{-2} = 4\xi^2 - 2$, $\zeta^3 + \zeta^{-3} = 8\xi^3 - 6\xi$.
- iv) $8\xi^3 + 4\xi^2 - 4\xi - 1 = 0$
- v) Το κανονικό 7-γωνο δεν κατασκευάζεται με κανόνα και διαβήτη.

25. Έστω $n = p_1^{m_1} p_2^{m_2} \cdots p_\lambda^{m_\lambda}$ η ανάλυση του φυσικού n σε γινόμενο διάφορων πρώτων παραγόντων. Δείξτε ότι:

- i) Αν p είναι πρώτος μεγαλύτερος του 2, $p^{n-1}(p-1)$ είναι δύναμη του 2 τότε και μόνο, όταν $p = 2^{2^v} + 1$.

Οι πρώτοι αριθμοί της μορφής $2^{2^v} + 1$ λέγονται αριθμοί Mersenne. (Ο Euler απέδειξε ότι $641/2^{2^5} + 1$, συνεπώς οι αριθμοί $2^{2^v} + 1$ δεν είναι για κάθε v πρώτοι).

- ii) Το κανονικό πολύγωνο κατασκευάζεται με κανόνα και διαβήτη, τότε και μόνο, όταν $n = 2^r p_1 p_2 \cdots p_\lambda$, όπου p_λ αριθμοί Mersenne.

26. Να κατασκευάζεται ένα σώμα με 9 στοιχεία με τη βοήθεια του πολυωνύμου $x^2 + x + 2 \in \mathbb{Z}_3[x]$.

27. Δείξτε ότι το πολυώνυμο $p = x^2 + x + 1$ είναι ανάγωγο στο δακτύλιο $\mathbb{Z}_2[x]$. Έστω a μια ρίζα του p σε μια επέκταση του $\mathbb{Z}_2$. Ν' αναλύσετε το πολυώνυμο p σε γινόμενο πολυωνύμων πρώτου βαθμού στο δακτύλιο $\mathbb{Z}_2(a)[x]$. (Να κάνετε τη διαίρεση του p με $x - a$).

28. Έστω K υπόσωμα του $\mathbb{C}$ το οποίο περιέχει τις ρίζες της εξίσωσης $x^n = 1$ ($n \geq 1$) και έστω $f = x^n - a \in K[x]$. Δείξτε ότι το σώμα ριζών του f επί του F είναι $F(\sqrt[n]{a})$, όπου a μια ρίζα του f στο $\mathbb{C}$.

29. Έστω το πολυώνυμο $p = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

- i) Βρείτε το σώμα ριζών E του p .
 ii) Δείξτε ότι η πολλαπλασιαστική ομάδα E^* είναι κυκλική.
 iii) Δείξτε ότι $p = (x - a)(x - a^2)(x - a^4)$, όπου a είναι γεννήτορας της E^* .
 iv) Βρείτε τους αυτομορφισμούς του E και δείξτε ότι αποτελούν ομάδα ισόμορφη της $\mathbb{Z}_3$.

30. Βρείτε τους αυτομορφισμούς του σώματος $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

31. Δείξτε ότι: i) το πολυώνυμο $f = x^4 - 4x + 2 \in \mathbb{Q}[x]$ είναι ανάγωγο επί του $\mathbb{Q}$.

- ii) Για κάθε ρίζα ρ του f , $[\mathbb{Q}(\rho) : \mathbb{Q}] = 2^2 = 4$.
 iii) Το f αναλύεται σε γινόμενο δυο πολυωνύμων στο δακτύλιο $\mathbb{R}[x]$.
 iv) Οι ρίζες του ενός παράγοντα είναι

$$\frac{1}{2} \left[\rho \pm \sqrt{-\rho + \frac{8}{\sqrt{\rho}}} \right]$$

όπου ρ μια θετική ρίζα του πολυωνύμου $t^3 - 8t - 16$, το οποίο είναι ανάγωγο επί του $\mathbb{Q}$.

- v) Δύο τουλάχιστον ρίζες του f δεν είναι κατασκευάσιμες.

14

Συμμετρικές ομάδες

Στοιχειώδεις ιδιότητες των μεταθέσεων βρέθηκαν από τους Lagrange, Galois και Abel. Συστηματική μελέτη της ομάδας μεταθέσεων έγινε από τον Cauchy, σε μια σειρά εργασιών που δημοσιεύτηκαν το 1840.

Ο Cauchy ασχολήθηκε με ομάδες μόνο μεταθέσεων. Την αφηρημένη έννοια, δηλαδή τον αξιωματικό ορισμό της ομάδας, εισήγαγε ο Cayley το 1853.

Στον Cayley οφείλεται το σημαντικό αποτέλεσμα ότι κάθε πεπερασμένη ομάδα τάξης n είναι ισόμορφη με μια υποομάδα της συμμετρικής ομάδας S_n .

Η μέθοδος Lagrange για λύση εξισώσεων βαθμού ≤ 4 με πράξεις επί των συντελεστών και εξαγωγή ριζικών, στηρίζεται στην παρατήρηση ότι οι συντελεστές της εξίσωσης

$$x^n + a_1 x^{n-1} + \dots + a_n = 0 \quad (a_i \in \mathbb{C})$$

δεν μεταβάλλονται με τις μεταθέσεις των ριζών $p_1, p_2, \dots, p_n$. Η παρατήρηση αυτή είναι συνέπεια των σχέσεων των ριζών και συντελεστών της εξίσωσης

Ορισμός 1. Κύκλος μήκους λ λέγεται μια μετάθεση σ που αφήνει σταθερά όλα τα στοιχεία που είναι διάφορα των $a_1, a_2, \dots, a_\lambda$ και

$$a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} \dots a_{\lambda-1} \xrightarrow{\sigma} a_\lambda \xrightarrow{\sigma} a_1 \quad (1)$$

Π.χ. η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix} \in S_6$ είναι κύκλος μήκους 3, γιατί $\sigma(a) = a$ για $a = 1, 4, 6$ και $2 \mapsto 3 \mapsto 5 \mapsto 2$. Η μετάθεση (1) γράφεται σύντομα

$$\sigma = (a_1 a_2 \dots a_\lambda)$$

Προφανώς $(a_2 a_3 \dots a_\lambda a_1) = (a_3 a_4 \dots a_\lambda a_1 a_2) = \dots$

και
$$(a_1 a_2 \dots a_\lambda)^{-1} = (a_\lambda a_{\lambda-1} \dots a_2 a_1)$$

$$(a_1 a_2 \dots a_\lambda)^\lambda = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = e$$

Ορισμός 2. Δύο κύκλοι $(a_1, a_2, \dots, a_\lambda), (\beta_1, \beta_2, \dots, \beta_k)$ λέγονται ξένοι, αν $a_i \neq \beta_j$ για κάθε $1 \leq i \leq \lambda$ και $1 \leq j \leq k$. Ένας κύκλος (uv) μήκους δύο λέγεται **αντιμετάθεση**.

Πρόταση 1. Δύο ξένοι κύκλοι αντιμετατίθενται.

Απόδειξη. Έστω δύο ξένοι κύκλοι $a = (a_1, a_2, \dots, a_m), \beta = (\beta_1, \beta_2, \dots, \beta_k)$. Έχουμε

$$a\beta(a_j) = \beta(a(a_j)) = \beta(a_{j+1}) = a_{j+1} \quad (j < m)$$

$$a\beta(a_m) = \beta(a(a_m)) = \beta(a_1) = a_1 \quad (j = m)$$

$$a\beta(i) = i \text{ για } i \neq a_j, \beta_p$$

$$\beta a(a_j) = a(\beta(a_j)) = a(a_j) = a_{j+1} = a\beta(a_j)$$

$$\beta a(a_m) = a(\beta(a_m)) = a(a_m) = a_1$$

$$\beta a(i) = i \text{ για } i \neq a_j, \beta_p$$

και

$$\beta a(\beta_p) = a(\beta(\beta_p)) = a(\beta_{p+1}) = \beta_{p+1} = a\beta(\beta_p), \quad p < k$$

$$\beta a(\beta_k) = a(\beta(\beta_k)) = a(\beta_1) = \beta_1 = a\beta(\beta_1)$$

δηλαδή $\beta a(x) = a\beta(x)$ για κάθε $x \in \{1, 2, \dots, n\}$. □

Θεώρημα 1. Κάθε μετάθεση $\sigma \in S_n$ είναι γινόμενο ξένων κύκλων. Οι κύκλοι ορίζονται μονοσήμαντα, όχι όμως και η τάξη τούς στο γινόμενο.

Απόδειξη. Θεωρούμε τα στοιχεία

$$\sigma(1), \sigma^2(1), \sigma^3(1), \dots \quad (1)$$

Αφού το $S = \{1, 2, \dots, n\}$ είναι πεπερασμένο, τα στοιχεία αυτά δεν είναι διάφορα. Έστω $\sigma^m(1)$ ο πρώτος όρος της ακολουθίας (1), ο οποίος συμπίπτει με προηγούμενο όρο της. Τότε $\sigma^m(1) = 1$, γιατί, αν $\sigma^m(1) = \sigma^k(1)$ και $k < m$, θα είχαμε $\sigma^{m-k}(1) = 1$ με $m - k < m$, αντίθετα με την επιλογή του m . Έστω

$$\tau_1 = (1 \ \sigma(1) \ \sigma^2(1) \ \dots \ \sigma^{m-1}(1))$$

Έστω i το πρώτο στοιχείο του S που δεν εμφανίζεται στον κύκλο τ_1 . Θεωρούμε τα στοιχεία

$$i, \sigma(i), \sigma^2(i), \dots, \sigma^k(i), \dots \quad (2)$$

Όπως είπαμε παραπάνω αυτά είναι πεπερασμένα το πλήθος και αν $\sigma^k(i)$ είναι το πρώτο στοιχείο που ισούται με προηγούμενο, τότε $\sigma^k(i) = i$ και

$$\tau_2 = (i, \sigma(i), \dots, \sigma^{k-1}(i))$$

είναι ένας κύκλος. Συνεχίζοντας με τον ίδιο τρόπο κατασκευάζουμε τους κύκλους $\tau_3, \dots, \tau_s$ στους οποίους εμφανίζονται όλα τα στοιχεία του συνόλου $\{1, 2, \dots, n\}$. Προφανώς

$$\sigma = \tau_1 \tau_2 \cdots \tau_s \quad \square$$

Παράδειγμα 1. Η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

να γραφεί σαν γινόμενο ξένων κύκλων.

Έχουμε $\sigma(1) = 6, \sigma^1(1) = \sigma(6) = 1$, συνεπώς τον κύκλο

$$\tau_1 = \begin{pmatrix} 1 & 6 \\ 6 & 1 \end{pmatrix} = (1 \ 6)$$

Τα στοιχεία που δεν εμφανίζονται στον κύκλο τ_1 είναι 2, 3, 4, 5. Έχουμε

$$\sigma(2) = 5, \sigma^2(2) = 3, \sigma^3(2) = 2,$$

και συνεπώς τον κύκλο

$$\tau_2 = (2 \ 5 \ 3)$$

Τέλος έχουμε τον κύκλο $\tau_3 = \begin{pmatrix} 4 \\ 4 \end{pmatrix} = (4)$. Άρα

$$\sigma = (1\ 6)(2\ 5\ 3)(4)$$

Παράδειγμα 2. Στην ομάδα S_n ($n \geq 3$) ναδειχτεί ότι $(1\ 2)(1\ 3) = (1\ 2\ 3)$.

Έχουμε

$$\begin{aligned} (12)(13) &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix} = (123) \end{aligned}$$

Γεννήτορες της ομάδας S_n

Κάθε μετάθεση σ είναι γινόμενο ξένων κύκλων. Αλλά κάθε κύκλος $a = (a_1 a_2 \cdots a_m)$ είναι γινόμενο αντιμεταθέσεων, γιατί

$$a = (a_1 a_2)(a_1 a_3) \cdots (a_1 a_m).$$

Συνεπώς οι αντιμεταθέσεις (u, v) παράγουν την ομάδα S_n . Υπάρχει ένα γνήσιο υποσύνολο του συνόλου των αντιμεταθέσεων που παράγει την ομάδα S_n . Πραγματικά, οι μεταθέσεις

$$(1, 2), (1, 3), \dots, (1, n)$$

παράγουν την ομάδα S_n , γιατί

$$(1, u)(1, v)(1, u) = (u, v)$$

Συζυγείς μεταθέσεις

Δύο μεταθέσεις f, σ λέγονται **συζυγείς**, αν υπάρχει μετάθεση a τέτοια, ώστε $f = a^{-1}\sigma a$. Υποθέτουμε ότι η μετάθεση σ γράφεται σαν γινόμενο ξένων κύκλων μήκους $l_1, l_2, \dots, l_m$. Με αλλαγή της σειράς των κύκλων μπορούμε να υποθέσουμε ότι $l_1 \leq l_2 \leq \cdots \leq l_m$. Η m -άδα $(l_1, l_2, \dots, l_m)$ λέγεται **τύπος** της μετάθεσης σ . Π.χ. η μετάθεση

$$\sigma = (10)(1, 6)(3, 4)(2, 5, 7, 8, 9) \in S_{10}$$

είναι τύπου $(1, 2, 2, 5)$.

Πρόταση 2. Δύο μεταθέσεις είναι συζυγείς τότε και μόνο, όταν είναι του αυτού τύπου.

Απόδειξη. Έστω ότι οι μεταθέσεις $f, \sigma \in S_n$ είναι του αυτού τύπου. Τότε

$$\begin{aligned}\sigma &= (a_1 a_2 \cdots a_k)(\beta_1 \beta_2 \cdots \beta_\lambda) \cdots (\gamma_1 \gamma_2 \cdots \gamma_m) \\ f &= (a'_1 a'_2 \cdots a'_k)(\beta'_1 \beta'_2 \cdots \beta'_\lambda) \cdots (\gamma'_1 \gamma'_2 \cdots \gamma'_m)\end{aligned}$$

οπότε για

$$a = \begin{pmatrix} a_1 & \cdots & a_k & \beta_1 & \cdots & \beta_\lambda & \cdots & \gamma_1 & \cdots & \gamma_m & \cdots & i & \cdots \\ a'_1 & \cdots & a'_k & \beta'_1 & \cdots & \beta'_\lambda & \cdots & \gamma'_1 & \cdots & \gamma'_m & \cdots & i & \cdots \end{pmatrix}$$

έχουμε $a^{-1}\sigma a = f$. Πραγματικά, για τους κύκλους $g = (a_1 a_2 \cdots a_k)$, $h = (a'_1 a'_2 \cdots a'_k)$ έχουμε

$$\begin{aligned}a^{-1}ga &= \begin{pmatrix} a'_1 & \cdots & a'_k \\ a_1 & \cdots & a_k \end{pmatrix} \begin{pmatrix} a_1 & \cdots & a_k \\ a_2 & \cdots & a_1 \end{pmatrix} \begin{pmatrix} a_1 & \cdots & a_k \\ a'_1 & \cdots & a'_k \end{pmatrix} = \begin{pmatrix} a'_1 & \cdots & a'_k \\ a_2 & \cdots & a_1 \end{pmatrix} \begin{pmatrix} a_1 & \cdots & a_k \\ a'_1 & \cdots & a'_k \end{pmatrix} \\ &= \begin{pmatrix} a'_1 & a'_2 & \cdots & a'_k \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} = (a'_1 \cdots a'_k) = h\end{aligned}$$

και επειδή

$$a^{-1}\sigma a = a^{-1}(a_1 \cdots a_k)aa^{-1}(\beta_1 \cdots \beta_\lambda)a \cdots a^{-1}(\gamma_1 \cdots \gamma_m)a$$

έχουμε $a^{-1}\sigma a = f$. □

2. ΑΡΤΙΕΣ, ΠΕΡΙΤΤΕΣ ΜΕΤΑΘΕΣΕΙΣ

Η ανάλυση μιας μετάθεσης σε γινόμενο αντιμεταθέσεων δεν είναι μοναδική. Μια σταθερά στην ανάλυση αυτή είναι ο αριθμός των αντιμεταθέσεων που είναι πάντοτε άρτιος ή πάντοτε περιττός.

Για την απόδειξη αυτού εξετάζουμε την επίδραση μιας μετάθεσης σ σε μια συνάρτηση n μεταβλητών $F(x_1, x_2, \dots, x_n)$. Ορίζουμε

$$\sigma(F) = F(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

Π.χ., αν

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad F(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_4),$$

τότε $\sigma(F) = (x_2 - x_3)(x_2 - x_1)$. Αν

$$G(x_1, x_2, x_3, x_4) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)(x_4 - x_1)(x_4 - x_2)(x_4 - x_3) = \prod_{i,j=1, i>j}^4 (x_i - x_j)$$

τότε

$$\sigma(G) = (x_3 - x_2)(x_4 - x_2)(x_4 - x_3)(x_1 - x_2)(x_1 - x_3)(x_1 - x_4) = -G$$

Γενικά, αν

$$G = \prod_{i,j=1, i>j}^4 (x_i - x_j) \quad , \quad x_i \in \mathbb{R}$$

τότε

$$\sigma(G) = G \quad \text{ή} \quad -G$$

γιατί $|G|$ είναι το γινόμενο όλων των $|x_i - x_j|$, όπως και το $|\sigma(G)|$. Συνεπώς $|\sigma(G)| = |G|$, δηλαδή $\sigma(G) = \pm G$.

Λήμμα. Για κάθε αντιμετάθεση $\sigma = (u, v)$, $\sigma(G) = -G$.

Απόδειξη. Στο γινόμενο G έχουμε τις διαφορές $x_u - x_i, x_v - x_i$ με $i < u$ και η επίδραση της σ στο γινόμενό τους $A = (x_u - x_i)(x_v - x_i)$ είναι $\sigma(A) = (x_v - x_i)(x_u - x_i) = A$. Για $v < i$ έχουμε επίσης τις διαφορές $x_i - x_u, x_i - x_v$ και το γινόμενό τους $B = (x_i - x_u)(x_i - x_v)$ γίνεται $\sigma(B) = (x_i - x_v)(x_i - x_u) = B$. Αν $u < i < v$, το γινόμενο $\Gamma = (x_i - x_u)(x_v - x_i)$ γίνεται $\sigma(\Gamma) = (x_i - x_v)(x_u - x_i) = \Gamma$. Τέλος και η διαφορά $x_i - x_j$ μένει αναλλοίωτη με την επίδραση της σ . Όμως η διαφορά $x_v - x_u$ γίνεται $-(x_v - x_u)$. Άρα $\sigma(G) = -G$. $\square$

Θεώρημα 2. Αν $\sigma = \tau_1 \tau_2 \cdots \tau_k = \theta_1 \theta_2 \cdots \theta_m$ και τ_i, θ_j είναι αντιμεταθέσεις, τότε

$$(-1)^k G = (-1)^m G$$

δηλαδή k, m άρτιοι ή k, m περιττοί.

Απόδειξη. Έχουμε $\tau_k(G) = -G$, $\tau_{k-1}\tau_k(G) = -(-G) = (-1)^2 G, \dots \sigma(G) = (-1)^k G$. Όμοια $\sigma(G) = (-1)^m G$. $\square$

Ορισμός 3. Μια μετάθεση σ λέγεται **άρτια ή περιττή**, αν είναι γινόμενο άρτιου πλήθους αντίστοιχα περιττού πλήθους αντιμεταθέσεων.

3. ΕΝΑΛΛΑΣΟΥΣΑ ΥΠΟΟΜΑΔΑ ΤΗΣ S_n

Η συνάρτηση $\chi : S_n \rightarrow \{1, -1\}$ με τιμή $\chi(\sigma) = 1$, αν η σ είναι άρτια και $\chi(\sigma) = -1$, αν η σ είναι περιττή, είναι ομομορφισμός της ομάδας S_n επί της πολλαπλασιαστικής ομάδας $\{1, -1\}$. Ο πυρήνας είναι μια κανονική υποομάδα A_n της S_n ($n \geq 2$) με δείκτη 2.

Ορισμός 1. Το σύνολο A_n των άρτιων μεταθέσεων είναι κανονική υποομάδα της S_n και λέγεται **εναλλάσουςα** υποομάδα της S_n .

Πρόταση 1. Η ομάδα A_n παράγεται από τους κύκλους μήκους 3 της μορφής

$$(123), (124), \dots, (12n).$$

Απόδειξη. Κάθε μετάθεση $\sigma \in A_n$ είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων. Συνεπώς οι αντιμεταθέσεις αυτές χωρίζονται σε ζεύγη. Έχουμε

$$\begin{aligned}(ij)(kl) &= (ijk)(kil) \\ (ij)(ik) &= (ijk) \\ (ijk) &= (12i)^{-1}(2jk)(12i) \\ (2jk) &= (12j)^{-1}(12k)(12j) \\ (ijk) &= (12k)(12j)(12k)^{-1}\end{aligned}$$

Οι δύο πρώτες ισότητες αποδεικνύουν ότι η A_4 παράγεται από όλους τους κύκλους μήκους 3. Οι υπόλοιπες ισότητες αποδεικνύουν ότι κάθε κύκλος μήκους 3 εκφράζεται με τους κύκλους $(12i)$ για $i = 3, 4, \dots, n$. $\square$

Θεώρημα (Abel) 1. Η ομάδα A_n για $n \geq 5$ είναι απλή.

Απόδειξη. Έστω $K \trianglelefteq A_n$, $K \neq \{e\}$. Θ' αποδείξουμε ότι $K = A_n$. Θ' αποδείξουμε πρώτα ότι η ομάδα K περιέχει μια μετάθεση της μορφής $(ij)(km)$. Για κάθε μετάθεση $\sigma \in K$ και $\varphi \in A_n$, έχουμε

$$\sigma\varphi\sigma^{-1}\varphi^{-1} = \sigma(\varphi\sigma^{-1}\varphi^{-1}) \in K$$

Σε κάθε περίπτωση η ομάδα K περιέχει μια μετάθεση σ της μορφής $(i-iv)$ του παρακάτω πίνακα και για την αναφερόμενη στον πίνακα μετάθεση $\varphi \in A_n$, βρίσκουμε την μετάθεση $\sigma\varphi\sigma^{-1}\varphi^{-1}$

	σ	φ	$\sigma\varphi\sigma^{-1}\varphi^{-1}$
i	$(a\beta\gamma\delta\dots)\dots$	$(\beta\gamma\delta)$	(a, δ, γ)
ii	$(a, \beta, \gamma)(\delta, \epsilon, \dots)\dots$	$(\beta\gamma\epsilon)$	$(a, \epsilon, \gamma, \beta, \delta)$
iii	$(a\beta\gamma)$	$(\beta\gamma\delta)$	$(a, \delta)(\beta, \gamma)$
iv	$(a\beta)(\gamma, \delta)\dots$	$(a\beta\gamma)$	$(a, \delta)(\beta, \gamma)$

Στην πρώτη περίπτωση τουλάχιστον τέσσερα στοιχεία δεν μένουν σταθερά, στη δεύτερη 5, στην τρίτη 3 ακριβώς και στην τέταρτη 4 τουλάχιστον. Η περίπτωση (ii) ανάγεται στην (i) και η (i) στη (iii). Στη συνέχεια αποδεικνύουμε ότι η K περιέχει όλες τις μεταθέσεις της μορφής $(a, \beta)(\gamma, \delta)$.

Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $(1, 2)(3, 4) \in K$. Οι μεταθέσεις

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ a & \beta & \gamma & \delta & \dots \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & \dots \\ \beta & a & \gamma & \delta & \dots \end{pmatrix}$$

διαφέρουν κατά μια αντιμετάθεση. Συνεπώς μια από αυτές ανήκει στην ομάδα A_n . Για οποιαδήποτε από αυτές, έστω σ , έχουμε, αφού $K \trianglelefteq A_4$,

$$\sigma^{-1}(1, 2)(3, 4)\sigma = (a, \beta)(\gamma, \delta) \in K.$$

Τέλος οι μεταθέσεις $(a, \beta)(\gamma, \delta)$ παράγουν την ομάδα A_n . Επειδή για $n \geq 5$, υπάρχουν $\xi, \eta \neq a, \beta, \gamma, \delta$ έχουμε

$$(a, \beta)(a, \delta) = (a, \beta)(\xi, \eta)(\xi, \eta)(a, \delta) \in \langle (a, \beta)(\gamma, \delta) \rangle$$

και άρα το συμπέρασμα. □

4. ΟΜΑΔΕΣ ΙΣΟΜΟΡΦΕΣ ΜΕ ΟΜΑΔΕΣ ΜΕΤΑΘΕΣΕΩΝ

Όπως έχουμε αναφέρει ένα σοβαρότατο πρόβλημα της θεωρίας των ομάδων είναι η ταξινόμηση των ομάδων, η καταγραφή δηλαδή σ' ένα πίνακα όλων των μη ισόμορφων ομάδων. Για κάθε ομάδα συνεπώς θα υπάρχει μια ισόμορφη ομάδα στον πίνακα. Η πρώτη αντιμετώπιση του προβλήματος φαίνεται απελπιστική. Το θεώρημα Cayley, που ακολουθεί, μεταθέτει το πρόβλημα της ταξινόμησης των πεπερασμένων ομάδων σ' εκείνο των πεπερασμένων ομάδων μεταθέσεων.

Θεώρημα (Cayley) 1. Κάθε ομάδα είναι ισόμορφη με μια υποομάδα μιας ομάδας μεταθέσεων.

Απόδειξη. Έστω G μια ομάδα και $a \in G$. Θεωρούμε τη συνάρτηση $f_a : G \rightarrow G$ με τιμή $f_a(x) = ax$. Η f_a είναι στοιχείο της συμμετρικής ομάδας S_G της ομάδας G . Πραγματικά, είναι αμφιμονοσήμαντη, γιατί $f_a(x) = f_a(y)$ συνεπάγεται $ax = ay$ και συνεπώς $x = y$. Είναι επί του G , γιατί $y = aa^{-1}y = f_a(a^{-1}y)$. Ορίζουμε τώρα μια συνάρτηση $F : G \rightarrow S_G$ θέτοντας $F(a) = f_a$. Η συνάρτηση είναι ομομορφισμός, γιατί $F(ab) = f_{ab}$ και $f_{ab}(x) = (ab)x = a(bx) = f_a(bx) = f_a \circ f_b(x)$, δηλαδή $f_{ab} = f_a \circ f_b = F(a) \circ F(b)$. Τέλος η

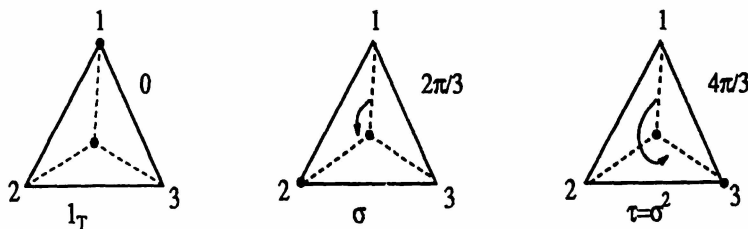
F είναι ισομορφισμός, γιατί $\ker F = \{1_G\}$, αφού $F(a) = 1_G$ τότε και μόνο, όταν $ax = x$ ή $a = e$. $\square$

Πόρισμα. Μια πεπερασμένη ομάδα G τάξης n είναι ισόμορφη με μια υποομάδα της ομάδας S_n .

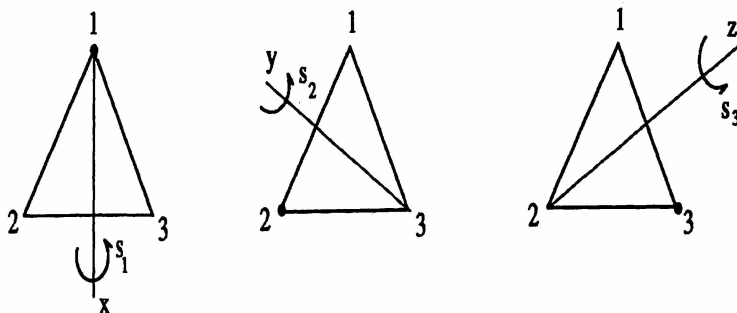
Στη συνέχεια δίνουμε παραδείγματα ομάδων και τις υποομάδες μεταθέσεων προς τις οποίες είναι ισόμορφες. Θα θεωρήσουμε ομάδες που εμφανίζονται στη Γεωμετρία. **Μετασχηματισμός** ενός συνόλου A στη Γεωμετρία, είναι μια συνάρτηση $f : A \rightarrow A$ αμφιμονοσήμαντη και επί, είναι δηλαδή μια μετάθεση του A .

Παράδειγμα 1. Οι μετασχηματισμοί που απεικονίζουν ένα ισόπλευρο τρίγωνο T στον εαυτό του αποτελούν μια ομάδα $\mathfrak{D}_3$ ισόμορφη της συμμετρικής ομάδας S_3 .

Απόδειξη. Οι μετασχηματισμοί που απεικονίζουν ένα ισόπλευρο τρίγωνο στον εαυτό του είναι οι στροφές $1_T, \sigma, \tau$ του επιπέδου του γύρω από το κέντρο του κατά γωνία $0^\circ, \frac{2\pi}{3}, \frac{4\pi}{3}$



και οι συμμετρίες s_1, s_2, s_3 ως προς τους άξονες x, y, z



Εύκολα βλέπουμε ότι $\mathcal{D}_3$ είναι μια ομάδα ως προς τη σύνθεση με πίνακα

	1_T	σ	σ^2	s_1	s_2	s_3	
1_T	1_T	σ	σ^2	s_1	s_2	s_3	$s_2 = \sigma s_1$
σ	σ	σ^2	1	s_2	s_3	s_1	
σ^2	σ^2	1	σ	s_3	s_1	s_2	
s_1	s_1	s_3	s_2	1	σ^2	σ	$s_3 = \sigma^2 s_1$
s_2	s_2	s_1	s_3	σ	1	σ^2	
s_3	s_3	s_2	s_1	σ^2	σ	1	

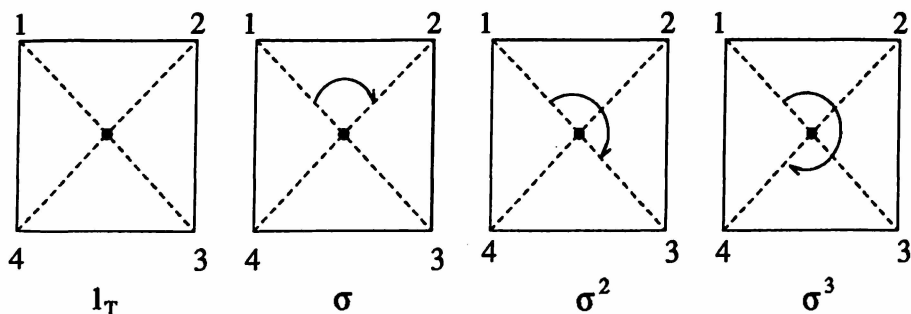
Η συνάρτηση της ομάδας $\mathcal{D}_3$ στην S_3 με πίνακα τιμών

x	1_T	σ	σ^2	s_1	s_2	s_3
$f(x)$	1_S	(123)	(132)	(23)	(12)	(13)

είναι ισομορφισμός της $\mathcal{D}_3$ επί της S_3 . Η διαπίστωση είναι άμεση, αν γράψουμε τον πίνακα της ομάδας S_3 . Θα παρατηρήσουμε ότι προκύπτει από τον πίνακα της $\mathcal{D}_3$ με την αντικατάσταση $x \mapsto f(x)$.

Παράδειγμα 2. Οι μετασχηματισμοί που απεικονίζουν ένα τετράγωνο στον εαυτό του αποτελούν μια ομάδα $\mathcal{D}_4$ ισόμορφη με υποομάδα της S_4 .

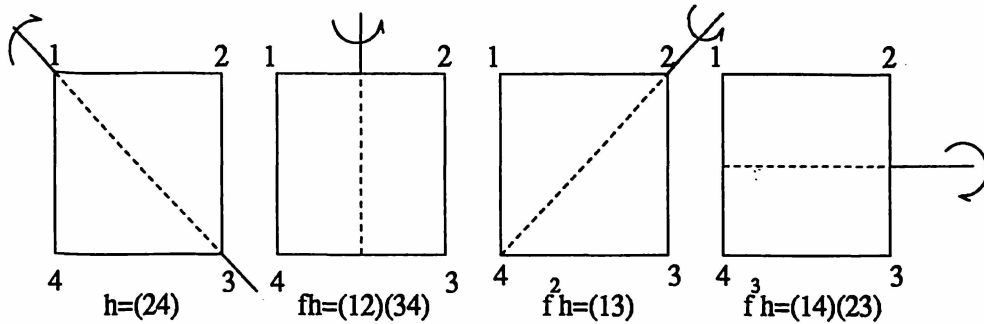
Απόδειξη. Οι στροφές του τετραγώνου γύρω από το κέντρο του κατά γωνίες $0^\circ, \frac{2\pi}{4}, 2 \cdot \frac{2\pi}{4}, 3 \cdot \frac{2\pi}{4}$ απεικονίζουν το τετράγωνο στον εαυτό του



Οι στροφές αυτές παρίστανται με τις εξής μεταθέσεις της ομάδας $S = S_4$:

$$1_S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad f = (1 \ 2 \ 3 \ 4), \quad f^2 = (1 \ 3)(2 \ 4), \quad f^3 = (1 \ 4 \ 3 \ 2)$$

Οι άλλοι μετασχηματισμοί που απεικονίζουν το τετράγωνο στον εαυτό του είναι οι συμμετρίες ως προς μια διαγώνιο και ως προς μια μεσοκάθετο των πλευρών του



Συνεπώς οι μετασχηματισμοί που απεικονίζουν ένα τετράγωνο στον εαυτό του αποτελούν μια ομάδα $\mathfrak{D}_4$ τάξης 8, η οποία παράγεται από τους μετασχηματισμούς σ, h που ορίστηκαν παραπάνω και είναι ισόμορφη με γνήσια υποομάδα της S_4 , γιατί $|S_4| = 24$.

Διεδρική ομάδα $\mathfrak{D}_n$

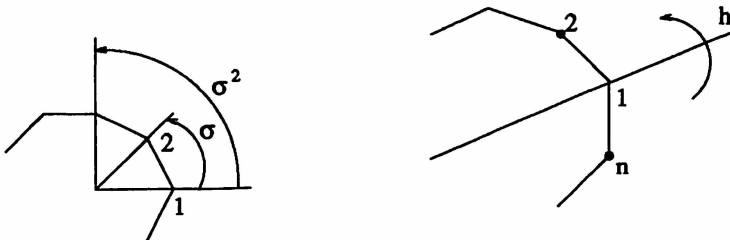
Οι μετασχηματισμοί που απεικονίζουν ένα κανονικό πολύγωνο στον εαυτό του λέγονται **συμμετρίες** του κανονικού πολυγώνου. Έστω $\mathfrak{D}_n$ το σύνολο των συμμετριών ενός κανονικού n -γώνου. Είδαμε στα παραδείγματα 1, 2 ότι $\mathfrak{D}_3, \mathfrak{D}_4$ είναι ομάδες και μάλιστα ότι

$$\mathfrak{D}_3 = \langle \sigma, s_1; \sigma^3 = 1, s_1^2 = 1, \sigma s_1 \sigma = s_1^{-1} \rangle \cong S_3$$

$$\mathfrak{D}_4 = \langle \sigma, h; \sigma^4 = 1, h^2 = 1, \sigma h \sigma = h^{-1} \rangle \cong \langle (1234), (24) \rangle$$

λέγονται **ομάδες συμμετριών** του ισοπλεύρου τριγώνου αντίστοιχα του τετραγώνου.

Θ' αποδείξουμε ότι οι συμμετρίες ενός κανονικού n -γώνου P_n αποτελούν μια ομάδα $\mathfrak{D}_n$ τάξης $2n$. Έστω e ο ταυτοτικός μετασχηματισμός του P_n και σ η στροφή κατά γωνία $\frac{2\pi}{n}$ γύρω από το κέντρο του.



Προφανώς $\sigma^n = e$ και

$$e, \sigma, \sigma^2, \dots, \sigma^{n-1}$$

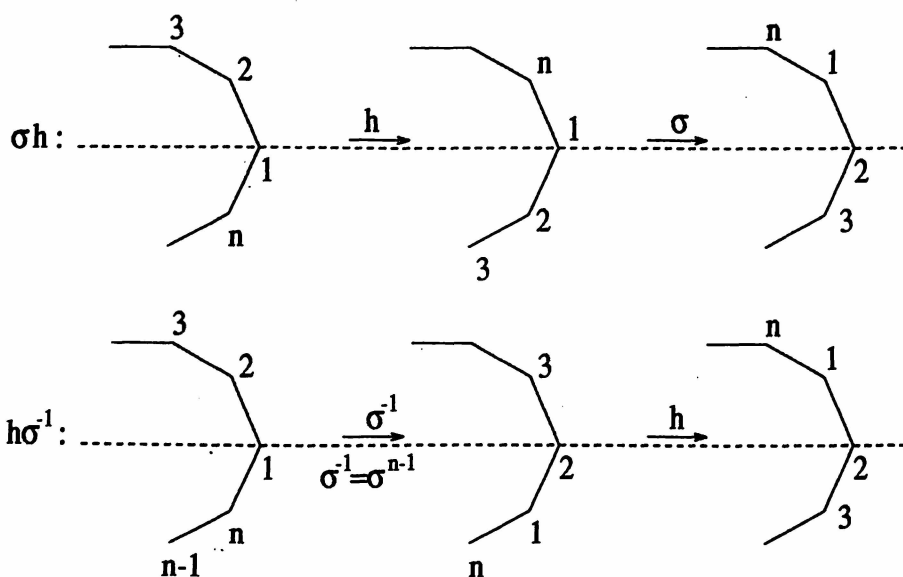
είναι διάφορες συμμετρίες του P_n . Έστω h η στροφή του πολυγώνου P_n γύρω από ένα άξονα συμμετρίας. Τα στοιχεία

$$e, \sigma, \sigma^2, \dots, \sigma^{n-1}, h, \sigma h, \sigma^2 h, \dots, \sigma^{n-1} h \quad (1)$$

αποτελούν μια ομάδα τάξης $2n$. Είναι η ομάδα $\mathfrak{D}_n$ των συμμετριών του κανονικού πολυγώνου P_n και λέγεται **διεδρική ομάδα τάξης n** .

Απόδειξη. Κάθε συμμετρία του P_n ορίζεται από τις εικόνες δύο διαδοχικών κορυφών του, π.χ. των 1, 2. Η εικόνα της κορυφής 1 μπορεί να είναι οποιαδήποτε από τις n κορυφές και η εικόνα της κορυφής 2 μια από τις γειτονικές κορυφές της εικόνας της 1. Συνεπώς η ομάδα $\mathfrak{D}_n$ έχει τάξη $2n$. $\square$

Αν η εικόνα της κορυφής 1 είναι η κορυφή $m+1$, η εικόνα της 2 θα είναι η κορυφή $m+2$ ή m . Αν η εικόνα της κορυφής 2 είναι $m+2$, η συμμετρία είναι σ^m . Αν η εικόνα της κορυφής 2 είναι m , η συμμετρία είναι $\sigma^m h$. Αλλά όπως φαίνεται από το παρακάτω σχήμα, έχουμε $\sigma h = h \sigma^{-1}$



συνεπώς $h \sigma h = \sigma^{-1}$, $h \sigma^m h = \sigma^{-m}$, $\sigma^m h = h \sigma^{-m} = h \sigma^{n-m}$. Επειδή

$$\begin{aligned} (\sigma^i h) \sigma^j &= \sigma^i h \sigma^j = \sigma^i \sigma^{n-j} h = \sigma^{n+i-j} h \\ (\sigma^i h) (\sigma^j h) &= \sigma^i h \sigma^j h = \sigma^i \sigma^{n-j} h h = \sigma^{n+i-j} \end{aligned}$$

η διεδρική ομάδα τάξης n είναι

$$\mathfrak{D}_n = \{e, \sigma, \sigma^2, \dots, \sigma^{n-1}, h, \sigma h, \sigma^2 h, \dots, \sigma^{n-1} h\}.$$

Για $n \geq 3$ η διεδρική ομάδα $\mathcal{D}_n$ δεν είναι αντιμεταθετική, γιατί $sh = hs^{-1} \neq hs$, συνεπώς δεν είναι ούτε κυκλική.

Θα χαρακτηρίσουμε κατά προσέγγιση ισομορφισμού τις πεπερασμένες ομάδες συμμετριών ενός επίπεδου σχήματος με ένα σταθερό σημείο.

Υπάρχουν επίπεδα σχήματα, των οποίων η συμμετρική ομάδα είναι άπειρη. Π.χ. οι συμμετρίες του κύκλου με ένα σταθερό σημείο, το κέντρο του, είναι άπειρες.

Θεώρημα 2. Κάθε πεπερασμένη υποομάδα της ομάδας των στροφών του επιπέδου είναι ισόμορφη με μια κυκλική ομάδα.

Απόδειξη. Κάθε στροφή A του επιπέδου γύρω από την αρχή ορίζεται από μια γωνία $\theta(A)$, με $0 \leq \theta(A) < 2\pi$. Έστω G μια πεπερασμένη υποομάδα της ομάδας των στροφών. Εκλέγουμε τη στροφή $A \in G$, έτσι ώστε $\theta(A)$ να είναι η μικρότερη θετική γωνία. Για κάθε $B \in G$, υπάρχει ακέραιος m με $m\theta(A) \leq \theta(B) < (m+1)\theta(A)$. Επειδή $\theta(BA^{-m}) = \theta(B) - m\theta(A)$, έχουμε $0 \leq \theta(BA^{-m}) < \theta(A)$. Συνεπώς $\theta(BA^{-m}) = 0$, $BA^{-m} = I$, $B = A^m$ και η G είναι κυκλική. $\square$

Θεώρημα 3. Κάθε πεπερασμένη υποομάδα της ομάδας των ορθογώνιων μετασχηματισμών του επιπέδου είναι ισόμορφη με μια κυκλική ή διεδρική ομάδα.

Απόδειξη. Η ομάδα των ορθογώνιων μετασχηματισμών του επιπέδου είναι ισόμορφη της ομάδας των ορθογώνιων πινάκων 2×2 των πινάκων δηλαδή A με $A^t A = I$. Οι πίνακες αυτοί έχουν* μια από τις παρακάτω μορφές

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \quad \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

Έστω G μια πεπερασμένη υποομάδα της ομάδας των ορθογώνιων πινάκων. Η συνάρτηση $f: G \rightarrow \{1, -1\}$ με $f(x) = \det x$ είναι ομομορφισμός ομάδων. Ο πυρήνας K αυτού είναι κανονική υποομάδα της G δείκτη 1 ή 2. Αν ο δείκτης είναι 1, η G περιέχει πίνακες της πρώτης μορφής, δηλαδή η G είναι ισόμορφη με μια πεπερασμένη ομάδα στροφών του επιπέδου, συνεπώς είναι κυκλική. Αν ο δείκτης είναι 2, τότε

$$G = K \cup AK = \{1, K, K^2, \dots, K^{n-1}, A, KA, K^2A, \dots, K^{n-1}A\}$$

με $A = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$ για κάποιο $\theta \in \mathbb{R}$. Άρα η G είναι ισόμορφη με τη διεδρική ομάδα τάξης n . $\square$

* βλ. Γραμμική Αλγεβρα II, Στρατηγόπουλος - Κοντολάτου

ΑΣΚΗΣΕΙΣ

1-6 Βρείτε τις μεταθέσεις

1. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

2. $(1\ 2\ 3\ 4\ 5)(2\ 3\ 4)$

3. $(3\ 6\ 2)(1\ 5)(4\ 2)$

4. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix}^3$

5. $(1\ 2\ 3)^{-1}, (1\ 2\ 4\ 6\ 5\ 7)^{-2}$

6. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}^{-1}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}^{-1}$

7. Γράψτε τις παρακάτω μεταθέσεις ως γινόμενο ξένων κύκλων

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 6 & 5 & 7 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 4 & 2 & 7 & 3 & 5 & 1 & 6 \end{pmatrix}$$

8. Βρείτε την τάξη της μετάθεσης

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}$$

9. Ποιές μεταθέσεις $\theta \in S_4$ αφήνουν αναλλοίωτο το πολυώνυμο $x_1^2 - 2x_2^2 + 2x_3 + x_4^2$; Αποτελούν υποομάδα της S_4 ;

10. Δείξτε ότι το πλήθος των αντιμεταθέσεων του S_n είναι $\frac{n(n-1)}{2}$.

11. Έστω $E = \mathbb{R}^* \times \mathbb{R}$. Στο E ορίζουμε ένα εσωτερικό νόμο T θέτοντας $(a, \beta)T(a', \beta') = (aa', a\beta' + \beta)$.

i) Δείξτε ότι (E, T) είναι ομάδα.

ii) Η ομάδα (E, T) είναι ισόμορφη με μια υποομάδα της συμμετρικής ομάδας του $\mathbb{R}$.

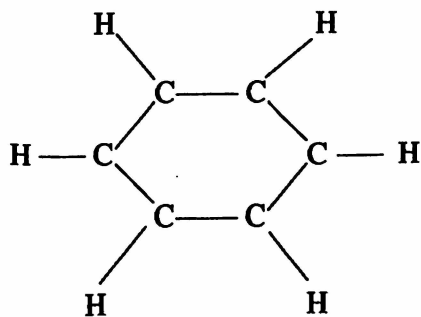
12. Αν φ είναι κύκλος μήκους λ στην συμμετρική ομάδα S_n , δείξτε ότι $f^{-1}\varphi f$ είναι κύκλος μήκους λ για κάθε $f \in S_n$.

13. Έστω $\varphi = (ax\beta), \sigma = (\beta\gamma\gamma)$. Δείξτε ότι $\varphi^{-1}\sigma^{-1}\varphi\sigma$ είναι κύκλος μήκους 3.

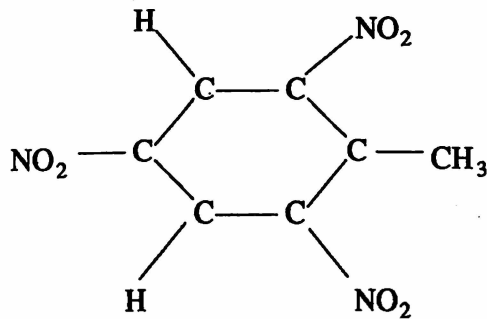
14. Βρείτε όλες τις δεξιές κλάσεις της ομάδας A_3 στην S_3 .
15. Έστω $\rho = (1234)$, $\varphi = (24)$. Δείξτε ότι $\langle \rho, \varphi \rangle \cong \mathcal{D}_4$.
16. Έστω G μια ομάδα και a, β δύο στοιχεία τάξης 5 και 2 αντίστοιχα. Αν $a^4\beta = \beta a$, δείξτε ότι $\langle a, \beta \rangle \cong \mathcal{D}_5$.
17. Δείξτε ότι οι αυτομορφισμοί της ομάδας $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι ομάδα ισόμορφη της S_3 .
18. Βρείτε 4 διάφορες υποομάδες της S_4 ισόμορφες της S_3 και 9 υποομάδες ισόμορφες της S_2 .
19. Βρείτε όλους τους ομομορφισμούς της ομάδας $(\mathbb{Z}, +)$ στην διεδρική ομάδα $\mathcal{D}_4$.
20. Δείξτε ότι $\mathcal{D}_6 \cong S_3 \times S_2$.
21. Δείξτε ότι

$$\text{Aut } \mathbb{Z} \cong \mathbb{Z}_2, \quad \text{Aut } \mathbb{Z}_3 \cong \mathbb{Z}_2, \quad \text{Aut } \mathbb{Z}_4 \cong \mathbb{Z}_2, \quad \text{Aut } \mathbb{Z}_6 \cong \mathbb{Z}_2.$$
22. Βρείτε όλες τις υποομάδες της διεδρικής ομάδας $\mathcal{D}_5$.
23. Δείξτε ότι η διεδρική ομάδα $\mathcal{D}_5$ είναι ισόμορφη της ομάδας που παράγεται από τους πίνακες

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} j & 0 \\ 0 & j-1 \end{pmatrix}, \quad \text{όπου } j = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$
24. Έστω G μια ομάδα και δύο στοιχεία a, β αυτής τάξης 2. Αν το $a\beta$ έχει τάξη n , δείξτε ότι $\langle a, \beta \rangle \cong \mathcal{D}_n$.
25. Βρείτε την ομάδα των στροφών ενός κανονικού τετραέδρου (η στροφή γίνεται γύρω από άξονα συμμετρίας).
26. Βρείτε την ομάδα συμμετριών των παρακάτω χημικών ενώσεων (οι $C-C$ δεσμοί είναι ισοδύναμοι)



Βενζόλιο,



Τρινιτροτολουόλιο

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ALEXANROFF, P.S., *Introduction à la théorie des groupes*, Dunod, Paris, 1968(Μετάφραση Α. Gloden).
2. BECKER, C., CHEVALLET, J., *Algèbre Générale*, Armand Colins, Paris, 1972.
3. BOURBAKI, N., *Algèbre, I ch.1-3*, Hermann, Paris, 1970.
4. CALVO, B., - *Exercices d'algèbre*, Armand Colin, Paris, 1971.
5. COHN, P., *Algebra*, John Wiley & Sons, 1974.
6. DAVEDOV, A., *Polynomes et Algèbre linéaire*, Vuibert, Paris, 1979.
7. DORNHOFF, L., HOHN, F., *Applied Modern Algebra*, MacMillan Publishing, 1978.
8. FRALEIGH, J., *A First Course in Abstract Algebra*, Addison-Welsey Publishing Co., 1976.
9. FREDON, D. - Y. SUREAU, *Algèbre*, Armand Colin, 1987.
10. GILBERT, W., *Modern Algebra with Applications*, John Wiley & Sons, 1976.
11. GODEMENT, R., *Algebra*, Hermann, 1968.
12. GOLDSTEIN, L., *Abstract Algebra*, Prentice - Hall, 1973.
13. GRIFFITHS, H. & HILTON, P., *Classical Mathematics*, Van Nostrand Reinhold, 1970.
14. HILLMAN, A. - ALEXANRSON, G., *A First Undergraduate Course in Abstract Algebra*, Wadsworth Publishing Co. 1978.
15. HUA L-K, *Introduction to Number Theory*, Springer-Verlag, 1982.
16. KOCHENDORFFER, R., *Introduction to Algebra*, Wotler - Noordhoff Publishing, 1972.
17. LANG, S., *Algebra*, Addison-Welsey Publishing, 1965.
18. LELONG-FERRAND, J., *Algèbre*, Dunod, 1978.

19. Mac LANE, S.-BIRKHOFF, G., *Solution développés des exercices Wetez-Hocque Miller J.*, Gauthier-Villars, 1972.
20. MUTAFIAN, C., *Le défi algébrique*, Vuiber, 1976.
21. PEASTAINGS, F.-SEVIN, J., *L' Algèbre*, Vuibert, 1980.
22. QUERRÉ, J., *Cours D' Algèbre*, Masson, 1976.
23. WARNER, S., *Classical Modern Algebra*, Prentice-Hall, 1971.
24. WALLACE, D., *Groups*, George Allen & Unwin Ltd, 1974.

Ευρετήριο

- Abel, 264
 Θεώρημα, 271
Bernstein, 64
Bezout ταυτότητα, 216
Boole, 71
Boole George, 19
Burali-Forti, 70
Cantor, 65, 66, 70
 παράδοξο, 70
Cauchy, 264
 ακολουθίες, 194
Cayley, 264, 272
Cohen, 66
De la Vallee Poussin, 92
Dedekind, 223
Dirichlet, 223
Eisenstein, 249
 κριτήριο, 226, 227
Euler, 222, 256, 124, 104
Fermat, 124, 222
 διοφαντική εξίσωση, 101
 θεώρημα, 137, 223, 232
Frobenius, 180
Galois, 145, 180, 264
Gauss, 210
 Λήμμα, 225, 226
Gelfond, 246
Hadamard, 92
Hasse, 37, 40
Hermite, 244
Hilbert, 246
Klein, 137, 154, 172
Kummer, 222, 223
Lagrange, 264
 θεώρημα, 132, 136
Legendre, 92
Lehmer, 91
Lindemann, 244, 255
Liouville, 244
modulo, 119
Pierce και DeMorgan, 23
Riemann, 92
Russel παράδοξο, 70
Schneider, 246
Taylor, 235-237
Tchebycheff, 92
Wilson, 125
Zorn, 71
Αλγεβρα Boole, 19
Διόφαντος, 101
Δυναμοσύνολο, 20
Ερατοσθένης, 91
Ευκλείδης, 92, 94, 250
 αλγόριθμος του, 216, 237
Θεώρημα πρώτων αριθμών, 92
Πυθαγόρας πίνακας, 43
ακολουθία ιδεωδών, 214, 224
ακέραια περιοχή, 182, 205, 209, 218, 232, 233, 235
 αντιμεταθετική, 182, 212
αντι-ισομορφισμός, 39
αντιστρέψιμο-ς,-οι, 124
 αριστερά, 124
 δεξιά, 124
 πίνακες, 136
αντίστροφο, 46, 114, 115, 117, 120-123, 130
 αριστερό, 46, 123
 δεξιά, 46
 δεξιό, 122, 123
αξιώματα, 70
αριθμοί ακέραιοι, 53

- ρητοί, 53, 56
 αλγεβρικοί, 244
 κατασκευάσιμοι, 251
 υπερβατικοί, 244
 φυσικοί, 51
 αρχή δυϊσμού, 72
 αυτομορφισμός, 154, 189
 εσωτερικός, 160, 161
 γραφική παράσταση, 26
 δακτύλιος, 67
 αντιμεταθετικός, 68
 μοναδιαίος, 68
 δακτύλιος,-οι, 116, 165
 Boole, 119
 Gauss, 118, 210, 217
 ακεραίων, 119
 ακολουθιών, 194
 ακέραια περιοχή, 117
 αντιμεταθετικός, 117, 120, 185,
 189, 194, 199
 μοναδιαίος, 230, 231
 εμφύτευση, 181
 επεκτάσεις, 181
 ευκλείδειοι, 210, 211, 216, 217, 225
 ιδεώδεις, 143, 149, 176, 188, 190,
 192, 206
 κλασμάτων, 185
 κύριοι, 209, 213, 215, 218, 224
 μηδενικός, 194
 μιγαδικών, 118
 μοναδιαίος, 117, 119, 120
 μονοσήμαντης παραγοντοποίησης,
 222–225, 227
 ομομορφισμοί, 175
 πηλίκο, 143, 148, 149
 πολυωνύμων, 198, 203, 227
 διαιρετότητα, 89, 209, 211
 ακέραιοι, 89
 διαιρέτης, 91, 212, 125
 αριστερός, 117
 δεξιός, 117
 μηδενός, 117, 120
 διακρίνουσα, βλ. πολώνυμο 237
 διαστήματα, 36
 διατεταγμένα ζεύγη, 21
 διατάξεις, 79
 διαφορά συνόλων, 21
 διαίρεση, 91, 90
 διπλασιασμός κύβου, 250, 254
 διάγραμμα αντιμεταθετικό, 157
 δομή,-ες 42, 43, 113
 αλγεβρική, 129, 165
 επέκταση, 184
 αντιμεταθετική, 114
 βασικές αλγεβρικές, 66
 προσθετική, 66
 ελάχιστο κοινό πολλαπλάσιο, 96
 ενδομορφισμός, 154
 εξωτερικός νόμος, 42
 εξίσωση Διοφαντική, 101
 επιμεριστικός, 116
 επιμορφισμός, 154, 156, 169, 175
 κανονικός, 157, 176
 επέκταση, 143
 αλγεβρική, 247, 250
 απλή, 199, 243
 βαθμός, 243
 διάσταση, 243
 ισομορφισμός, 260
 πεπερασμένη, 243, 247, 250
 τετραγωνική, 254
 εσωτερικός νόμος διμελούς, 42
 ιδιότητες αντιμεταθετική, 45
 επιμεριστική, 49
 προσεταριστική, 45
 ευθύ γινόμενο, 166, 167, 169
 εσωτερικό, 168
 άθροισμα, 166
 ευκλείδεια στάθμη, 210, 211
 ημιομάδα, 113, 115, 122, 124, 165
 θεώρημα, 18
 Κινέζικο, 101, 103
 αριθμητική, 95
 ιδεώδεις, 211
 αριστερό, 189, 190, 192
 γνήσιο, 189
 δεξιό, 189, 190, 192
 κύριο, 190, 206, 209, 212, 249

- μηδενικό, 189
- μέγιστο, 193, 213
- παραγόμενο, 189
- πρώτο, 213
- άθροισμα, 192
- πρώτο, 194
- ισομορφισμός, 39, 154, 157, 169, 175, 200
- K-ισομορφισμός, 260
- επεκτάσεων, βλ. επέκταση 260
- πρώτο θεώρημα, 157
- σωμάτων, 214
- φυσικός, 181
- ισόμορφος, 181
- καρτεσιανό γινόμενο, 21
- κλάση, 119
 - ακεραίου, 119
 - ακεραίων modulo m , 34
 - αντιπρόσωπος, 32
 - αριστερή, 133, 144, 146
 - δεξιά, 144
 - πληθάριθμος, 57
 - στοιχείου, 32
 - σχέσης ισοδυναμίας, 32
- κοινό πολλαπλάσιο, 96, 218
- ελάχιστο, 96, 218
- κοινός διαιρέτης, 93, 215
- μέγιστος, 93, 215
- κάτω πέρας, 41
- κάτω φράγμα, 41
- κύκλος,-οι
 - αντιμετάθεση, 266
 - μήκους λ , 266
 - ξένοι, 266
- μεταθέσεις, 79
- μεταθέτης, 162
- μετασχηματισμοί, 153
- μετάθεση,-εις, 265
 - περιττές, 269, 270
 - συζυγείς, 268
 - τύπος, 268
 - άρτια, 270, 269
- μονοειδές, 113, 165
- μονομορφισμός, 154
- μονώνυμο, 234
- νόμοι εσωτερικοί εξωτερικοί, 42, 69
 - πίνακας, 43
 - επέκταση, 44
 - ποιοτικές ιδιότητες, 44
- ομομορφισμός, 153, 157, 170, 179, 199, 230
- Frobenius, 180
- αμφιμονοσήμαντος, 201
- εικόνα, 154
- εκτίμησης, 231
- μηδενικός, 189
- πυρήνας, 154, 175
- ταυτοτικός, 200, 230
- ομάδα, 67, 113, 131
 - S_n , 268
 - Γεννήτορες, 268
- Klein, 137, 154, 166, 172
- αβελιανή, 67
- αντιμεταθετική, 67, 69, 116, 147, 149
- ανάγωγος, 171
- αυτομορφισμοί, 161
- διεδρική, 276
- ευθύ γινόμενο, 165
- ισόμορφες, 272
- ισόμορφη, 153, 154
- κυκλική, 134-136, 166
 - πεπερασμένη, 138
 - ταξινόμηση, 159
 - υποομάδες, 138
- μεταθέσεων, 272
- ομομορφισμοί, 152
- ομόμορφη, 154
- ορισμοί, 122
- πεπερασμένη, 132, 145, 264
- πηλίκο, 143, 144, 158
- πολλαπλασιαστική, 131, 133, 135
- προσθετική, 131, 136
- συμμετρικές, 264
- συμμετρική, 173
- ταξινόμηση, 272
- τάξη, 132, 136, 154
- ουδέτερο, 116, 117, 123, 130, 132, 134

- αριστερά, 45
- αριστερό, 123
- δεξιά, 45
- δεξιό, 123
- στοιχείο, 113
- παράγωγος πολυωνύμου, 233
- πηλίκο, 91
- πληθάριθμοι, 56, 57
 - διάταξη, 64
- πολλαπλάσιο, 212
- πολλαπλότητα, 235
- πολυωνυμικές ισοδυναμίες, 106
- πολυώνυμο, 201
 - ανάγωγο, 226, 248
 - βαθμός, 202
 - βαθμός γινομένου, 202, 204
 - διακρίνουσα, 237
 - ελάχιστο, 248
 - εναδικό, 202
 - κυκλοτομικό, 227
 - κύριος συντελεστής, 202, 205
 - μεταβλητής x , 201
 - μη σταθερό, 242
 - μηδενικό, 201
 - παράγωγος, βλ. παράγωγος 233, 235
 - πρωτοβάθμιο, 242
 - ρίζες, βλ. ρίζα, -ες 230, 231
 - σταθερό, 234
 - σταθερός όρος, 202
 - συνδεδεμένο, 213
 - τιμή, 201
- πολύγωνο κανονικό, 255
- προβολές, 26
- προσεταιριστικ-ός, -η, 113
- προσθήκη, 249
- πρόταση, 17, 18
- πρώτος ακέραιος, 91
- πρώτος, -οι, 125
 - αριθμός, 120
 - σχετικά, 120, 139, 167
- πέρας, 41
- ρίζα, -ες, 233, 235
 - ακέραιες, 238
 - απλές, 237
 - πολλαπλή, 236
 - πολλαπλότητα, 231, 236-238
 - πολυωνύμου, 230
 - ρητές, 238
- σειρά τυπική, 233
- στοιχείο, -α, 17
 - αλγεβρικά, 242
 - αλγεβρικό, 243, 247
 - αντιστρέψιμο, 124, 213
 - αντιστρέψιμο, 212
 - αντίθετο, 48
 - αντίστροφο, 46
 - ανάγωγα, 224
 - ανάγωγο, 213, 216, 224
 - γεννήτορες, 133
 - ειδικά, 40
 - ισοδύναμο, 144
 - κλάση, 32
 - μεγαλύτερο ή μονάδα, 40
 - μικρότερο ή μηδέν, 40
 - μοναδιαίο, 212
 - ξένα μεταξύ τους, 216
 - ομαλό, 46, 117, 122, 130
 - ουδέτερο, 45
 - συγκρίσιμα, 35
 - συνδεδεμένα, 212
 - σχετικά ελάχιστο, 40
 - σχετικά μέγιστο, 40
 - τάξη, 136
 - υπερβατικό, 243
- συμπλήρωμα υποσυνόλου, 22
- συνδυασμοί, 79
- συνάρτηση
 - αριθμητική, 103
 - μονομελής, 42
 - πολλαπλασιαστική, 103
 - πολυωνυμική, 201
 - χαρακτηριστική, 66
- συνάρτηση, -εις, 17, 25
 - αμφιμονοσήμαντη, 25
 - αντίστροφη, 27
 - ανάλυση, 34
 - αρχέτυπο, 25
 - γράφημα, 26

- επέκταση, 26
- περιορισμός, 26
- προβολές, 26
- σύνθεση, 26
- ταυτοτική, 26
- τιμή, 25
- ίσεις, 25
- σχέσεις, 17, 30
 - αντισυμμετρική, 31, 35
 - αυτοπαθητική, 31, 35
 - διαιρετότητας, 36
 - διμελής, 30
 - διάταξης, 35, 55, 64
 - ολική, 35
 - ιδιότητες, 31
 - ισοδυναμίας, 31, 57, 119, 144, 213
 - κλάσεις, 32
 - συμβιβαστή, 49
 - μερικής διάταξης, 35
 - μεταβατική, 31, 35
 - περιέχεται, 36
 - συμμετρική, 31
- σύνολο, -α, 17, 19, 23, 27, 29, 30, 32
 - αριθμήσιμο, 57
 - δεικτών, 25
 - διαμέριση, 32
 - διατεταγμένο, 35, 37, 41
 - διαφορά, 21
 - δυναμοσύνολο, 20
 - ισοδύναμα, 57
 - καρτεσιανό γινόμενο, 21
 - κενό, 19
 - ξένα μεταξύ τους, 20
 - οικογένειες, 25
 - ολικά διατεταγμένο, 35
 - πεπερασμένο, 41, 58
 - πηλίκιο, 32, 33
 - πλήθος στοιχείων, 56
 - συμμετρική διαφορά, 23
 - τιμών, 25
 - τομή, 20
 - άπειρο, 58
 - ένωση, 20
- σώμα, -τα, 68, 116, 120, 121, 125, 236, 237
- Galois, 180
 - αντιμεταθετικά, 118
 - αντιμεταθετικό, 68, 235
 - ελάχιστο, 184
 - επεκτάσεις, 242
 - επέκταση, βλ. επέκταση 242
 - κλασμάτων, 182
 - μοναδικότητα, 184
 - πρώτα, 179
 - ρητών, 179
 - ριζών πολυωνύμων, 256
- τελεστές, 42
- τετραγωνικά ελεύθερος, 104
- τετραγωνικό υπόλοιπο, 107
- τετραγωνισμός κύκλου, 244, 250, 254
- τριχοτόμηση γωνίας, 250, 254
- υποδακτύλιος, 129, 199, 223
- υποδομή, 129
- υποομάδα, 129, 131
 - αναλλοίωτη, 161
 - γεννήτορες, 133
 - δείκτης, 132
 - εναλλάσσουσα, 271
 - ευθύ γινόμενο, 169
 - ιδιότητες, 131
 - ισόμορφη, 168
 - κανονική, 143-145, 156, 168, 169, 188
 - κέντρο, 131
 - μεταθετών, 162
 - παραγόμενη, 133
- υποσύνολο, -α, 19
 - αλυσίδα, 35
 - γνήσιο, 19
 - κλειστό, 42
 - συμπλήρωμα, 22
- υπόλοιπο, 91
- υπόσωμα, -τα, 129
 - ισόμορφο, 179
 - πρώτα, 178
- χαρακτηριστική, 178, 234-237
- χώρος διανυσματικός, 69, 242
 - διάσταση, 243

