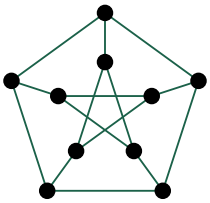
Διακριτά Μαθηματικά

Μ. Μυτιληναίος Π. Κατερίνης Γ. Αμανατίδης

Σημειώσεις για το μάθημα «Διακριτά Μαθηματικά»
Οικονομικό Πανεπιστήμιο Αθηνών



Αναθεωρημένη έκδοση 2026 — ΠΡΟΣΧΕΔΙΟ

Περιεχόμενα

Εισαγωγή **iii**
Τι είναι η μαθηματική απόδειξη; . . . iii
Παραδείγματα απλών αποδείξεων . . . iv

I Θεμελιώδεις έννοιες **1**

1 Σύνολα, σχέσεις και συναρτήσεις **2**
1.1 Σύνολα . . . 2
1.1.1 Στοιχεία, ισότητα και υποσύνολα . . . 2
1.1.2 Πράξεις μεταξύ συνόλων . . . 4
1.1.3 Δυναμοσύνολο και πληθικότητα . . . 8
1.2 Σχέσεις . . . 11
1.2.1 Διατεταγμένα ζεύγη και σχέσεις . . . 11
1.2.2 Ιδιότητες σχέσεων . . . 14
1.2.3 Σχέσεις ισοδυναμίας και διαμερίσεις . . . 15
1.2.4 Σχέσεις διάταξης . . . 17
1.3 Συναρτήσεις . . . 20
1.3.1 Ορισμός, εικόνα και αντίστροφη εικόνα . . . 20
1.3.2 Ενριπτικές, επιρριπτικές και αμφιμονοσήμαντες συναρτήσεις . . . 22
1.3.3 Σύνθεση συναρτήσεων . . . 23
1.3.4 Μερικές ειδικές συναρτήσεις . . . 24

2 Φυσικοί αριθμοί, επαγωγή και ισοδύναμα σύνολα **27**
2.1 Φυσικοί Αριθμοί. Αρχή της Επαγωγής . . . 27
2.1.1 Η αρχή της καλής διάταξης και η αρχή της επαγωγής . . . 27
2.1.2 Επαγωγικές αποδείξεις . . . 28
2.1.3 Ισχυρή επαγωγή . . . 29
2.2 Ισοδυναμία συνόλων. Αριθμήσιμα και υπεραριθμήσιμα σύνολα . . . 33
2.2.1 Ισοδύναμα σύνολα . . . 33
2.2.2 Πεπερασμένα και αριθμήσιμα σύνολα . . . 34
2.2.3 Υπεραριθμήσιμα σύνολα . . . 37

3 Λογική **40**
3.1 Γενικά . . . 40
3.2 Προτασιακός Λογισμός . . . 41
3.2.1 Η γλώσσα του προτασιακού λογισμού . . . 41
3.2.2 Αποτιμήσεις και πίνακες αλήθειας . . . 43
3.2.3 Ταυτολογίες, ταυτολογική συνεπαγωγή και ισοδυναμία . . . 44
3.2.4 Συναρτήσεις Boole και πλήρη σύνολα συνδέσμων . . . 48
3.3 Πράξεις μεταξύ Συνόλων και Λογικοί σύνδεσμοι . . . 53
3.4 Κατηγορηματική Λογική. Ποσοδείκτες . . . 54
3.4.1 Κατηγορήματα και ποσοδείκτες . . . 54
3.4.2 Πολλαπλοί ποσοδείκτες . . . 56
3.4.3 Άρνηση ποσοδοτημένων προτάσεων . . . 57

3.5 Τι είναι απόδειξη 60
3.5.1 Επιχειρήματα και αποδείξεις 60
3.5.2 Ευθεία απόδειξη και αντιπαράδειγμα 60
3.5.3 Αντιθετοαντιστροφή και απαγωγή σε άτοπο 61
3.6 Δυο θεμελιώδεις τεχνικές απόδειξης 64
3.6.1 Η αρχή του περιστερώνα 64
3.6.2 Η γενικευμένη αρχή του περιστερώνα 65
3.6.3 Η αρχή της διαγωνοποίησης 66

A Απαντήσεις και υποδείξεις **69**

Βιβλιογραφία **80**

Εισαγωγή

Προσοχή! Οι παρούσες σημειώσεις είναι ένα *πρώτο προσχέδιο* των Κεφαλαίων 1-3 της αναθεωρημένης έκδοσης των πανεπιστημιακών σημειώσεων των Μ. Μυτιληναίου και Π. Κατερίνη. Είναι πιθανόν να περιέχουν λάθη σε αυτήν την πρώτη μορφή. Σε γενικές γραμμές, το μπλε κείμενο είναι οι προσθήκες στις αρχικές σημειώσεις.

Μια διαδικασία λέγεται *διακριτή* αν μπορεί να πραγματοποιηθεί βήμα-προς-βήμα. Παραδείγματος χάρη, το να ακολουθήσουμε μια συνταγή, το να πολλαπλασιάσουμε δύο τριψήφιους αριθμούς, και το να λύσουμε μια δευτεροβάθμια εξίσωση είναι διακριτές διαδικασίες.

Διακριτά μαθηματικά είναι τα μαθηματικά που χρησιμοποιούμε για να αναλύσουμε διακριτές διαδικασίες. Η λέξη *διακριτός* σημαίνει «ξεχωριστός, διακεκριμένος»: τα διακριτά μαθηματικά μελετούν αντικείμενα που ξεχωρίζουν το ένα από το άλλο, όπως οι φυσικοί αριθμοί $0, 1, 2, 3, \ldots$ (το πλήθος των παιδιών μιας οικογένειας μπορεί να είναι 2 ή 3, αλλά όχι 2,41).

Για να αναλύσουμε «συνεχείς» διαδικασίες όπως την κίνηση μιας μπάλας που ρίξαμε ή την κίνηση ενός ηλεκτρονίου σ' ένα σύρμα, χρησιμοποιούμε «συνεχή μαθηματικά» (όπως τον Απειροστικό Λογισμό) αντί διακριτά μαθηματικά. Τα σύνολα που μελετά ο Απειροστικός Λογισμός, όπως το $\mathbb{R}$ ή το διάστημα $[0, \infty)$, είναι *συνεχή*: δεν έχουν «κενά». (Δεν αρκεί να υπάρχουν πάντα άπειρα στοιχεία ανάμεσα σε δύο οποιαδήποτε στοιχεία τους· αυτό ισχύει και για το $\mathbb{Q}$, στο οποίο όμως «λείπουν» σημεία, όπως το $\sqrt{2}$.) Επειδή όμως οι υπολογιστές πραγματοποιούν διαδικασίες βήμα-προς-βήμα, τα διακριτά μαθηματικά έχουν γίνει ένα σημαντικό εργαλείο στην επιστήμη των υπολογιστών.

Όπως γνωρίζουμε, μια λίστα από βήμα-προς-βήμα οδηγίες για την πραγματοποίηση μιας διαδικασίας λέγεται *αλγόριθμος*. Άρα τα διακριτά μαθηματικά χρησιμοποιούνται για την ανάλυση των αλγορίθμων.

Σε αυτές τις σημειώσεις θα μελετήσουμε τις βασικές δομές των διακριτών μαθηματικών: τα σύνολα, τις σχέσεις και τις συναρτήσεις και τη λογική (Μέρος I), τις τεχνικές απαρίθμησης, δηλαδή πώς *μετράμε* πόσα αντικείμενα ενός είδους υπάρχουν (Μέρος II), τα γραφήματα (Μέρος III) και τις ακολουθίες που ορίζονται αναδρομικά (Μέρος IV). Είναι τα βασικά εργαλεία για τη μοντελοποίηση προβλημάτων με «μετρήσιμα», διακριτά συστατικά.

Πάνω απ' όλα όμως, το μάθημα είναι μια εισαγωγή στη *μαθηματική απόδειξη*. Στο σχολείο τα μαθηματικά ταυτίζονται συχνά με τους υπολογισμούς· εδώ το ζητούμενο είναι πολύ συχνά να εξηγήσουμε *γιατί* κάτι ισχύει, και μάλιστα σε όλες τις περιπτώσεις, και όχι μόνο να υπολογίσουμε κάτι σε μία. Σχεδόν κάθε ενότητα περιέχει αποδείξεις, και πολλές ασκήσεις ζητούν από εσάς να γράψετε μία. Η ικανότητα να διαβάζουμε, να βρίσκουμε και να γράφουμε σωστές και σαφείς αποδείξεις είναι ίσως το σημαντικότερο εφόδιο που προσφέρει το μάθημα, και θα σας χρειαστεί σε κάθε μάθημα που χρησιμοποιεί μαθηματικά. Οι τεχνικές απόδειξης μελετώνται συστηματικά στο Κεφάλαιο 3 (Ενότητες 3.5 και 3.6) και η επαγωγή στο Κεφάλαιο 2, αλλά τις χρησιμοποιούμε από την πρώτη σελίδα. Γι' αυτό ξεκινάμε με μια σύντομη, άτυπη γνωριμία.

Τι είναι η μαθηματική απόδειξη;

Στο σχολείο μάθαμε ότι το άθροισμα των γωνιών κάθε τριγώνου είναι $180°$. Μπορούμε να σχεδιάσουμε δέκα, εκατό ή χίλια τρίγωνα και να μετρήσουμε τις γωνίες τους, αλλά έτσι δεν θα μάθουμε ποτέ με βεβαιότητα ότι το ίδιο ισχύει για *κάθε* τρίγωνο: τα τρίγωνα είναι άπειρα, και κάθε μέτρηση έχει σφάλμα. Τη βεβαιότητα αυτή τη δίνει μόνο μια απόδειξη.

Μαθηματική απόδειξη. Μια *μαθηματική απόδειξη* μιας πρότασης είναι ένα επιχείρημα που δείχνει, χωρίς περιθώριο αμφιβολίας, ότι η πρόταση είναι αληθής. Ξεκινά από αξιώματα, ορισμούς και προτάσεις που έχουν ήδη αποδειχθεί, και φτάνει στην πρόταση με διαδοχικά βήματα, καθένα από τα οποία προκύπτει λογικά από τα προηγούμενα.

Μερικές παρατηρήσεις για αυτόν τον (άτυπο) ορισμό.

- Οι περισσότερες προτάσεις που αποδεικνύουμε έχουν τη μορφή «αν ισχύει η *υπόθεση* p, τότε ισχύει το *συμπέρασμα* q», συχνά μαζί με ένα «για κάθε»: «για κάθε ακέραιο n, αν ο n είναι περιττός, τότε ο n^2 είναι περιττός». Μια πρόταση που έχει αποδειχθεί λέγεται, ανάλογα με τη σημασία της, *θεώρημα*, *πρόταση*, *λήμμα* (βοηθητικό αποτέλεσμα) ή *πόρισμα* (άμεση συνέπεια ενός θεωρήματος).
- Μια απόδειξη πρέπει να καλύπτει *όλες* τις περιπτώσεις. Όσα παραδείγματα κι αν ελέγξουμε, δεν αποδεικνύουν μια πρόταση που αφορά άπειρες περιπτώσεις (θα δούμε ένα χαρακτηριστικό παράδειγμα στην Πρόταση 4 παρακάτω).
- Μια απόδειξη γράφεται για έναν αναγνώστη, που πρέπει να μπορεί να ελέγξει κάθε βήμα της. Γράφουμε σε πλήρεις προτάσεις, εξηγούμε τι υποθέτουμε και τι θέλουμε να δείξουμε, και δεν παραλείπουμε βήματα που δεν είναι προφανή για κάποιον που ξέρει τους ορισμούς αλλά όχι τη λύση.
- Το πρώτο βήμα είναι σχεδόν πάντα να γράψουμε με ακρίβεια τους *ορισμούς* των εννοιών που εμφανίζονται. Για παράδειγμα, ένας ακέραιος n είναι *άρτιος* αν $n = 2k$ για κάποιον ακέραιο k, και *περιττός* αν $n = 2k + 1$ για κάποιον ακέραιο k· ένας φυσικός αριθμός $p > 1$ είναι *πρώτος* αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο p.

Το τι ακριβώς σημαίνει «προκύπτει λογικά» το εξετάζει η μαθηματική λογική, της οποίας τα βασικά θα δούμε στο Κεφάλαιο 3.

Λίγη ιστορία. Η ιδέα της απόδειξης γεννήθηκε στην αρχαία Ελλάδα. Κατά την παράδοση, ο Θαλής ο Μιλήσιος (6ος αιώνας π.Χ.) ήταν ο πρώτος που απέδειξε γεωμετρικές προτάσεις, όπως ότι κάθε διάμετρος χωρίζει τον κύκλο σε δύο ίσα μέρη. Τα *Στοιχεία* του Ευκλείδη (περίπου 300 π.Χ.) οργάνωσαν τη γεωμετρία και τη θεωρία αριθμών της εποχής σε 13 βιβλία: ξεκινούν από ορισμούς, *αιτήματα* (τα σημερινά αξιώματα) και «κοινές έννοιες», και αποδεικνύουν από αυτά, τη μία μετά την άλλη, 465 προτάσεις. Αυτή η *αξιωματική μέθοδος* παρέμεινε το πρότυπο της μαθηματικής αυστηρότητας για περισσότερα από δύο χιλιάδες χρόνια· μία από τις αποδείξεις των *Στοιχείων*, ότι υπάρχουν άπειροι πρώτοι αριθμοί, τη βλέπουμε παρακάτω (Πρόταση 3). Τον 19ο αιώνα ο Απειροστικός Λογισμός, που ως τότε στηριζόταν σε μεγάλο βαθμό στη διαίσθηση, θεμελιώθηκε με την ίδια αυστηρότητα, και στις αρχές του 20ού αιώνα η ίδια η έννοια της απόδειξης έγινε αντικείμενο μαθηματικής μελέτης: η μαθηματική λογική (Frege, Hilbert και άλλοι) περιγράφει μια απόδειξη ως μια πεπερασμένη ακολουθία προτάσεων που ακολουθεί αυστηρούς κανόνες. Το 1931 ο Gödel έδειξε ότι σε κάθε τέτοιο σύστημα αξιωμάτων χωρίς αντιφάσεις, του οποίου τα αξιώματα μπορούν να απαριθμηθούν από έναν αλγόριθμο και το οποίο περιέχει την αριθμητική των φυσικών αριθμών, υπάρχουν προτάσεις που ούτε αποδεικνύονται ούτε διαψεύδονται μέσα σε αυτό. Σήμερα στις αποδείξεις συμμετέχουν και οι υπολογιστές: το Θεώρημα των Τεσσάρων Χρωμάτων (Κεφάλαιο **??**) αποδείχθηκε το 1976 με τη βοήθεια υπολογιστή, και το 2005 η απόδειξή του ελέγχθηκε πλήρως από ένα πρόγραμμα επαλήθευσης αποδείξεων.

Παραδείγματα απλών αποδείξεων

Οι τέσσερις προτάσεις αυτής της ενότητας χρειάζονται μόνο μαθηματικά του Γυμνασίου: ακέραιους αριθμούς, άρτιους και περιττούς, πρώτους αριθμούς. Καθεμία δείχνει μια διαφορετική τεχνική

απόδειξης· όλες θα τις ξανασυναντήσουμε, με περισσότερη θεωρία, στο Κεφάλαιο 3.

Πρόταση 1. *Το άθροισμα δύο περιττών ακεραίων είναι άρτιος αριθμός.*

Απόδειξη. Έστω m και n δύο περιττοί ακέραιοι. Από τον ορισμό του περιττού, υπάρχουν ακέραιοι k και ℓ τέτοιοι ώστε $m = 2k + 1$ και $n = 2\ell + 1$. Τότε

$$m + n = (2k + 1) + (2\ell + 1) = 2k + 2\ell + 2 = 2(k + \ell + 1).$$

Αφού ο $k + \ell + 1$ είναι ακέραιος, ο $m + n$ είναι άρτιος. □

Αυτή είναι μια *ευθεία απόδειξη*: ξεκινάμε από την υπόθεση και με διαδοχικά βήματα φτάνουμε στο συμπέρασμα. Τρία σημεία αξίζουν προσοχή. Πρώτα, «μεταφράσαμε» την υπόθεση με τον ορισμό του περιττού, ώστε να μπορέσουμε να κάνουμε πράξεις, και στο τέλος μεταφράσαμε πίσω το αποτέλεσμα με τον ορισμό του άρτιου. Δεύτερο, χρησιμοποιήσαμε *διαφορετικά* γράμματα k και ℓ: αν γράφαμε $m = 2k + 1$ και $n = 2k + 1$, θα είχαμε υποθέσει σιωπηρά ότι $m = n$, και θα είχαμε αποδείξει μόνο ότι ο $2m$ είναι άρτιος. Τρίτο, οι έλεγχοι $3 + 5 = 8$ ή $7 + 11 = 18$ πείθουν, αλλά δεν αποδεικνύουν· η απόδειξη καλύπτει ταυτόχρονα όλα τα (άπειρα) ζευγάρια, επειδή οι m και n ήταν *οποιοιδήποτε* περιττοί ακέραιοι.

Πρόταση 2. *Αν a και b είναι ακέραιοι με $a + b \geq 15$, τότε $a \geq 8$ ή $b \geq 8$.*

Απόδειξη. Θα αποδείξουμε την *αντιθετοαντίστροφη* πρόταση: αν δεν ισχύει ότι «$a \geq 8$ ή $b \geq 8$», τότε δεν ισχύει ότι $a + b \geq 15$. Αν δεν ισχύει ούτε $a \geq 8$ ούτε $b \geq 8$, τότε, αφού οι a και b είναι ακέραιοι, $a \leq 7$ και $b \leq 7$. Προσθέτοντας τις δύο ανισότητες παίρνουμε $a + b \leq 14$, άρα δεν ισχύει $a + b \geq 15$. □

Μια πρόταση «αν p, τότε q» και η αντιθετοαντίστροφή της «αν όχι q, τότε όχι p» είναι είτε και οι δύο αληθείς είτε και οι δύο ψευδείς (Κεφάλαιο 3), οπότε αρκεί να αποδείξουμε όποια είναι ευκολότερη. Εδώ μια ευθεία απόδειξη θα δυσκολευόταν, αφού το συμπέρασμα «$a \geq 8$ ή $b \geq 8$» δεν λέει *ποιος* από τους δύο αριθμούς είναι μεγάλος. Η άρνησή του όμως, «$a \leq 7$ *και* $b \leq 7$», μας δίνει δύο ανισότητες που μπορούμε να χρησιμοποιήσουμε αμέσως. Παρατηρήστε ότι χρησιμοποιήσαμε την υπόθεση ότι οι a, b είναι *ακέραιοι*: για πραγματικούς αριθμούς η πρόταση είναι ψευδής ($a = b = 7{,}5$). Προσοχή επίσης στην *αντίστροφη* πρόταση, «αν $a \geq 8$ ή $b \geq 8$, τότε $a + b \geq 15$»: είναι ψευδής ($a = 8, b = 0$), αν και η αρχική είναι αληθής. Η ιδέα της πρότασης («αν το άθροισμα είναι μεγάλο, κάποιος όρος είναι μεγάλος») είναι η γενικευμένη αρχή του περιστερώνα, που θα δούμε στην Ενότητα 3.6.

Πρόταση 3 (Ευκλείδης). *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Ας υποθέσουμε, για να καταλήξουμε σε άτοπο, ότι οι πρώτοι αριθμοί είναι πεπερασμένοι στο πλήθος, οι $p_1, p_2, \dots, p_k$. Θεωρούμε τον αριθμό

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

Αφού $N > 1$, ο N έχει έναν πρώτο διαιρέτη p (κάθε ακέραιος μεγαλύτερος από το 1 έχει πρώτο διαιρέτη, βλέπε και Παράδειγμα 2.10). Ο p είναι ένας από τους $p_1, \dots, p_k$, άρα διαιρεί το γινόμενο $p_1 p_2 \cdots p_k$. Αφού διαιρεί και τον N, διαιρεί και τη διαφορά τους $N - p_1 p_2 \cdots p_k = 1$. Αυτό είναι άτοπο, αφού $p > 1$. Άρα η υπόθεσή μας ήταν λανθασμένη, και οι πρώτοι αριθμοί είναι άπειροι. □

Αυτή είναι μια απόδειξη με *απαγωγή σε άτοπο*: υποθέτουμε ότι η πρόταση που θέλουμε να δείξουμε είναι ψευδής, και από αυτή την υπόθεση καταλήγουμε σε κάτι που είναι σίγουρα ψευδές (ένα «άτοπο», εδώ ότι ένας αριθμός μεγαλύτερος από το 1 διαιρεί το 1). Αφού κάθε βήμα ήταν σωστό, το

λάθος βρίσκεται στην υπόθεση. Η τεχνική είναι ιδιαίτερα χρήσιμη όταν η πρόταση λέει ότι κάτι *δεν* υπάρχει ή ότι κάτι είναι άπειρο, γιατί η άρνησή της μας δίνει κάτι συγκεκριμένο να χειριστούμε (εδώ μια πεπερασμένη λίστα όλων των πρώτων). Ο ίδιος ο Ευκλείδης (*Στοιχεία*, Βιβλίο IX, Πρόταση 20) το διατύπωσε ως εξής: οι πρώτοι αριθμοί είναι περισσότεροι από κάθε δοσμένο πλήθος πρώτων. Μια συχνή παρανόηση είναι ότι ο N είναι ο ίδιος πρώτος· δεν είναι απαραίτητα, αφού $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$. Η απόδειξη χρειάζεται μόνο ότι ο N έχει *κάποιο* πρώτο διαιρέτη, γεγονός που θα αποδείξουμε με (ισχυρή) επαγωγή στο Παράδειγμα 2.10.

Πρόταση 4. *Ο ισχυρισμός «για κάθε θετικό ακέραιο n, ο αριθμός $n^2 - n + 11$ είναι πρώτος» είναι ψευδής.*

Απόδειξη. Για $n = 11$ έχουμε $11^2 - 11 + 11 = 121 = 11 \cdot 11$, που δεν είναι πρώτος. Άρα ο $n = 11$ είναι ένα *αντιπαράδειγμα*. □

Για να δείξουμε ότι μια πρόταση της μορφής «για κάθε n, ...» είναι ψευδής, αρκεί *ένα* αντιπαράδειγμα. Κι όμως, ο ισχυρισμός μοιάζει αρχικά πολύ πειστικός: για $n = 1, 2, \dots, 10$ ο $n^2 - n + 11$ παίρνει τις τιμές

$$11,\ 13,\ 17,\ 23,\ 31,\ 41,\ 53,\ 67,\ 83,\ 101,$$

που είναι όλες πρώτοι αριθμοί. Δέκα επιβεβαιώσεις δεν αποδεικνύουν τίποτα (θυμηθείτε τη δεύτερη παρατήρηση για τον ορισμό της απόδειξης). Πώς θα βρίσκαμε το αντιπαράδειγμα χωρίς να δοκιμάζουμε έναν-έναν τους αριθμούς; Γράφοντας $n^2 - n + 11 = n(n-1) + 11$, βλέπουμε ότι για $n = 11$ και οι δύο προσθετέοι διαιρούνται με το 11. Το διάσημο πολυώνυμο $n^2 + n + 41$ του Euler δίνει πρώτους αριθμούς για $n = 0, 1, \dots, 39$, αλλά όχι για $n = 40$ (Ενότητα 3.5). Στην έρευνα, μια πρόταση που έχει ελεγχθεί σε τεράστιο πλήθος περιπτώσεων αλλά δεν έχει αποδειχθεί λέγεται *εικασία*· η εικασία του Goldbach, ότι κάθε άρτιος μεγαλύτερος από το 2 είναι άθροισμα δύο πρώτων, έχει ελεγχθεί με υπολογιστή για όλους τους άρτιους μέχρι το $4 \cdot 10^{18}$, αλλά παραμένει ανοιχτό πρόβλημα.

Όποιος θέλει να εξασκηθεί περισσότερο στη γραφή αποδείξεων, θα βρει στο βιβλίο του Velleman [Vel] μια συστηματική εισαγωγή, ενώ το κλασικό βιβλίο του Pólya [Pól] δίνει πρακτικές οδηγίες για το πώς βρίσκουμε τη λύση ενός προβλήματος, και την απόδειξή της.

Μέρος Ι

Θεμελιώδεις έννοιες

Κεφάλαιο 1

Σύνολα, σχέσεις και συναρτήσεις

1.1 Σύνολα

1.1.1 Στοιχεία, ισότητα και υποσύνολα

Η έννοια του συνόλου είναι μια απ' τις πιο σημαντικές έννοιες των μαθηματικών. Παραδείγματα συνόλων υπάρχουν παντού, π.χ., το σύνολο των βιβλίων της βιβλιοθήκης του Πανεπιστημίου, το σύνολο των ανθρώπων στη γη, το σύνολο των άστρων του σύμπαντος. Τα αντικείμενα ενός συνόλου τα λέμε *στοιχεία* του συνόλου. Για να συμβολίζουμε ότι ένα στοιχείο a ανήκει σε ένα σύνολο A γράφουμε $a \in A$ και λέμε ότι το a ανήκει στο A ή ότι το a είναι στοιχείο του A. Για παράδειγμα, το 3 ανήκει στο σύνολο των φυσικών αριθμών, και το γράφουμε $3 \in \mathbb{N}$, ενώ το ότι το π είναι πραγματικός αριθμός το γράφουμε $\pi \in \mathbb{R}$.

Αν το a δεν ανήκει στο σύνολο A γράφουμε $a \notin A$. Συνήθως χρησιμοποιούμε μικρά γράμματα για στοιχεία συνόλων και κεφαλαία για σύνολα. Για να συμβολίσουμε το σύνολο που αποτελείται από τα στοιχεία $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ θα γράφουμε $\{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$. Θα λέμε ότι δύο σύνολα A και B είναι *ίσα* και θα γράφουμε $A = B$ όταν έχουν τα ίδια ακριβώς στοιχεία. Αυτό σημαίνει ότι ένα σύνολο καθορίζεται μονοσήμαντα από τα στοιχεία του. Για παράδειγμα τα σύνολα $\{\alpha, \beta, \gamma\}$ και $\{\beta, \gamma, \alpha\}$ είναι ίσα και γράφουμε $\{\alpha, \beta, \gamma\} = \{\beta, \gamma, \alpha\}$. Όταν δύο σύνολα A και B δεν είναι ίσα, γράφουμε $A \neq B$.

Με άλλα λόγια, ένα σύνολο είναι μια *μη διατεταγμένη* συλλογή αντικειμένων: δεν μας ενδιαφέρει ούτε η σειρά με την οποία γράφουμε τα στοιχεία του ούτε το αν κάποιο στοιχείο γράφεται περισσότερες από μία φορές. Έτσι, για παράδειγμα,

$$\{1, 2, 3\} = \{3, 1, 2\} = \{1, 1, 2, 3, 3, 3\}.$$

Τα στοιχεία ενός συνόλου μπορεί να είναι οποιαδήποτε αντικείμενα: αριθμοί, γράμματα, άνθρωποι, αλλά και άλλα σύνολα.

Παράδειγμα 1.1 (Ένα «περίεργο» σύνολο). Το σύνολο $A = \{1,\ b,\ \{x, y, z\},\ \emptyset\}$ έχει *τέσσερα* στοιχεία: τον αριθμό 1, το γράμμα b, το σύνολο $\{x, y, z\}$ και το κενό σύνολο $\emptyset$ (το σύνολο που δεν έχει κανένα στοιχείο· βλ. τον πίνακα που ακολουθεί). Είναι $x \in A$; Όχι! Κανένα από τα τέσσερα στοιχεία του A δεν είναι το x· το x είναι στοιχείο *ενός στοιχείου* του A, του $\{x, y, z\}$. Ισχύει όμως $\{x, y, z\} \in A$ και $\emptyset \in A$.

Μερικά σύνολα χρησιμοποιούνται τόσο συχνά ώστε έχουν δικό τους σύμβολο:

Σύμβολο	Περιγραφή
$\emptyset$	το *κενό σύνολο*, που δεν έχει κανένα στοιχείο
$\mathbb{N}$	οι *φυσικοί αριθμοί* $\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	οι *ακέραιοι* $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}_+$	οι *θετικοί ακέραιοι* $\{1, 2, 3, \dots\}$
$\mathbb{Q}$	οι *ρητοί* αριθμοί
$\mathbb{R}$	οι *πραγματικοί* αριθμοί

Προσοχή: κάποιοι συγγραφείς δεν συμπεριλαμβάνουν το 0 στο $\mathbb{N}$. Σε αυτές τις σημειώσεις το 0 είναι φυσικός αριθμός.

Ορισμός 1.2 (Υποσύνολο). Αν A και B είναι σύνολα και αν κάθε στοιχείο του A είναι και στοιχείο του B, λέμε ότι το A είναι *υποσύνολο* του B, ή ότι το B περιέχει το A, και γράφουμε $A \subseteq B$ ή $B \supseteq A$. Αν επιπλέον $A \neq B$, το A λέγεται *γνήσιο υποσύνολο* του B και γράφουμε $A \subset B$.

Η διαφορά ανάμεσα στα $\subseteq$ και $\subset$ είναι ανάλογη με τη διαφορά ανάμεσα στα $\leq$ και $<$ για τους αριθμούς. Το κενό σύνολο είναι υποσύνολο *κάθε* συνόλου: $\emptyset \subseteq A$ για κάθε A. Πράγματι, για να μην ίσχυε $\emptyset \subseteq A$ θα έπρεπε να υπάρχει στοιχείο του $\emptyset$ που δεν ανήκει στο A· όμως το $\emptyset$ δεν έχει κανένα στοιχείο. (Λέμε ότι ο ισχυρισμός «κάθε στοιχείο του $\emptyset$ ανήκει στο A» είναι *κενά αληθής*.)

Εύκολα μπορούμε να δείξουμε ότι για κάθε σύνολο A, $A \subseteq A$, δηλαδή η σχέση του περιέχεσθαι είναι αυτοπαθής (ή ανακλαστική). Αν τα A και B είναι σύνολα και $A \subseteq B$ και $B \subseteq A$ τότε τα σύνολα A, B έχουν τα ίδια στοιχεία και άρα $A = B$. Δηλαδή η σχέση του περιέχεσθαι ($\subseteq$) είναι αντισυμμετρική. Επίσης αν $A \subseteq B$ και $B \subseteq C$ τότε $A \subseteq C$ (μεταβατική ιδιότητα).

Επειδή η αντισυμμετρική ιδιότητα θα χρησιμοποιείται συνεχώς, ας δούμε την απόδειξή της αναλυτικά.

Πρόταση 1.3. *Αν $A \subseteq B$ και $B \subseteq A$, τότε $A = B$.*

Απόδειξη. Έστω τυχόν $a \in A$. Αφού $A \subseteq B$, έχουμε $a \in B$. Άρα κάθε στοιχείο του A είναι στοιχείο του B. Αντίστροφα, έστω τυχόν $b \in B$. Αφού $B \subseteq A$, έχουμε $b \in A$. Άρα κάθε στοιχείο του B είναι στοιχείο του A. Επομένως τα A και B έχουν ακριβώς τα ίδια στοιχεία, δηλαδή $A = B$. □

Παρατήρηση 1.4 (Η μέθοδος του διπλού εγκλεισμού). Η Πρόταση 1.3 δίνει τον βασικό τρόπο για να αποδείξουμε ότι δύο σύνολα A και B είναι ίσα: δείχνουμε *χωριστά* ότι $A \subseteq B$ (κάθε στοιχείο του A ανήκει στο B) και ότι $B \subseteq A$ (κάθε στοιχείο του B ανήκει στο A). Θα χρησιμοποιούμε αυτή τη μέθοδο συνεχώς.

Παρατηρούμε ότι η σχέση του ανήκειν ($\in$) και η σχέση του περιέχεσθαι ($\subseteq$) είναι διαφορετικές. Για παράδειγμα η $\subseteq$ είναι πάντοτε αυτοπαθής ενώ η $\in$ όχι, δηλαδή $A \subseteq A$ ενώ δεν ξέρουμε αν $A \in A$. Επίσης η $\subseteq$ είναι μεταβατική ενώ η $\in$ όχι.

Παράδειγμα 1.5 (Αληθές, ψευδές ή χωρίς νόημα;). Έστω $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6\}$ και $C = \{1, 2, 3\}$. Ποιες από τις παρακάτω προτάσεις είναι αληθείς, ποιες ψευδείς και ποιες δεν έχουν νόημα;

$$\text{(α) } A \subset B \qquad \text{(β) } B \subset A \qquad \text{(γ) } B \in C \qquad \text{(δ) } \emptyset \in A$$
$$\text{(ε) } \emptyset \subset A \qquad \text{(στ) } 3 \in C \qquad \text{(ζ) } 3 \subset C \qquad \text{(η) } \{3\} \subset C$$

Λύση. (α) Ψευδές, αφού $1 \in A$ αλλά $1 \notin B$. (β) Αληθές. (γ) Ψευδές: τα στοιχεία του C είναι αριθμοί, όχι σύνολα. (δ) Ψευδές: τα στοιχεία του A είναι έξι αριθμοί και το $\emptyset$ δεν είναι κανένας από αυτούς. (ε) Αληθές: το $\emptyset$ είναι υποσύνολο κάθε συνόλου, και $\emptyset \neq A$. (στ) Αληθές. (ζ) Χωρίς νόημα: το 3 δεν είναι σύνολο, οπότε δεν έχει νόημα να ρωτάμε αν είναι υποσύνολο του C. (η) Αληθές: $\{3\} \subseteq C$ και $\{3\} \neq C$. ◊

Για να συμβολίσουμε τα σύνολα αντικειμένων που έχουν κάποια ιδιότητα θα χρησιμοποιούμε τον συμβολισμό $\{x : \varphi(x)\}$. Αυτό το σύνολο έχει ως στοιχεία αυτά ακριβώς τα αντικείμενα που έχουν την ιδιότητα φ. Επομένως

$$a \in \{x : \varphi(x)\} \quad \text{αν και μόνο αν} \quad \varphi(a).$$

Έτσι γράφουμε $\{x : x \in \mathbb{N} \text{ και } x \leq 20\}$.

Ο συμβολισμός αυτός λέγεται *συμβολισμός δόμησης συνόλου*. Για παράδειγμα, το $\{x \in \mathbb{N} : x \text{ είναι άρτιος}\}$ διαβάζεται «το σύνολο όλων των x του $\mathbb{N}$ *τέτοιων ώστε* το x να είναι άρτιος». Η άνω-κάτω τελεία (σε άλλα βιβλία η κάθετη γραμμή $|$) χωρίζει τα στοιχεία από τη *συνθήκη* που πρέπει να ικανοποιούν.

Παράδειγμα 1.6 (Διαβάζοντας σύνολα). Περιγράψτε με λόγια τα παρακάτω σύνολα και απαριθμήστε μερικά στοιχεία τους:

$$\text{(α) } \{x : x+3 \in \mathbb{N}\} \qquad \text{(β) } \{x \in \mathbb{N} : x+3 \in \mathbb{N}\}$$

$$\text{(γ) } \{x : x \in \mathbb{N} \text{ ή } -x \in \mathbb{N}\} \qquad \text{(δ) } \{x : x \in \mathbb{N} \text{ και } -x \in \mathbb{N}\}$$

Λύση. (α) Είναι το σύνολο $\{-3, -2, -1, 0, 1, 2, \dots\}$ των αριθμών που, αν τους προσθέσουμε 3, δίνουν φυσικό. (β) Εδώ το x πρέπει *ήδη* να είναι φυσικός, άρα το σύνολο είναι το $\{0, 1, 2, 3, \dots\} = \mathbb{N}$. (γ) Όλοι οι ακέραιοι, δηλαδή το $\mathbb{Z}$. (δ) Μόνο το 0 είναι φυσικός με αντίθετο επίσης φυσικό, άρα το σύνολο είναι το $\{0\}$. ◊

Πρέπει όμως να προσέχουμε γιατί η συλλογή των x που έχουν την ιδιότητα φ δεν είναι πάντα σύνολο. Σίγουρα είναι σύνολο όταν πάρουμε από ένα σύνολο A αυτά τα στοιχεία που έχουν την ιδιότητα φ, κάτι που το συμβολίζουμε $\{x \in A : \varphi(x)\}$. Διαφορετικά, δηλαδή όταν πάρουμε τα αντικείμενα x που έχουν μια ιδιότητα χωρίς κανένα περιορισμό από πού προέρχονται, μπορεί να μην σχηματίσουμε σύνολο. Για παράδειγμα, έστω ότι στον ρόλο της $\varphi(x)$ έχουμε την πρόταση $x \notin x$. Αν δεν υπήρχε περιορισμός τότε το $R = \{x : x \notin x\}$ θα ήταν σύνολο. Το R αποτελείται από τα σύνολα που δεν ανήκουν στον εαυτό τους. Να είναι $R \in R$;

$$\text{Αν } R \in R \text{ τότε } R \notin R, \text{ και}$$
$$\text{αν } R \notin R \text{ τότε } R \in R.$$

Άρα έχουμε μια αντίφαση, επομένως το R δεν μπορεί να είναι σύνολο. Το παραπάνω παράδειγμα λέγεται *παράδοξο του Russell*. Γι' αυτό το λόγο γράφουμε, π.χ., $\{x \in \mathbb{R} : x < 7 \text{ και } |x| \geq 5\}$.

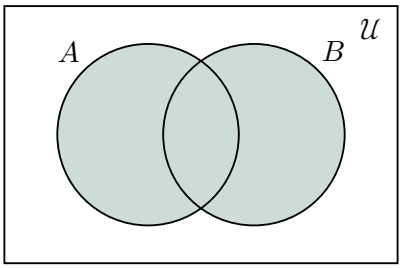
Παρατήρηση 1.7. Το παράδοξο διατυπώθηκε από τον B. Russell το 1901. Το πρόβλημα δημιουργείται μόνο όταν αφήνουμε το «σύμπαν αναφοράς» απεριόριστο. Αν περιορίσουμε την αναζήτηση σε ένα ήδη υπάρχον σύνολο A, τότε το $\{x \in A : x \notin x\}$ *είναι* καλά ορισμένο σύνολο (ένα υποσύνολο του A). Γι' αυτό, όταν χτίζουμε νέα σύνολα από μια ιδιότητα, τα παίρνουμε σχεδόν πάντα ως υποσύνολα ενός ήδη γνωστού συνόλου.

Το σύνολο $\{a\}$ που περιέχει ένα μόνο στοιχείο λέγεται *μονοσύνολο* και αυτό που περιέχει δύο μόνο στοιχεία, π.χ., το $\{\alpha, \beta\}$, λέγεται *ζεύγος*. Το κενό σύνολο $\emptyset$ είναι μοναδικό (αφού ένα σύνολο καθορίζεται από τα στοιχεία του). Παραδείγματος χάρη $\emptyset = \{x \in \mathbb{R} : x^2 + 1 = 0\}$, $\emptyset = \{x \in \mathbb{N} : x > 10 \text{ και } x < 5\}$.

1.1.2 Πράξεις μεταξύ συνόλων

Υπάρχει ένα είδος διαγράμματος που λέγεται *διάγραμμα του Venn* το οποίο μπορούμε να χρησιμοποιούμε για να απεικονίσουμε σύνολα που επιλέξαμε από ένα σύνολο αναφοράς $\mathcal{U}$ (το *σύμπαν*, βλ. παρακάτω). Πρώτα σχεδιάζουμε ένα ορθογώνιο που αντιπροσωπεύει το $\mathcal{U}$, και μετά μέσα σ' αυτό σχεδιάζουμε κύκλους ή άλλα σχήματα που αντιπροσωπεύουν σύνολα.

Ορισμός 1.8 (Ένωση). Έστω A, B σύνολα. Το σύνολο που έχει στοιχεία όλα τα στοιχεία του A και όλα τα στοιχεία του B λέγεται *ένωση* των A και B, και συμβολίζεται με $A \cup B$. Έχουμε λοιπόν, $A \cup B = \{a : a \in A \text{ ή } a \in B\}$ (βλέπε Σχήμα 1.1).



Σχήμα 1.1. Διάγραμμα του Venn: η ένωση $A \cup B$ (σκιασμένη).

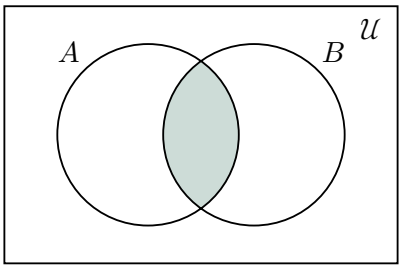
Είναι φανερό από τον ορισμό της ένωσης συνόλων ότι $a \in A \cup B \Leftrightarrow (a \in A$ ή $a \in B)$. Παραθέτουμε μερικές ιδιότητες της ένωσης που αποδεικνύονται εύκολα:

$$\begin{aligned} A \cup \emptyset &= A \\ A \cup B &= B \cup A && \text{(αντιμεταθετικότητα)} \\ A \cup (B \cup C) &= (A \cup B) \cup C && \text{(προσεταιριστικότητα)} \\ A \cup A &= A && \text{(ταυτοδυναμία)} \\ A \subseteq B &\Leftrightarrow A \cup B = B. \end{aligned}$$

Ορισμός 1.9 (Τομή). Αν A και B είναι σύνολα, η *τομή* των A και B είναι το σύνολο $A \cap B$ που ορίζεται από την ισότητα

$$A \cap B = \{a \,:\, a \in A \text{ και } a \in B\}$$

(βλέπε Σχήμα 1.2).



Σχήμα 1.2. Διάγραμμα του Venn: η τομή $A \cap B$ (σκιασμένη).

Οι βασικές ιδιότητες των τομών, όπως και οι αποδείξεις τους, είναι παρόμοιες με αυτές των ενώσεων:

$$\begin{aligned} A \cap \emptyset &= \emptyset \\ A \cap B &= B \cap A && \text{(αντιμεταθετικότητα)} \\ A \cap (B \cap C) &= (A \cap B) \cap C && \text{(προσεταιριστικότητα)} \\ A \cap A &= A && \text{(ταυτοδυναμία)} \\ A \subseteq B &\Leftrightarrow A \cap B = A. \end{aligned}$$

Δύο σύνολα A, B με τομή το κενό σύνολο, δηλαδή $A \cap B = \emptyset$, λέγονται *ξένα μεταξύ τους*.

Παράδειγμα 1.10. Αν $A = \{1, 2, 3\}$ και $B = \{2, 3, 4\}$, τότε $A \cup B = \{1, 2, 3, 4\}$ και $A \cap B = \{2, 3\}$. Τα σύνολα $\{1, 2\}$ και $\{3, 4\}$ είναι ξένα μεταξύ τους.

Οι ιδιότητες του $\emptyset$, η αντιμεταθετικότητα και η προσεταιριστικότητα θυμίζουν τις αντίστοιχες ιδιότητες της πρόσθεσης και του πολλαπλασιασμού αριθμών (το $\emptyset$ παίζει για την ένωση τον ρόλο

που παίζει το 0 για την πρόσθεση). Η ιδιότητα $A \cup A = A$ όμως δεν έχει ανάλογο στους αριθμούς: γενικά $x + x \neq x$. Οι δύο τελευταίες ιδιότητες συνδυάζονται στην επόμενη πρόταση.

Πρόταση 1.11 (Χαρακτηρισμός του υποσυνόλου). *Για οποιαδήποτε σύνολα A και B τα ακόλουθα είναι ισοδύναμα:*

$$\textit{(i)}\ A \subseteq B, \qquad \textit{(ii)}\ A \cup B = B, \qquad \textit{(iii)}\ A \cap B = A.$$

Απόδειξη. (i)⇒(ii). Υποθέτουμε $A \subseteq B$ και δείχνουμε $A \cup B = B$ με διπλό εγκλεισμό. Αν $x \in A \cup B$, τότε $x \in A$ ή $x \in B$· αν $x \in A$, τότε $x \in B$ αφού $A \subseteq B$. Σε κάθε περίπτωση $x \in B$, άρα $A \cup B \subseteq B$. Αντίστροφα, αν $x \in B$ τότε προφανώς $x \in A \cup B$, άρα $B \subseteq A \cup B$.

(ii)⇒(iii). Υποθέτουμε $A \cup B = B$. Πάντα ισχύει $A \cap B \subseteq A$. Αν $x \in A$, τότε $x \in A \cup B = B$, άρα $x \in A \cap B$· δηλαδή $A \subseteq A \cap B$. Άρα $A \cap B = A$.

(iii)⇒(i). Υποθέτουμε $A \cap B = A$. Αν $x \in A$, τότε $x \in A \cap B$, άρα $x \in B$. Επομένως $A \subseteq B$. □

Δύο χρήσιμες αλήθειες για τις ενώσεις και τις τομές είναι οι παρακάτω ισότητες:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Αυτές οι ισότητες λέγονται *επιμεριστικοί νόμοι.*

Θυμίζουν την επιμεριστική ιδιότητα $a(b+c) = ab+ac$ των αριθμών, αλλά εδώ ισχύουν *και προς τις δύο κατευθύνσεις*: η τομή επιμερίζεται στην ένωση και η ένωση στην τομή (ενώ στους αριθμούς η πρόσθεση *δεν* επιμερίζεται στον πολλαπλασιασμό). Ας αποδείξουμε τον πρώτο νόμο. Αντί για διπλό εγκλεισμό, χρησιμοποιούμε μια *αλυσίδα ισοδυναμιών*: για οποιοδήποτε x,

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \text{ και } x \in B \cup C \\ &\iff x \in A \text{ και } (x \in B \text{ ή } x \in C) \\ &\iff (x \in A \text{ και } x \in B) \text{ ή } (x \in A \text{ και } x \in C) \\ &\iff x \in A \cap B \text{ ή } x \in A \cap C \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Αφού τα δύο σύνολα έχουν ακριβώς τα ίδια στοιχεία, είναι ίσα. Το κρίσιμο βήμα είναι το τρίτο, όπου χρησιμοποιήσαμε ότι το «και» επιμερίζεται στο «ή»· θα το ξαναδούμε ως ταυτολογία στην προτασιακή λογική (Κεφάλαιο 3). Ο δεύτερος νόμος αποδεικνύεται με τον ίδιο τρόπο (Άσκηση 14).

Ορισμός 1.12 (Διαφορά). Αν A και B είναι σύνολα, η *διαφορά* του B από το A, ή το *σχετικό συμπλήρωμα* του B στο A, ορίζεται από

$$A \setminus B = \{x \in A : x \notin B\}.$$

Για να διατυπώσουμε τις ιδιότητες του συμπληρώματος, υποθέτουμε ότι όλα τα σύνολα που θα αναφέρουμε είναι υποσύνολα ενός συνόλου $\mathcal{U}$ και ότι όλα τα συμπληρώματα θα σχηματισθούν σε σχέση με το $\mathcal{U}$. Γράφουμε $A' = \mathcal{U} \setminus A$. Το σύνολο $\mathcal{U}$ λέγεται *σύμπαν* (ή *καθολικό σύνολο*) και το A' *συμπλήρωμα* του A· σε άλλα βιβλία συμβολίζεται και $\overline{A}$ ή A^c. Οι βασικές ιδιότητες για τα συμπληρώματα είναι:

$$(A')' = A, \quad \emptyset' = \mathcal{U}, \quad \mathcal{U}' = \emptyset$$
$$A \cap A' = \emptyset, \quad A \cup A' = \mathcal{U}$$
$$A \subseteq B \Leftrightarrow B' \subseteq A'.$$

Η τελευταία ιδιότητα λέει ότι όσο «μεγαλώνει» ένα σύνολο, τόσο «μικραίνει» το συμπλήρωμά του. Επίσης, $A \setminus B = A \cap B'$, αφού και τα δύο σύνολα αποτελούνται από τα στοιχεία του A που δεν ανήκουν στο B.

Παράδειγμα 1.13. Έστω $\mathcal{U} = \{1, 2, \dots, 10\}$ και $A = \{2, 3, 5, 7\}$ (οι πρώτοι αριθμοί του $\mathcal{U}$). Τότε $A' = \{1, 4, 6, 8, 9, 10\}$. Αν $B = \{1, 2, 3\}$, τότε $A \setminus B = \{5, 7\}$ και $B \setminus A = \{1\}$.

Δύο πολύ σημαντικές ισότητες για τα συμπληρώματα είναι οι παρακάτω *νόμοι του De Morgan*:

$$(A \cup B)' = A' \cap B', \qquad (A \cap B)' = A' \cup B'.$$

Το συμπλήρωμα μιας ένωσης είναι η τομή των συμπληρωμάτων, και το συμπλήρωμα μιας τομής είναι η ένωση των συμπληρωμάτων. Για την απόδειξη του πρώτου νόμου χρησιμοποιούμε πάλι μια αλυσίδα ισοδυναμιών: για κάθε $x \in \mathcal{U}$,

$$\begin{aligned} x \in (A \cup B)' &\iff x \notin A \cup B \\ &\iff \text{δεν ισχύει ότι } (x \in A \text{ ή } x \in B) \\ &\iff x \notin A \text{ και } x \notin B \\ &\iff x \in A' \text{ και } x \in B' \\ &\iff x \in A' \cap B'. \end{aligned}$$

Ο δεύτερος νόμος αποδεικνύεται όμοια (Άσκηση 14). Θα ξαναδούμε τους νόμους του De Morgan, με ακριβώς την ίδια μορφή, στην προτασιακή λογική, για τους συνδέσμους «ή» και «και» στη θέση των $\cup$ και $\cap$ (Κεφάλαιο 3). Μια «οπτική» επαλήθευση του πρώτου νόμου δίνεται στο Σχήμα 1.4.

Μερικές εύκολες ασκήσεις για τα συμπληρώματα είναι οι παρακάτω:

$$\begin{aligned} A \setminus B &= A \cap B' \\ A \setminus (A \setminus B) &= A \cap B \\ A \cap (B \setminus C) &= (A \cap B) \setminus (A \cap C) \\ A \cap B &\subseteq (A \cap C) \cup (B \cap C') \\ (A \cup C) \cap (B \cup C') &\subseteq A \cup B. \end{aligned}$$

Την πρώτη από αυτές τη δείξαμε παραπάνω. Ως υπόδειγμα, αποδεικνύουμε τη δεύτερη με διπλό εγκλεισμό (οι υπόλοιπες ζητούνται στην Άσκηση 15).

Πρόταση 1.14. *Για οποιαδήποτε σύνολα A και B ισχύει $A \setminus (A \setminus B) = A \cap B$.*

Απόδειξη. ($\subseteq$) Έστω $x \in A \setminus (A \setminus B)$. Τότε $x \in A$ και $x \notin A \setminus B$, δηλαδή *δεν* ισχύει «$x \in A$ και $x \notin B$». Αφού $x \in A$, αυτό που δεν ισχύει πρέπει να είναι το $x \notin B$· άρα $x \in B$. Συνεπώς $x \in A \cap B$.

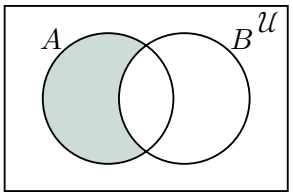
($\supseteq$) Έστω $x \in A \cap B$. Τότε $x \in A$ και $x \in B$. Αφού $x \in B$, δεν ισχύει $x \in A \setminus B$. Άρα $x \in A$ και $x \notin A \setminus B$, δηλαδή $x \in A \setminus (A \setminus B)$. □

Ορισμός 1.15 (Συμμετρική διαφορά). Η *συμμετρική διαφορά* δύο συνόλων A και B είναι το σύνολο

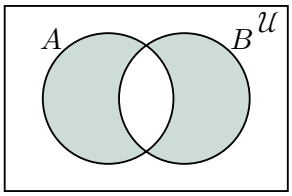
$$A \triangle B = (A \setminus B) \cup (B \setminus A),$$

δηλαδή το σύνολο των στοιχείων που ανήκουν σε *ακριβώς ένα* από τα A και B.

Για παράδειγμα, αν $A = \{1, 2, 3\}$ και $B = \{2, 3, 4\}$, τότε $A \triangle B = \{1, 4\}$. Ισοδύναμα, $A \triangle B = (A \cup B) \setminus (A \cap B)$: «ό,τι ανήκει σε *κάποιο* από τα δύο σύνολα, αλλά όχι *και στα δύο*» (βλ. Σχήμα 1.3). Η $\triangle$ είναι αντιμεταθετική και προσεταιριστική, και ισχύουν $A \triangle \emptyset = A$ και $A \triangle A = \emptyset$ (Άσκηση 20).

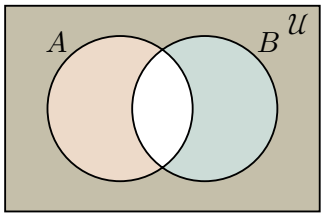


(α) $A \setminus B$

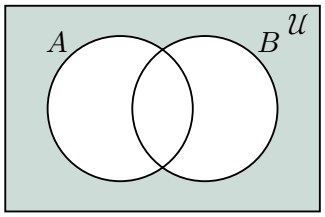


(β) $A \triangle B$

Σχήμα 1.3. Διαγράμματα Venn για τη διαφορά και τη συμμετρική διαφορά (σκιασμένες).



(α) A' (πράσινο) και B' (πορτοκαλί)



(β) $(A \cup B)'$

Σχήμα 1.4. Οπτική επαλήθευση του πρώτου νόμου του De Morgan. Στο (α) η περιοχή που είναι σκιασμένη *και με τα δύο* χρώματα (η πιο σκούρα) είναι το $A' \cap B'$, και συμπίπτει με την περιοχή που είναι σκιασμένη στο (β), δηλαδή με το $(A \cup B)'$. Οι περιοχές με ένα μόνο χρώμα είναι το $A \setminus B$ (μόνο πορτοκαλί) και το $B \setminus A$ (μόνο πράσινο).

Παράδειγμα 1.16 (Ένα μεγάλο παράδειγμα). Έστω $\mathcal{U} = \{1, 2, \dots, 10\}$, $A = \{1, 2, \dots, 6\}$, $B = \{2, 4, 6\}$, $C = \{1, 2, 3\}$ και $D = \{7, 8, 9\}$. Να βρεθούν τα σύνολα

$$A \cup B, \quad A \cap B, \quad B \cap C, \quad A \cap D, \quad (B \cup C)', \quad A \setminus B, \quad B \triangle C.$$

Λύση. Αφού $B \subseteq A$, από την Πρόταση 1.11 έχουμε $A \cup B = A = \{1, \dots, 6\}$ και $A \cap B = B = \{2, 4, 6\}$. Επίσης $B \cap C = \{2\}$ και $A \cap D = \emptyset$ (τα A, D είναι ξένα). Αφού $B \cup C = \{1, 2, 3, 4, 6\}$, είναι $(B \cup C)' = \{5, 7, 8, 9, 10\}$. Τέλος, $A \setminus B = \{1, 3, 5\}$ και, αφού $B \setminus C = \{4, 6\}$ και $C \setminus B = \{1, 3\}$, $B \triangle C = \{1, 3, 4, 6\}$. ◊

Παράδειγμα 1.17 (Τρία σύνολα). Ποια περιοχή ενός διαγράμματος Venn τριών συνόλων αναπαριστά το σύνολο $(B \cap C) \cup (C \cap A')$;

Λύση. Από τον (πρώτο) επιμεριστικό νόμο (και την αντιμεταθετικότητα της τομής),

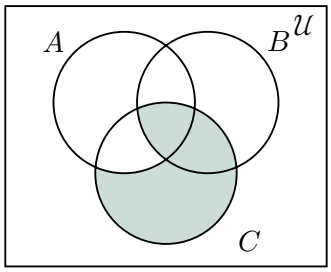
$$(B \cap C) \cup (C \cap A') = C \cap (B \cup A'),$$

δηλαδή πρόκειται για τα στοιχεία του C που ανήκουν στο B ή δεν ανήκουν στο A. Από το C εξαιρούνται λοιπόν ακριβώς τα στοιχεία που ανήκουν στο A αλλά όχι στο B· η περιοχή φαίνεται στο Σχήμα 1.5. Με τους νόμους του De Morgan, $B \cup A' = (A \cap B')'$, οπότε το ίδιο σύνολο γράφεται και $C \setminus (A \setminus B)$: δύο διαφορετικές εκφράσεις, *ίδιο* σύνολο. ◊

1.1.3 Δυναμοσύνολο και πληθικότητα

Ορισμός 1.18 (Δυναμοσύνολο). Για κάθε σύνολο A, το σύνολο όλων των υποσυνόλων του υπάρχει, συμβολίζεται με $\mathcal{P}(A)$ και λέγεται το *δυναμοσύνολο* του A, δηλαδή

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



Σχήμα 1.5. Το σύνολο $(B \cap C) \cup (C \cap A')$ του Παραδείγματος 1.17 (σκιασμένο).

Έχουμε $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$ και

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Προσέξτε ότι το $\mathcal{P}(\emptyset)$ *δεν* είναι κενό: έχει ένα στοιχείο, το $\emptyset$, αφού το κενό σύνολο έχει ένα υποσύνολο, τον εαυτό του. Τα δυναμοσύνολα των συνόλων με 0, 1 και 2 στοιχεία έχουν 1, 2 και 4 στοιχεία, αντίστοιχα. Το μοτίβο θα εξηγηθεί στην Πρόταση 1.21.

Παράδειγμα 1.19 (Κατασκευή βήμα-βήμα). Έστω $A = \{1, 2, 3\}$. Για να βρούμε το $\mathcal{P}(A)$ χωρίς να ξεχάσουμε κάποιο υποσύνολο, τα γράφουμε κατά μέγεθος: το υποσύνολο με 0 στοιχεία είναι το $\emptyset$· αυτά με 1 στοιχείο είναι τα $\{1\}, \{2\}, \{3\}$· αυτά με 2 στοιχεία είναι τα $\{1, 2\}, \{1, 3\}, \{2, 3\}$· και αυτό με 3 στοιχεία είναι το $\{1, 2, 3\}$. Άρα

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Προσοχή: $2 \in A$ αλλά $2 \notin \mathcal{P}(A)$, αφού τα στοιχεία του $\mathcal{P}(A)$ είναι σύνολα. Ισχύει όμως $\{2\} \in \mathcal{P}(A)$ και $\{2\} \subseteq A$.

Ορισμός 1.20 (Πληθικότητα). Η *πληθικότητα* $|A|$ ενός πεπερασμένου συνόλου A είναι το πλήθος των στοιχείων του.

Για παράδειγμα, $|\{23, 24, \dots, 38\}| = 38 - 23 + 1 = 16$ και $|\{1, \{2, 3, 4\}, \emptyset\}| = 3$ (τρία στοιχεία, δύο από τα οποία είναι σύνολα), ενώ για το «περίεργο» σύνολο του Παραδείγματος 1.1 είναι $|A| = 4$. Τι σημαίνει «πλήθος στοιχείων» για *άπειρα* σύνολα, όπως το $\mathbb{N}$ ή το $\mathbb{R}$, θα το δούμε στο Κεφάλαιο 2.

Πρόταση 1.21. *Αν το A είναι πεπερασμένο σύνολο με $|A| = n$, τότε $|\mathcal{P}(A)| = 2^n$.*

Απόδειξη. Έστω $A = \{a_1, a_2, \dots, a_n\}$. Για να περιγράψουμε ένα υποσύνολο $X \subseteq A$ αρκεί να αποφασίσουμε, για *κάθε* a_i, αν $a_i \in X$ ή $a_i \notin X$. Έτσι κάθε υποσύνολο του A αντιστοιχεί σε μία ακολουθία n αποφάσεων «μέσα/έξω», δηλαδή σε μία ακολουθία n δυαδικών ψηφίων (bits): το ψηφίο στη θέση i είναι 1 αν $a_i \in X$ και 0 αν $a_i \notin X$. Για παράδειγμα, για $n = 3$ η ακολουθία 101 αντιστοιχεί στο υποσύνολο $\{a_1, a_3\}$. Διαφορετικά υποσύνολα δίνουν διαφορετικές ακολουθίες, και κάθε ακολουθία προκύπτει από κάποιο υποσύνολο. Για κάθε ψηφίο υπάρχουν 2 επιλογές, άρα υπάρχουν συνολικά $2 \cdot 2 \cdots 2 = 2^n$ ακολουθίες, και επομένως 2^n υποσύνολα. □

Στην απόδειξη χρησιμοποιήσαμε (άτυπα) την *πολλαπλασιαστική αρχή* της απαρίθμησης, την οποία θα διατυπώσουμε με ακρίβεια στο Κεφάλαιο **??**.

Ασκήσεις

1. ⁻ Βρείτε το σύνολο $\mathcal{P}(\{a, b, c, d\})$.

2. Βρείτε την πληθικότητα κάθε συνόλου:

(α) $A = \{3, 4, \dots, 15\}$·

(β) $B = \{n \in \mathbb{N} : 2 < n \leq 200\}$·

(γ) $C = \{n \leq 100 : n \in \mathbb{N}$ και υπάρχει $m \in \mathbb{N}$ με $n = 2m + 1\}$·

(δ) $D = \{\mathbb{N}\}$·

(ε) ⋆ $E = \{2, |E|\}$ (!).

3. Βρείτε σύνολα A και B τέτοια ώστε $A \subseteq B$ *και* $A \in B$.

4. Μπορεί να υπάρχει ένα βιβλίο που αναφέρει όλα τα βιβλία που *δεν* αναφέρουν τον εαυτό τους, και μόνο αυτά; Εξηγήστε, και συγκρίνετε με το παράδοξο του Russell.

5. ⁻ Έστω $2\mathbb{Z}$ το σύνολο των άρτιων ακεραίων, $3\mathbb{Z}$ το σύνολο των πολλαπλασίων του 3, κ.ο.κ.

(α) Ισχύει $\mathbb{Z}_+ \subseteq 2\mathbb{Z}$; Ισχύει $2\mathbb{Z} \subseteq \mathbb{Z}_+$;

(β) Βρείτε το $2\mathbb{Z} \cap 3\mathbb{Z}$ και περιγράψτε το με λόγια.

(γ) Γράψτε το $\{x \in \mathbb{Z} :$ υπάρχει $y \in \mathbb{Z}$ με $x = 2y$ ή $x = 3y\}$ ως ένωση ή τομή δύο από τα παραπάνω σύνολα.

6. ⁻ Για σύνολα πραγματικών αριθμών A και B ορίζουμε $AB = \{ab : a \in A$ και $b \in B\}$. Αν $A = \{1, 2\}$ και $B = \{2, 3, 4\}$, πόσο είναι το $|AB|$; Πόσο είναι το $|A \times B|$ (βλ. Ενότητα 1.2);

7. Πληθικότητα ένωσης και τομής.

(α) Βρείτε δύο σύνολα A, B με $|A| = 5$, $|B| = 7$ και $|A \cup B| = 9$. Πόσο πρέπει να είναι το $|A \cap B|$;

(β) Το ίδιο, για $|A| = 5$, $|B| = 6$ και $|A \cup B| = 9$.

(γ) Υπάρχουν σύνολα A, B με $|A| = |B|$, $|A \cup B| = 10$ και $|A \cap B| = 5$;

8. Έστω $A = \{1, 2, \dots, 10\}$ και $\mathcal{B}_2 = \{B \subseteq A : |B| = 2\}$. Βρείτε το $|\mathcal{B}_2|$. Στη συνέχεια, για $A = \{1, 2, \dots, 12\}$ και $\mathcal{B}_3 = \{B \subseteq A : |B| = 3\}$, βρείτε το $|\mathcal{B}_3|$ χωρίς να απαριθμήσετε τα στοιχεία του.

9. Έστω $X = \{n \in \mathbb{N} : 10 \leq n < 20\}$. Βρείτε παραδείγματα συνόλων με τις παρακάτω ιδιότητες και εξηγήστε σύντομα γιατί λειτουργούν:

(α) ένα σύνολο $A \subseteq \mathbb{N}$ με $|A| = 10$ τέτοιο ώστε $X \setminus A = \{10, 12, 14\}$·

(β) ένα σύνολο $B \in \mathcal{P}(X)$ με $|B| = 5$·

(γ) ένα σύνολο $C \subseteq \mathcal{P}(X)$ με $|C| = 5$·

(δ) ένα σύνολο $D \subseteq X \times X$ με $|D| = 5$(βλ. Ενότητα 1.2)·

(ε) ένα σύνολο $E \subseteq X$ τέτοιο ώστε $|E| \in E$.

10. ⁻ Με σύμπαν το $\mathbb{R}$, έστω $A = \{x \in \mathbb{R} : 0 < x \leq 2\}$, $B = \{x \in \mathbb{R} : 1 \leq x < 4\}$ και $C = \{x \in \mathbb{R} : 3 \leq x < 9\}$. Βρείτε τα σύνολα $A \cup B$, $A \cap B$, A', $A \cup C$, $A \cap C$, B', $A' \cap B'$, $A' \cup B'$, $(A \cap B)'$ και $(A \cup B)'$. Ποια από αυτά είναι ίσα μεταξύ τους, και γιατί;

11. ⁻ Σχεδιάστε ένα διάγραμμα Venn για καθένα από τα σύνολα $A \cup B'$, $(A \cup B)'$, $A \cap (B \cup C)$, $(A \cap B) \cup C$, $A' \cap B \cap C'$ και $(A \cup B) \setminus C$.

12. Αποδείξτε ότι αν $A \subseteq B$ και $B \subseteq C$, τότε $A \subseteq C$. Δώστε παράδειγμα συνόλων A, B, C, το καθένα με δύο στοιχεία, με $A \in B$ και $B \in C$ αλλά $A \notin C$.

13. Αποδείξτε τους *νόμους της απορρόφησης*: $A \cup (A \cap B) = A$ και $A \cap (A \cup B) = A$.

14. Αποδείξτε τους επιμεριστικούς νόμους και τους νόμους του De Morgan. (Τον πρώτο νόμο κάθε ζεύγους τον αποδείξαμε στο κείμενο.)

15. Αποδείξτε, με διπλό εγκλεισμό ή με αλυσίδα ισοδυναμιών, ότι για οποιαδήποτε σύνολα A, B, C (υποσύνολα ενός σύμπαντος $\mathcal{U}$):

(α) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ και $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$·

(β) $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$·

(γ) $A \cap B \subseteq (A \cap C) \cup (B \cap C')$·

(δ) $(A \cup C) \cap (B \cup C') \subseteq A \cup B$.

16. Αποδείξτε ότι καθεμία από τις παρακάτω συνθήκες είναι ισοδύναμη με την $A \subseteq B$: (α) $A \cap B' = \emptyset$· (β) $A' \cup B = \mathcal{U}$· (γ) $B' \subseteq A'$· (δ) $A \setminus B = \emptyset$.

17. Αποδείξτε ότι $(A \cap B) \cup C = A \cap (B \cup C)$ αν και μόνο αν $C \subseteq A$.

18. Δείξτε ότι $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$ και $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Ισχύει πάντα ισότητα στο δεύτερο;

19. Αληθές ή ψευδές; Για όσα ισχύουν για οποιαδήποτε σύνολα A, B, C δώστε απόδειξη, για τα υπόλοιπα αντιπαράδειγμα (ένα διάγραμμα Venn βοηθά να το βρείτε).

(α) $A \setminus (B \setminus C) = (A \setminus B) \setminus C$·

(β) $(A \setminus B) \setminus C = A \setminus (B \cup C)$·

(γ) $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$·

(δ) αν $A \cap C = B \cap C$ *και* $A \cup C = B \cup C$, τότε $A = B$. Αρκεί μία μόνο από τις δύο υποθέσεις;

20. Αποδείξτε ότι $A \triangle B = (A \cup B) \setminus (A \cap B)$, ότι $A \triangle B = B \triangle A$, ότι $A \triangle \emptyset = A$ και ότι $A \triangle A = \emptyset$.

21. * Αποδείξτε ότι $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ και ότι $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. Στη συνέχεια δείξτε ότι αν $A \triangle B = A \triangle C$, τότε $B = C$.

22. * Βρείτε τα σύνολα A και B αν $A = \{3, |B|\}$ και $B = \{1, |A|, |B|\}$.

1.2 Σχέσεις

Σε έναν μήνα με 31 ημέρες, η 3η του μήνα «μοιάζει» περισσότερο με την 24η παρά με τη 15η. Γιατί; Επειδή η 3η και η 24η πέφτουν την *ίδια ημέρα της εβδομάδας*: η διαφορά τους, $24 - 3 = 21$, είναι πολλαπλάσιο του 7. Αυτό ορίζει έναν τρόπο να *συσχετίζουμε* ζεύγη ημερών, $a \sim b$ αν και μόνο αν το 7 διαιρεί το $a - b$, ο οποίος χωρίζει τις ημέρες του μήνα σε ομάδες (Δευτέρες, Τρίτες, κ.λπ.), έτσι ώστε κάθε ημέρα να ανήκει σε ακριβώς μία ομάδα. Σε αυτή την ενότητα τυποποιούμε αυτή την ιδέα: τι είναι μια *σχέση*, ποιες ιδιότητες μπορεί να έχει, και πώς οδηγεί σε έννοιες όπως η *ισοδυναμία* και η *διάταξη*.

1.2.1 Διατεταγμένα ζεύγη και σχέσεις

Γνωρίζουμε ότι ένα σύνολο με δύο μόνο στοιχεία λέγεται ζεύγος, π.χ., το $\{\alpha, \beta\}$. Αν όμως ξέρουμε και ποιο από τα δύο στοιχεία είναι πρώτο και ποιο από τα δύο στοιχεία είναι δεύτερο, τότε λέμε ότι έχουμε ένα *διατεταγμένο ζεύγος* και το συμβολίζουμε με (α, β). Δηλαδή το διατεταγμένο ζεύγος (α, β)

έχει πρώτο στοιχείο το α και δεύτερο το β· σε αντίθεση με το ζεύγος, μπορεί να είναι και $\alpha = \beta$. Το α λέγεται και *πρώτη συντεταγμένη* ενώ το β *δεύτερη συντεταγμένη* του διατεταγμένου ζεύγους (α, β).

Δύο διατεταγμένα ζεύγη (α, β) και (γ, δ) είναι ίσα, $(\alpha, \beta) = (\gamma, \delta)$ αν και μόνο αν $\alpha = \gamma$ και $\beta = \delta$, δηλαδή έχουν τις πρώτες συντεταγμένες ίσες και τις δεύτερες ίσες. Αυτό δεν ισχύει για τα ζεύγη. Για παράδειγμα, $\{1, 2\} = \{2, 1\}$, ενώ $(1, 2) \neq (2, 1)$· γενικά $(\alpha, \beta) \neq (\beta, \alpha)$, εκτός αν $\alpha = \beta$.

Ορισμός 1.22 (Καρτεσιανό γινόμενο). Έστω τώρα δύο σύνολα A και B. Το σύνολο όλων των διατεταγμένων ζευγών (α, β) με $\alpha \in A$ και $\beta \in B$ είναι ένα σύνολο που συμβολίζεται με $A \times B$ και το λέμε *Καρτεσιανό γινόμενο* των A και B.

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

Προφανώς $A \times B \neq B \times A$ γενικά.

Παράδειγμα 1.23. Αν $A = \{1, 2\}$ και $B = \{3, 4, 5\}$, τότε

$$A \times B = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\},$$

ενώ $(3, 1) \in B \times A$ αλλά $(3, 1) \notin A \times B$. Επίσης $A \times A = \{(1,1), (1,2), (2,1), (2,2)\}$. Γενικά, αν τα A και B είναι πεπερασμένα, τότε $|A \times B| = |A| \cdot |B|$, αφού για κάθε μία από τις $|A|$ επιλογές της πρώτης συντεταγμένης υπάρχουν $|B|$ επιλογές για τη δεύτερη. Για παράδειγμα, $|B \times B| = 3 \cdot 3 = 9$.

Η ιδέα επεκτείνεται σε περισσότερα από δύο σύνολα. Για σύνολα $A_1, A_2, \ldots, A_n$, το *(γενικευμένο) Καρτεσιανό γινόμενο*

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \,:\, a_i \in A_i \text{ για κάθε } i = 1, \ldots, n\}$$

είναι το σύνολο όλων των *διατεταγμένων n-άδων* με i-οστή συντεταγμένη από το A_i· δύο n-άδες είναι ίσες αν έχουν ίσες τις αντίστοιχες συντεταγμένες τους. Όπως πριν, για πεπερασμένα σύνολα

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Όταν όλα τα σύνολα είναι ίσα με A, γράφουμε $A^n = A \times A \times \cdots \times A$ (n φορές). Για παράδειγμα, το $\{0, 1\}^n$ είναι το σύνολο όλων των ακολουθιών n δυαδικών ψηφίων, και $|\{0, 1\}^n| = 2^n$: είναι το ίδιο μέτρημα με αυτό της Πρότασης 1.21.

Ορισμός 1.24 (Διμελής σχέση). *Διμελής σχέση* μεταξύ των στοιχείων δύο συνόλων X και Y ονομάζουμε κάθε υποσύνολο $R \subseteq X \times Y$. Αν $(x, y) \in R$ τότε θα λέμε ότι το x βρίσκεται στη σχέση R με το y και θα το συμβολίζουμε επίσης και ως xRy. Τις διμελείς σχέσεις θα τις λέμε *σχέσεις*. Συχνά ενδιαφερόμαστε για σχέσεις μεταξύ των στοιχείων ενός συνόλου, δηλαδή για $R \subseteq X \times Y$ με $X = Y$.

Μία *σχέση στο σύνολο* X σημαίνει μια διμελής σχέση μεταξύ των στοιχείων του X, δηλαδή ένα υποσύνολο του $X \times X$. Έτσι, π.χ., η ανισότητα των πραγματικών αριθμών είναι μια σχέση στο $\mathbb{R}$ και η συνθήκη «το 3 διαιρεί τη διαφορά $x - y$» ορίζει μια σχέση στο σύνολο των ακεραίων $\mathbb{Z}$, δηλαδή

$$< \;= \{(x, y) \,:\, x, y \in \mathbb{R} \text{ με } x < y\} \subseteq \mathbb{R} \times \mathbb{R}$$

$$\equiv_3 = \{(x, y) \,:\, x, y \in \mathbb{Z} \text{ με } 3 \mid (x - y)\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

Το *πεδίο ορισμού* μιας σχέσης $R \subseteq X \times Y$ είναι το σύνολο $\{x \in X \,:\, \text{για κάποιο } y \in Y,\ xRy\}$, και το *πεδίο τιμών* της R είναι το σύνολο $\{y \in Y \,:\, \text{για κάποιο } x \in X,\ xRy\}$ (για σχέση στο A είναι $X = Y = A$).

Παράδειγμα 1.25 (Η σχέση «διαιρεί»). Στο $A = \{1, 2, 3, 4\}$ θεωρούμε τη σχέση R με xRy αν και μόνο αν $x \mid y$ (το x διαιρεί το y). Τότε

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}.$$

Το πεδίο ορισμού και το πεδίο τιμών της R είναι και τα δύο ίσα με $\{1, 2, 3, 4\}$. Αυτό δεν ισχύει πάντα: για τη σχέση $S = \{(1,2), (1,3), (2,4)\}$ στο ίδιο σύνολο, το πεδίο ορισμού είναι το $\{1, 2\}$ και το πεδίο τιμών το $\{2, 3, 4\}$.

Ορισμός 1.26 (Αντίστροφη σχέση). Η *αντίστροφη* μιας σχέσης $R \subseteq X \times Y$ είναι η σχέση

$$R^{-1} = \{(y, x) \,:\, (x, y) \in R\} \subseteq Y \times X.$$

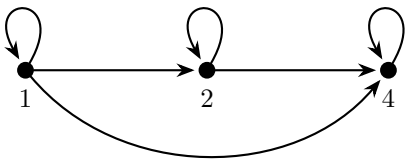
Για τη σχέση S του Παραδείγματος 1.25 έχουμε $S^{-1} = \{(2,1), (3,1), (4,2)\}$. Η αντίστροφη της $<$ στο $\mathbb{R}$ είναι η $>$. Το πεδίο ορισμού της R^{-1} είναι το πεδίο τιμών της R, και αντίστροφα.

Ορισμός 1.27 (Σύνθεση σχέσεων). Για σχέσεις $R \subseteq X \times Y$ και $S \subseteq Y \times Z$, η *σύνθεσή* τους είναι η σχέση

$$S \circ R = \{(x, z) \in X \times Z \,:\, \text{υπάρχει } y \in Y \text{ με } (x, y) \in R \text{ και } (y, z) \in S\}.$$

Παράδειγμα 1.28. Έστω $X = \{1, 2\}$, $Y = \{a, b\}$, $Z = \{p, q\}$, $R = \{(1, a), (2, a), (2, b)\}$ και $S = \{(a, p), (b, q)\}$. Το 1 «φτάνει» στο a μέσω της R και το a φτάνει στο p μέσω της S, άρα $(1, p) \in S \circ R$. Όμοια $(2, p) \in S \circ R$ (μέσω του a) και $(2, q) \in S \circ R$ (μέσω του b). Άρα $S \circ R = \{(1, p), (2, p), (2, q)\}$.

Μια σχέση R σε ένα πεπερασμένο σύνολο A μπορεί να αναπαρασταθεί με ένα *κατευθυνόμενο γράφημα*: σχεδιάζουμε μία κορυφή για κάθε στοιχείο του A και ένα βέλος από την κορυφή a στην κορυφή b για κάθε ζεύγος $(a, b) \in R$· ένα ζεύγος (a, a) αναπαρίσταται με έναν *βρόχο* στην κορυφή a. Για παράδειγμα, το Σχήμα 1.6 δείχνει τη σχέση «διαιρεί» στο $\{1, 2, 4\}$. Τα κατευθυνόμενα γραφήματα θα τα μελετήσουμε συστηματικά στο Κεφάλαιο **??**.



Σχήμα 1.6. Το κατευθυνόμενο γράφημα της σχέσης «διαιρεί» στο σύνολο $\{1, 2, 4\}$.

Παρατηρήστε στο σχήμα ότι: (α) σε κάθε κορυφή υπάρχει βρόχος, δηλαδή κάθε στοιχείο σχετίζεται με τον εαυτό του· (β) δεν υπάρχει κανένα ζεύγος «αντίθετων» βελών μεταξύ δύο διαφορετικών κορυφών· (γ) το βέλος $1 \to 4$ υπάρχει, όπως «αναμένεται», αφού υπάρχουν τα βέλη $1 \to 2$ και $2 \to 4$. Αυτές οι τρεις παρατηρήσεις αντιστοιχούν σε τρεις από τις ιδιότητες σχέσεων που ορίζουμε αμέσως τώρα.

1.2.2 Ιδιότητες σχέσεων

Ορισμός 1.29 (Αυτοπαθής, συμμετρική, μεταβατική σχέση). Μια σχέση R στο A ($R \subseteq A \times A$) είναι *αυτοπαθής* αν aRa ($(a,a) \in R$) για κάθε $a \in A$. Είναι *συμμετρική* αν aRb συνεπάγεται bRa και είναι *μεταβατική* αν aRb και bRc συνεπάγονται aRc.

Στο κατευθυνόμενο γράφημα μιας σχέσης (σε πεπερασμένο σύνολο), η R είναι αυτοπαθής αν και μόνο αν κάθε κορυφή έχει βρόχο· συμμετρική αν και μόνο αν για κάθε βέλος υπάρχει και το «αντίθετό» του· και μεταβατική αν και μόνο αν για κάθε «διαδρομή δύο βημάτων» $a \to b \to c$ υπάρχει και το «απευθείας» βέλος $a \to c$.

Παράδειγμα 1.30. Θεωρούμε τις σχέσεις $\leq$ και $<$ στο $\mathbb{R}$, τη σχέση «διαιρεί» ($|$) στο $\mathbb{Z}_+$, και τις σχέσεις στο $\mathbb{Z}$

$$a \approx b \iff |a-b| \leq 3 \qquad \text{και} \qquad a \bowtie b \iff a+b=0.$$

- *Αυτοπάθεια.* Οι $\leq$, $|$ και $\approx$ είναι αυτοπαθείς ($a \leq a$, $a \mid a$, $|a-a| = 0 \leq 3$). Οι $<$ και $\bowtie$ δεν είναι: $1 \not< 1$ και $1+1 \neq 0$.
- *Συμμετρία.* Οι $\approx$ και $\bowtie$ είναι συμμετρικές, αφού $|a-b| = |b-a|$ και $a+b = b+a$. Οι $\leq$ και $|$ δεν είναι: $3 \leq 4$ αλλά $4 \not\leq 3$, και $2 \mid 6$ αλλά $6 \nmid 2$.
- *Μεταβατικότητα.* Οι $\leq$, $<$ και $|$ είναι μεταβατικές. Η $\approx$ δεν είναι: $1 \approx 3$ και $3 \approx 5$, αλλά $|1-5| = 4 > 3$. Ούτε η $\bowtie$: $5 \bowtie (-5)$ και $(-5) \bowtie 5$, αλλά $5+5 \neq 0$.

Η συμμετρία μιας σχέσης εκφράζεται πολύ απλά με τη βοήθεια της αντίστροφης σχέσης.

Πρόταση 1.31. *Μια σχέση R στο A είναι συμμετρική αν και μόνο αν $R = R^{-1}$.*

Απόδειξη. ($\Rightarrow$) Έστω ότι η R είναι συμμετρική. Αν $(a,b) \in R$, τότε από τη συμμετρία $(b,a) \in R$, άρα $(a,b) \in R^{-1}$ από τον ορισμό της αντίστροφης σχέσης. Επομένως $R \subseteq R^{-1}$. Αντίστροφα, αν $(a,b) \in R^{-1}$, τότε $(b,a) \in R$ και από τη συμμετρία $(a,b) \in R$· άρα $R^{-1} \subseteq R$. Συνεπώς $R = R^{-1}$.

($\Leftarrow$) Έστω ότι $R = R^{-1}$. Αν $(a,b) \in R$, τότε $(a,b) \in R^{-1}$, δηλαδή $(b,a) \in R$. Άρα η R είναι συμμετρική. □

Ορισμός 1.32 (Αντισυμμετρική σχέση). Μια σχέση R στο A ($A \neq \emptyset$) λέγεται *αντισυμμετρική* αν για κάθε a και b

$$aRb \text{ και } bRa \Rightarrow a = b.$$

Για παράδειγμα, η $\leq$ στο $\mathbb{R}$ είναι αντισυμμετρική (αν $a \leq b$ και $b \leq a$, τότε $a = b$) αλλά δεν είναι συμμετρική, ενώ η $\approx$ του Παραδείγματος 1.30 είναι συμμετρική αλλά όχι αντισυμμετρική ($1 \approx 2$ και $2 \approx 1$). Στο κατευθυνόμενο γράφημα, η R είναι αντισυμμετρική αν και μόνο αν κανένα βέλος μεταξύ δύο *διαφορετικών* κορυφών δεν έχει το «αντίθετό» του.

Παρατήρηση 1.33 (Προσοχή). Η αντισυμμετρική σχέση *δεν* είναι το αντίθετο της συμμετρικής. Μια σχέση μπορεί να μην είναι ούτε συμμετρική ούτε αντισυμμετρική (δείτε το επόμενο παράδειγμα), και μπορεί να είναι και τα δύο, όπως δείχνει η επόμενη πρόταση.

Πρόταση 1.34. *Αν η σχέση R στο A είναι* και *συμμετρική* και *αντισυμμετρική, τότε $R \subseteq \{(a,a) : a \in A\}$.*

Απόδειξη. Έστω $(a,b) \in R$. Από τη συμμετρία, $(b,a) \in R$. Έχουμε λοιπόν aRb και bRa, άρα από την αντισυμμετρία $a = b$. Επομένως κάθε στοιχείο της R είναι της μορφής (a,a). □

Έτσι, οι δύο ιδιότητες συνυπάρχουν μόνο στη σχέση της ισότητας $\{(a,a) : a \in A\}$ και στα υποσύνολά της.

Παράδειγμα 1.35 (Ελέγχοντας τις ιδιότητες). Στο $A = \{1,2,3,4\}$ έστω

$$R = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(2,3)\}.$$

Η R είναι αυτοπαθής, αφού περιέχει όλα τα ζεύγη (a,a). Δεν είναι συμμετρική, αφού $(2,3) \in R$ αλλά $(3,2) \notin R$. Δεν είναι μεταβατική, αφού $(1,2),(2,3) \in R$ αλλά $(1,3) \notin R$. Δεν είναι ούτε αντισυμμετρική, αφού $(1,2),(2,1) \in R$ αλλά $1 \neq 2$.

1.2.3 Σχέσεις ισοδυναμίας και διαμερίσεις

Ορισμός 1.36 (Σχέση ισοδυναμίας). Μια σχέση στο σύνολο A που είναι αυτοπαθής, συμμετρική και μεταβατική λέγεται *σχέση ισοδυναμίας*.

Το πρότυπο παράδειγμα σχέσης ισοδυναμίας είναι η *ισότητα*: $a = a$· αν $a = b$ τότε $b = a$· αν $a = b$ και $b = c$ τότε $a = c$. Μια σχέση ισοδυναμίας είναι, διαισθητικά, οτιδήποτε «συμπεριφέρεται σαν ισότητα»: εκφράζει την ιδέα ότι δύο αντικείμενα είναι «ουσιαστικά το ίδιο» ως προς κάποιο χαρακτηριστικό (π.χ., ημέρες που πέφτουν την ίδια ημέρα της εβδομάδας).

Ορισμός 1.37 (Κλάση ισοδυναμίας, σύνολο πηλίκο). Αν R είναι μια σχέση ισοδυναμίας στο σύνολο A ($A \neq \emptyset$) η *κλάση ισοδυναμίας* του $a \in A$ ως προς την R είναι το σύνολο $[a]_R = \{b \in A : aRb\}$. Το σύνολο όλων των κλάσεων ισοδυναμίας ως προς την R είναι το σύνολο $A/R = \{[a]_R : a \in A\}$, είναι υποσύνολο του $\mathcal{P}(A)$ και λέγεται *σύνολο πηλίκο*.

Τα σύνολα $[a]_R$, $a \in A$ μέλη του A/R έχουν τις παρακάτω ιδιότητες:

1. $[a]_R = [b]_R \Leftrightarrow aRb$ για $a, b \in A$,
2. $[a]_R \neq [b]_R \Rightarrow [a]_R \cap [b]_R = \emptyset$,
3. $\bigcup\{[a]_R : a \in A\} = A$.

Η (1) είναι εύκολη (την αποδεικνύουμε παρακάτω). Για την (2) δείχνουμε ότι αν δύο κλάσεις έχουν κοινό στοιχείο, τότε είναι ίσες. Έστω $c \in [a]_R \cap [b]_R$. Τότε aRc και bRc, και επειδή η R είναι συμμετρική θα έχουμε cRb. Από τα aRc και cRb έχουμε aRb, επειδή η R είναι μεταβατική, και από την (1) θα έχουμε $[a]_R = [b]_R$. Όσον αφορά την (3), επειδή κάθε $a \in A$ ανήκει σε κάποια κλάση ισοδυναμίας (για παράδειγμα $a \in [a]_R$) είναι προφανές ότι η ένωση όλων των κλάσεων ισοδυναμίας είναι το A.

Για πληρότητα, δίνουμε και την απόδειξη της (1).

Απόδειξη της (1). ($\Rightarrow$) Έστω $[a]_R = [b]_R$. Αφού η R είναι αυτοπαθής, bRb, δηλαδή $b \in [b]_R = [a]_R$. Άρα aRb.

($\Leftarrow$) Έστω aRb. Δείχνουμε πρώτα ότι $[b]_R \subseteq [a]_R$: αν $c \in [b]_R$, τότε bRc, και από τη μεταβατικότητα (aRb και bRc) έχουμε aRc, δηλαδή $c \in [a]_R$. Επίσης, από τη συμμετρία έχουμε bRa, οπότε με το ίδιο επιχείρημα (με τους ρόλους των a και b αντεστραμμένους) $[a]_R \subseteq [b]_R$. Άρα $[a]_R = [b]_R$. □

Επομένως το σύνολο A/R είναι σύνολο υποσυνόλων του A που η ένωσή τους μας κάνει το A, τα δε υποσύνολα αυτά είναι ξένα μεταξύ τους ανά δύο από την ιδιότητα (2). Δηλαδή το σύνολο A/R είναι μια *διαμέριση* (ή *μερισμός*) του A, που σημαίνει

1. $[a]_R \in A/R \Rightarrow [a]_R \neq \emptyset$,
2. $\bigcup(A/R) = A$,
3. δύο διαφορετικά μέλη του A/R είναι ξένα μεταξύ τους.

Ας δώσουμε τον γενικό ορισμό και ας διατυπώσουμε το αποτέλεσμα ως θεώρημα.

Ορισμός 1.38 (Διαμέριση). Μια *διαμέριση* (ή *μερισμός*) ενός συνόλου A είναι μια συλλογή μη κενών υποσυνόλων του A, ανά δύο ξένων μεταξύ τους, των οποίων η ένωση είναι το A. Τα μέλη της διαμέρισης λέγονται και *μερίδια*.

Θεώρημα 1.39. *Κάθε σχέση ισοδυναμίας R στο A ορίζει μια διαμέριση του A, το σύνολο πηλίκο A/R.*

Η απόδειξη δόθηκε ακριβώς πριν: κάθε κλάση $[a]_R$ είναι μη κενή, αφού $a \in [a]_R$· διαφορετικές κλάσεις είναι ξένες, από την ιδιότητα (2)· και η ένωση των κλάσεων είναι το A, από την ιδιότητα (3). Ισχύει και το αντίστροφο:

Θεώρημα 1.40. *Κάθε διαμέριση $\mathcal{D}$ ενός συνόλου A ορίζει μια σχέση ισοδυναμίας $R_\mathcal{D}$ στο A: $a\ R_\mathcal{D}\ b$ αν και μόνο αν τα a και b ανήκουν στο ίδιο μερίδιο της $\mathcal{D}$. Επιπλέον, οι κλάσεις ισοδυναμίας της $R_\mathcal{D}$ είναι ακριβώς τα μερίδια της $\mathcal{D}$.*

Απόδειξη. Αυτοπάθεια: κάθε $a \in A$ ανήκει σε κάποιο μερίδιο, αφού η ένωση των μεριδίων είναι το A· άρα $a\ R_\mathcal{D}\ a$. *Συμμετρία:* αν τα a, b ανήκουν στο ίδιο μερίδιο, τότε προφανώς και τα b, a. *Μεταβατικότητα:* έστω $a, b \in P$ και $b, c \in Q$ για κάποια μερίδια P, Q. Τότε $b \in P \cap Q$, και αφού διαφορετικά μερίδια είναι ξένα, $P = Q$· άρα τα a, c ανήκουν στο ίδιο μερίδιο. Τέλος, αν $a \in P$, τότε $[a]_{R_\mathcal{D}}$ αποτελείται από τα στοιχεία που βρίσκονται στο ίδιο μερίδιο με το a, δηλαδή $[a]_{R_\mathcal{D}} = P$. □

Οι σχέσεις ισοδυναμίας και οι διαμερίσεις είναι επομένως, ουσιαστικά, *δύο όψεις της ίδιας ιδέας.*

Παράδειγμα 1.41. Ορίζουμε την σχέση $\equiv_4$ στο σύνολο των ακεραίων $\mathbb{Z}$. Θα λέμε $(a, b) \in \equiv_4$, $a \equiv_4 b$ αν και μόνο αν η διαφορά $a - b$ είναι πολλαπλάσιο του 4, δηλαδή αν $a - b = 4k$ για κάποιο $k \in \mathbb{Z}$:

$$a \equiv_4 b \Leftrightarrow a - b = 4k \text{ για κάποιο } k \in \mathbb{Z}.$$

Έχουμε $a \equiv_4 a$ για κάθε $a \in \mathbb{Z}$, αφού $a - a = 0 = 0 \cdot 4$.

Αν $a \equiv_4 b$ τότε $a - b = 4k \Rightarrow b - a = -4k = 4(-k) \Rightarrow b \equiv_4 a$.

Αν $a \equiv_4 b$ και $b \equiv_4 c$:

$$\left.\begin{aligned} a - b &= 4\lambda \\ b - c &= 4\mu \end{aligned}\right\} \Rightarrow a - c = 4(\lambda + \mu),\ \lambda, \mu \in \mathbb{Z} \Rightarrow a \equiv_4 c.$$

Άρα η σχέση $\equiv_4$ στο $\mathbb{Z}$ είναι αυτοπαθής, συμμετρική και μεταβατική και επομένως είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$. Οι κλάσεις ισοδυναμίας είναι:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x = 4k \text{ για } k \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\} \\
[1] &= \{x \in \mathbb{Z} : x = 4k + 1 \text{ για } k \in \mathbb{Z}\} = \{\dots, -7, -3, 1, 5, 9, \dots\} \\
[2] &= \{x \in \mathbb{Z} : x = 4k + 2 \text{ για } k \in \mathbb{Z}\} = \{\dots, -6, -2, 2, 6, 10, \dots\} \\
[3] &= \{x \in \mathbb{Z} : x = 4k + 3 \text{ για } k \in \mathbb{Z}\} = \{\dots, -5, -1, 3, 7, 11, \dots\}.
\end{aligned}$$

Κάθε ακέραιος a είναι της μορφής $4k$ ή $4k+1$ ή $4k+2$ ή $4k+3$ για $k \in \mathbb{Z}$, ανάλογα με το τι υπόλοιπο αφήνει αν διαιρεθεί με το 4. Έχουμε λοιπόν $\mathbb{Z}/\equiv_4 = \{[0], [1], [2], [3]\}$, ανά δύο οι κλάσεις είναι ξένες μεταξύ τους και $\bigcup(\mathbb{Z}/\equiv_4) = \mathbb{Z}$. Άρα το σύνολο $\mathbb{Z}/\equiv_4$ είναι μια διαμέριση του $\mathbb{Z}$. Μπορούμε να έχουμε σχέσεις παρόμοιες με την παραπάνω, τις $\equiv_n$ για $n \in \mathbb{N}$.

Παράδειγμα 1.42 («Ίδιο πρόσημο»). Στο $A = \mathbb{Z} \setminus \{0\}$ ορίζουμε $a \sim b$ αν και μόνο αν $a \cdot b > 0$, δηλαδή αν οι a και b έχουν το ίδιο πρόσημο. Η $\sim$ είναι αυτοπαθής, αφού $a \cdot a = a^2 > 0$ για $a \neq 0$· συμμετρική, αφού $ab = ba$· και μεταβατική, αφού αν οι a, b έχουν το ίδιο πρόσημο και οι b, c έχουν

το ίδιο πρόσημο, τότε και οι a, c έχουν το ίδιο πρόσημο. Είναι λοιπόν σχέση ισοδυναμίας, με δύο κλάσεις: $[1] = \mathbb{Z}_+$ (οι θετικοί ακέραιοι) και $[-1]$ (οι αρνητικοί ακέραιοι). Η αντίστοιχη διαμέριση του A έχει δύο μερίδια.

1.2.4 Σχέσεις διάταξης

Ορισμός 1.43 (Μερική διάταξη). *Μερική διάταξη* στο A λέγεται μια σχέση στο A που είναι αυτοπαθής, αντισυμμετρική και μεταβατική. Δηλαδή η $R \subseteq A \times A$ είναι μια μερική διάταξη στο A αν:

$$aRa, \text{ για κάθε } a \in A$$
$$aRb \text{ και } bRa \Rightarrow a = b$$
$$aRb \text{ και } bRc \Rightarrow aRc.$$

Αν επιπλέον για κάθε $a, b \in A$ είτε aRb είτε bRa τότε η μερική διάταξη R λέγεται *ολική* ή *γραμμική διάταξη*. Ένα *μερικά διατεταγμένο σύνολο* X είναι ένα σύνολο X με μια μερική διάταξη στο X. Αν $\preceq$ είναι μια μερική διάταξη στο X και για $x, y \in X$ έχουμε $x \preceq y$ και $x \neq y$ γράφουμε $x \prec y$ και η $\prec$ είναι τότε μια σχέση στο X με ιδιότητες:

1. Δεν υπάρχουν x και y τέτοια ώστε $x \prec y$ και $y \prec x$, και
2. Αν $x \prec y$ και $y \prec z$ τότε $x \prec z$.

Ένα μερικά διατεταγμένο σύνολο το γράφουμε και ως ζεύγος $(X, \preceq)$. Το πρότυπο παράδειγμα μερικής διάταξης είναι η $\leq$ στο $\mathbb{N}$ ή στο $\mathbb{R}$, που είναι μάλιστα ολική. Δύο σημαντικά παραδείγματα μερικών διατάξεων που *δεν* είναι ολικές είναι η σχέση $\subseteq$ στο $\mathcal{P}(X)$, όταν $|X| \geq 2$ (π.χ., για τα $\{a\}$ και $\{b\}$ δεν ισχύει ούτε $\{a\} \subseteq \{b\}$ ούτε $\{b\} \subseteq \{a\}$), και η διαιρετότητα στο $\mathbb{Z}_+$.

Παράδειγμα 1.44 (Η διαιρετότητα στο $\mathbb{Z}_+$). Για $a, b \in \mathbb{Z}_+$ ορίζουμε $a \mid b$ αν και μόνο αν υπάρχει $k \in \mathbb{Z}_+$ με $b = ka$. Η $\mid$ είναι αυτοπαθής, αφού $a = 1 \cdot a$. Είναι αντισυμμετρική: αν $a \mid b$ και $b \mid a$, τότε $b = ka$ και $a = \ell b$ για κάποια $k, \ell \in \mathbb{Z}_+$, οπότε $a = \ell ka$ και άρα $\ell k = 1$· αφού οι k, ℓ είναι θετικοί ακέραιοι, $k = \ell = 1$, δηλαδή $a = b$. Είναι μεταβατική: αν $b = ka$ και $c = jb$ με $k, j \in \mathbb{Z}_+$, τότε $c = (jk)a$ με $jk \in \mathbb{Z}_+$, άρα $a \mid c$. Επομένως η $\mid$ είναι μερική διάταξη στο $\mathbb{Z}_+$. Δεν είναι όμως ολική: ούτε $2 \mid 3$ ούτε $3 \mid 2$· τα 2 και 3 είναι *μη συγκρίσιμα* στοιχεία.

Αν X είναι ένα μερικά διατεταγμένο σύνολο (ή ολικά διατεταγμένο) τότε μπορεί να συμβεί το X να έχει ένα στοιχείο a τέτοιο ώστε $a \preceq x$ για κάθε $x \in X$. Σ' αυτή την περίπτωση λέμε ότι το a είναι το *ελάχιστο στοιχείο* του X ως προς τη διάταξη $\preceq$ του X. Παρόμοια αν το X έχει στοιχείο b τέτοιο ώστε $a \preceq b$ για κάθε $a \in X$, τότε το b είναι το *μέγιστο στοιχείο* του X ως προς τη διάταξη $\preceq$ στο X.

Πρόταση 1.45. *Αν ένα μερικά διατεταγμένο σύνολο $(X, \preceq)$ έχει ελάχιστο (αντίστοιχα, μέγιστο) στοιχείο, τότε αυτό είναι μοναδικό.*

Απόδειξη. Αν τα a και a' είναι και τα δύο ελάχιστα στοιχεία, τότε $a \preceq a'$ (αφού το a είναι ελάχιστο) και $a' \preceq a$ (αφού το a' είναι ελάχιστο). Από την αντισυμμετρία, $a = a'$. Η απόδειξη για το μέγιστο είναι όμοια. □

Για παράδειγμα, στο $(\mathcal{P}(X), \subseteq)$ το ελάχιστο στοιχείο είναι το $\emptyset$ και το μέγιστο το X, ενώ το $(\mathbb{Z}, \leq)$ δεν έχει ούτε ελάχιστο ούτε μέγιστο στοιχείο.

Όπως πριν, αν X είναι ένα μερικά διατεταγμένο σύνολο ως προς τη μερική διάταξη $\preceq$ στο X, το $a \in X$ λέγεται *σχετικό ελάχιστο* ή *ελάσσον στοιχείο* του X αν δεν υπάρχει στοιχείο $x \in X$ με $x \preceq a$ και $x \neq a$. Παρόμοια το $b \in X$ λέγεται *σχετικό μέγιστο* ή *μείζον στοιχείο* του X αν δεν υπάρχει x με $b \preceq x$ και $b \neq x$.

Ένα ελάχιστο στοιχείο είναι πάντα ελάσσον, αλλά το αντίστροφο δεν ισχύει: σε μια μερική (όχι ολική) διάταξη μπορεί να μην υπάρχει ελάχιστο στοιχείο, αλλά να υπάρχουν *πολλά* ελάσσονα.

Παράδειγμα 1.46. Στο $X = \{2, 3, 4, 5, 6\}$ με τη διαιρετότητα, τα 2, 3 και 5 είναι ελάσσονα στοιχεία (κανένα στοιχείο του X διαφορετικό από αυτά δεν τα διαιρεί), αλλά δεν υπάρχει ελάχιστο στοιχείο: κανένα στοιχείο του X δεν διαιρεί όλα τα υπόλοιπα. Τα μείζονα στοιχεία είναι τα 4, 5 και 6 (το 5 είναι και ελάσσον και μείζον), και δεν υπάρχει μέγιστο.

Θεώρημα 1.47 (Ύπαρξη ελάσσονος στοιχείου). *Κάθε μη κενό, πεπερασμένο μερικά διατεταγμένο σύνολο $(X, \preceq)$ έχει τουλάχιστον ένα ελάσσον στοιχείο.*

Απόδειξη. Ξεκινάμε από ένα οποιοδήποτε $x_1 \in X$. Αν το x_1 είναι ελάσσον, τελειώσαμε. Αλλιώς υπάρχει $x_2 \in X$ με $x_2 \prec x_1$. Αν το x_2 είναι ελάσσον, τελειώσαμε· αλλιώς υπάρχει $x_3 \prec x_2$, κ.ο.κ. Έτσι κατασκευάζουμε μια ακολουθία $x_1 \succ x_2 \succ x_3 \succ \cdots$. Από τη μεταβατικότητα της $\prec$ έχουμε $x_j \prec x_i$ για κάθε $i < j$, οπότε όλα τα x_i είναι διαφορετικά μεταξύ τους (αν ήταν $x_i = x_j$ με $i < j$, θα είχαμε $x_i \prec x_i$, δηλαδή $x_i \neq x_i$, άτοπο). Αφού το X είναι πεπερασμένο, η ακολουθία δεν μπορεί να συνεχίζεται για πάντα: έχει το πολύ $|X|$ όρους. Άρα η διαδικασία σταματά σε κάποιο x_n, που είναι ελάσσον στοιχείο. □

Η υπόθεση ότι το X είναι πεπερασμένο είναι απαραίτητη: το $(\mathbb{Z}, \leq)$ δεν έχει κανένα ελάσσον στοιχείο.

Έστω τώρα το μερικά διατεταγμένο σύνολο $(X, \preceq)$. Το $c \in X$ λέγεται *κάτω φράγμα* του $E \subseteq X$ αν $c \preceq x$ για κάθε $x \in E$ και το $d \in X$ λέγεται *άνω φράγμα* του $E \subseteq X$ αν $x \preceq d$ για κάθε $x \in E$.

Προσοχή: ένα φράγμα του E πρέπει να ανήκει στο X, αλλά *όχι* απαραίτητα στο E. Για παράδειγμα, στο $(\mathbb{R}, \leq)$ το 0 είναι κάτω φράγμα του διαστήματος $E = (0, 1)$, ενώ $0 \notin E$· κάτω φράγματα του E είναι όλοι οι αριθμοί $c \leq 0$, και άνω φράγματα όλοι οι $d \geq 1$.

Ασκήσεις

1. ⁻ Βρείτε το σύνολο $A \times A$ αν $A = \{a, b, c\}$. Βρείτε το σύνολο των (μη διατεταγμένων) ζευγών από στοιχεία του A.

2. Αποδείξτε ότι αν A, B, X και Y είναι σύνολα, τότε

i) $(A \cup B) \times X = (A \times X) \cup (B \times X)$

ii) $(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)$

3. Πεδία, αντίστροφη και σύνθεση σχέσεων.

(α) Έστω $A = \{3, 4, 5\}$, $B = \{4, 5, 6\}$ και S η σχέση από το A στο B με $x \ S \ y$ αν και μόνο αν $x \mid y$. Γράψτε τα ζεύγη της S και της S^{-1}, και το πεδίο ορισμού και το πεδίο τιμών της καθεμιάς.

(β) Στο $\{1, 2, 3, 4\}$ έστω $R = \{(1, 2), (2, 3), (3, 4)\}$. Βρείτε τις σχέσεις $R \circ R$, $R^{-1} \circ R$ και $R \circ R^{-1}$ και σχεδιάστε τα κατευθυνόμενα γραφήματά τους. Είναι ίσες οι $R^{-1} \circ R$ και $R \circ R^{-1}$; Είναι κάποια από αυτές η σχέση ισότητας $\{(a, a) : a \in \{1, 2, 3, 4\}\}$;

4. ⁻ Στο σύνολο $A = \{a, b, c, d\}$ θεωρήστε τη σχέση

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c)\}.$$

Σχεδιάστε το κατευθυνόμενο γράφημά της και ελέγξτε αν η R είναι αυτοπαθής, συμμετρική, μεταβατική, αντισυμμετρική. Είναι σχέση ισοδυναμίας; Είναι μερική διάταξη; Είναι ολική διάταξη;

5. Βρείτε, αν υπάρχει, μια σχέση στο $\{1,2,3,4\}$ που να είναι

(α) αυτοπαθής και συμμετρική, αλλά όχι μεταβατική·

(β) αυτοπαθής και μεταβατική, αλλά όχι συμμετρική·

(γ) συμμετρική και μεταβατική, αλλά όχι αυτοπαθής.

Σε κάθε περίπτωση γράψτε τα ζεύγη της και σχεδιάστε το κατευθυνόμενο γράφημά της.

6. Τι είναι λάθος στο παρακάτω «επιχείρημα» ότι κάθε συμμετρική και μεταβατική σχέση είναι αυτοπαθής; «Έστω R συμμετρική και μεταβατική σχέση στο A. Αφού η R είναι συμμετρική, αν aRb τότε bRa. Αφού η R είναι μεταβατική, από τα aRb και bRa έπεται aRa. Αυτό ισχύει για κάθε a, άρα η R είναι αυτοπαθής.»

7. Αληθές ή ψευδές: για κάθε σχέση R σε ένα σύνολο A, η R^{-1} είναι συμμετρική αν και μόνο αν η R είναι συμμετρική. Αιτιολογήστε.

8. Έστω R και S σχέσεις σε ένα σύνολο A. Αληθές ή ψευδές; Αν κάποιο είναι ψευδές, δώστε αντιπαράδειγμα στο $A=\{1,2,3\}$.

(α) Αν οι R,S είναι συμμετρικές, τότε και η $R\cap S$ είναι συμμετρική.

(β) Αν οι R,S είναι συμμετρικές, τότε και η $R\cup S$ είναι συμμετρική.

(γ) Αν οι R,S είναι μεταβατικές, τότε και η $R\cup S$ είναι μεταβατική.

(δ) Αν οι R,S είναι αντισυμμετρικές, τότε και η $R\cup S$ είναι αντισυμμετρική.

9. Αποδείξτε ότι μια σχέση R στο A είναι μεταβατική αν και μόνο αν $R\circ R\subseteq R$.

10. Δείξτε ότι η $\equiv_5$ είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$ αν ($a\equiv_5 b \Leftrightarrow a-b=5k$, για κάποιο $k\in\mathbb{Z}$). Ποιες είναι οι κλάσεις ισοδυναμίας της;

11. Έστω $A=\{1,2,\dots,9\}$ και $\sim$ η σχέση στο $A\times A$ με $(a,b)\sim(c,d)$ αν και μόνο αν $a+d=b+c$.

(α) Αποδείξτε ότι η $\sim$ είναι σχέση ισοδυναμίας.

(β) Βρείτε την κλάση ισοδυναμίας $[(2,5)]$.

12. ⁻ Ποια από τα παρακάτω είναι διαμερίσεις του $S=\{1,2,3,4,5,6\}$; (α) $\{\{1,2,3\},\{1,4,5,6\}\}$· (β) $\{\{1,2\},\{3,5,6\}\}$· (γ) $\{\{1,3,5\},\{2,4\},\{6\}\}$· (δ) $\{\{1,3,5\},\{2,4,6,7\}\}$.

13. Βρείτε όλες τις διαμερίσεις του $\{1,2,3\}$. Πόσες σχέσεις ισοδυναμίας υπάρχουν στο $\{1,2,3\}$; Σχεδιάστε το κατευθυνόμενο γράφημα της καθεμίας.

14. Έστω $\mathbb{N}$ το σύνολο των φυσικών. Ορίζουμε τη σχέση $a\mid b \Leftrightarrow a$ διαιρεί το $b \Leftrightarrow$ υπάρχει $k\in\mathbb{N}$ με $b=ka$. Δείξτε ότι η παραπάνω σχέση είναι σχέση μερικής διάταξης στο $\mathbb{N}$. Είναι ολική διάταξη; γιατί; (Πρβλ. Παράδειγμα 1.44· εδώ προσέξτε ιδιαίτερα το 0.)

15. Ορίζουμε την σχέση $\lhd$ στο $\mathbb{N}\times\mathbb{N}$ ως εξής: $(\alpha,\beta)\lhd(\gamma,\delta)\Leftrightarrow \alpha<\gamma$ ή ($\alpha=\gamma$ και $\beta\le\delta$). Δείξτε ότι η $\lhd$ είναι μια σχέση μερικής διάταξης στο $\mathbb{N}\times\mathbb{N}$. Είναι ολική; (Η $\lhd$ λέγεται *λεξικογραφική διάταξη*: έτσι ακριβώς συγκρίνουμε λέξεις σε ένα λεξικό.)

16. Θεωρήστε το σύνολο X των θετικών διαιρετών του 36, με τη διαιρετότητα.

(α) Βρείτε το ελάχιστο και το μέγιστο στοιχείο του X.

(β) Βρείτε τα άνω και τα κάτω φράγματα του $E=\{4,6\}$.

(γ) Βρείτε τα ελάσσονα και τα μείζονα στοιχεία του $X\setminus\{1,36\}$. Έχει ελάχιστο ή μέγιστο στοιχείο;

17. ⋆ Έστω $(X, \preceq)$ ένα μερικά διατεταγμένο σύνολο.

(α) Δείξτε ότι αν το X είναι πεπερασμένο και έχει *ακριβώς ένα* ελάσσον στοιχείο, τότε αυτό είναι το ελάχιστο στοιχείο του. (Υπόδειξη: για τυχόν x, εφαρμόστε το Θεώρημα 1.47 στο σύνολο $\{y \in X : y \preceq x\}$.)

(β) Δείξτε με παράδειγμα ότι αυτό δεν ισχύει αν το X είναι άπειρο.

1.3 Συναρτήσεις

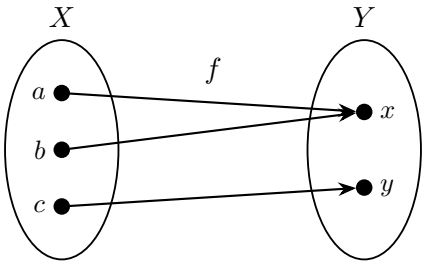
Έστω $\mathcal{S}$ το σύνολο των φοιτητών του τρίτου έτους ενός τμήματος και $\mathcal{C}$ το σύνολο των μαθημάτων του τρίτου έτους. Η σχέση «ο φοιτητής s παρακολουθεί το μάθημα c» είναι μια σχέση από το $\mathcal{S}$ στο $\mathcal{C}$, και ένας φοιτητής μπορεί να παρακολουθεί *πολλά* μαθήματα. Ας υποθέσουμε όμως ότι κάθε φοιτητής πρέπει να πάρει *ακριβώς ένα* μάθημα κορμού από μια σχετική λίστα. Τότε η σχέση «ο φοιτητής s παρακολουθεί το μάθημα κορμού c» έχει μια πολύ ειδική ιδιότητα: *κάθε* στοιχείο του πρώτου συνόλου σχετίζεται με *ακριβώς ένα* στοιχείο του δεύτερου. Αυτή η ιδιότητα ορίζει μία από τις σημαντικότερες έννοιες των μαθηματικών, τη *συνάρτηση*.

1.3.1 Ορισμός, εικόνα και αντίστροφη εικόνα

Ορισμός 1.48 (Συνάρτηση). Έστω X και Y σύνολα. Μια *συνάρτηση* από το X στο Y είναι μια σχέση f τέτοια ώστε το πεδίο ορισμού της είναι το X και για κάθε $x \in X$ υπάρχει ένα και μόνο ένα $y \in Y$ με $(x, y) \in f$. Δηλαδή μια συνάρτηση f από το X στο Y είναι ένα $f \subseteq X \times Y$ με πεδίο ορισμού το X, τέτοιο ώστε αν $(x, y) \in f$ και $(x, z) \in f$ τότε $y = z$. Συνήθως το μοναδικό y που αντιστοιχεί στο $x \in X$ με $(x, y) \in f$ συμβολίζεται $f(x)$. Αντί λοιπόν να γράφουμε $(x, y) \in f$ ή xfy για την συνάρτηση f, γράφουμε $y = f(x)$. Το στοιχείο y λέγεται *τιμή* της f στο x. Τη φράση «η f είναι μια συνάρτηση από το X στο Y» τη συμβολίζουμε με $f : X \to Y$.

Με λίγα λόγια: κάθε $x \in X$ «στέλνεται» *κάπου* στο Y (ύπαρξη) και *πουθενά αλλού* (μοναδικότητα).

Παράδειγμα 1.49. Έστω $X = \{a, b, c\}$ και $Y = \{x, y\}$.



Σχήμα 1.7. Η συνάρτηση $f : X \to Y$ του Παραδείγματος 1.49.

Η σχέση $f = \{(a, x), (b, x), (c, y)\} \subseteq X \times Y$ είναι μια συνάρτηση από το X στο Y. Έχουμε $f : X \to Y$ και

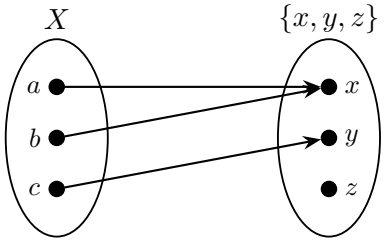
$$(a, x) \in f \Leftrightarrow f(a) = x$$
$$(b, x) \in f \Leftrightarrow f(b) = x$$
$$(c, y) \in f \Leftrightarrow f(c) = y.$$

Στο διάγραμμα βελών του Σχήματος 1.7 κάθε στοιχείο του X έχει *ακριβώς ένα* εξερχόμενο βέλος· αυτό είναι ακριβώς το «κριτήριο» για να είναι μια σχέση από το X στο Y συνάρτηση. Αντίθετα, η

σχέση $\{(a,x),(a,y),(b,x),(c,y)\}$ δεν είναι συνάρτηση (το a έχει δύο εικόνες), ούτε η $\{(a,x),(c,y)\}$ (το b δεν έχει εικόνα).

Το σύνολο όλων των συναρτήσεων από το X στο Y είναι υποσύνολο του δυναμοσυνόλου $\mathcal{P}(X\times Y)$ και συμβολίζεται με Y^X. Έστω $f : X \to Y$ μια συνάρτηση, το σύνολο $\{(x,y) : y = f(x)\} \subseteq X \times Y$ λέγεται *γράφημα* της f. Το πεδίο ορισμού της $f : X \to Y$ είναι το σύνολο $\{x \in X : f(x) = y \text{ για κάποιο } y \in Y\} = X$, ενώ το *πεδίο τιμών* της είναι το σύνολο $\{y \in Y : f(x) = y \text{ για κάποιο } x \in X\} \subseteq Y$.

Το σύνολο Y λέγεται *πεδίο άφιξης* (ή *σύνολο-στόχος*) της $f : X \to Y$. Το πεδίο τιμών *δεν* χρειάζεται να είναι όλο το πεδίο άφιξης. Στο Παράδειγμα 1.49 το πεδίο τιμών ήταν το $\{x,y\} = Y$, αλλά αν θεωρήσουμε την ίδια αντιστοίχιση ως συνάρτηση $f : X \to \{x,y,z\}$ (Σχήμα 1.8), το πεδίο άφιξης είναι το $\{x,y,z\}$, ενώ το πεδίο τιμών παραμένει $\{x,y\}$.



Σχήμα 1.8. Μια συνάρτηση της οποίας το πεδίο τιμών, $\{x,y\}$, είναι γνήσιο υποσύνολο του πεδίου άφιξης, $\{x,y,z\}$.

Αν $A \subseteq X$, τότε το σύνολο $\{y \in Y : \text{υπάρχει } x \in A,\ f(x) = y\} \subseteq Y$ λέγεται *εικόνα* του A μέσω της f και συμβολίζεται με $f(A)$. Αν $f : X \to Y$ τότε $f(X) =$ πεδίο τιμών της.

Δοσμένης μιας συνάρτησης $f : X \to Y$ και $B \subseteq Y$ τότε ορίζουμε το σύνολο $f^{-1}(B) = \{x \in X : f(x) \in B\}$ και το λέμε *αντίστροφη εικόνα* του B μέσω της f. Το $f^{-1}(B)$ αποτελείται από εκείνα τα στοιχεία του X που η f απεικονίζει στο B.

Παράδειγμα 1.50. Έστω $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = x^2$. Τότε $f(\{-2,-1,1\}) = \{1,4\}$ (τα -1 και 1 έχουν την ίδια εικόνα), $f(\mathbb{R}) = [0,\infty)$, $f^{-1}(\{4,9\}) = \{-3,-2,2,3\}$ και $f^{-1}(\{-1\}) = \emptyset$.

Παρατήρηση 1.51. Η αντίστροφη εικόνα ορίζεται για *κάθε* συνάρτηση $f : X \to Y$ και για κάθε $B \subseteq Y$· η f δεν χρειάζεται να έχει κάποια ειδική ιδιότητα. Δεν πρέπει όμως να τη συγχέουμε με την *αντίστροφη συνάρτηση* που θα ορίσουμε παρακάτω: η αντιστοίχιση $B \mapsto f^{-1}(B)$ δεν είναι συνάρτηση από το Y στο X, αλλά συνάρτηση από το $\mathcal{P}(Y)$ στο $\mathcal{P}(X)$.

Πρόταση 1.52. *Για κάθε συνάρτηση $f : X \to Y$ και για κάθε $A, B \subseteq X$ ισχύει $f(A \cup B) = f(A) \cup f(B)$.*

Απόδειξη. ($\subseteq$) Έστω $y \in f(A \cup B)$. Τότε υπάρχει $x \in A \cup B$ με $f(x) = y$. Αν $x \in A$, τότε $y \in f(A)$· αν $x \in B$, τότε $y \in f(B)$. Σε κάθε περίπτωση $y \in f(A) \cup f(B)$.

($\supseteq$) Έστω $y \in f(A) \cup f(B)$. Αν $y \in f(A)$, τότε υπάρχει $x \in A \subseteq A \cup B$ με $f(x) = y$, άρα $y \in f(A \cup B)$. Όμοια αν $y \in f(B)$. □

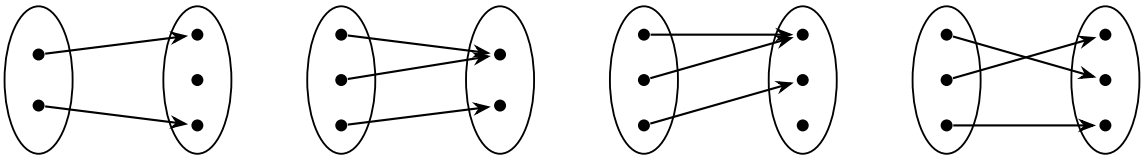
Για την τομή ισχύει μόνο ο εγκλεισμός $f(A \cap B) \subseteq f(A) \cap f(B)$, και όχι πάντα ισότητα (Άσκηση 2).

1.3.2 Ενριπτικές, επιρριπτικές και αμφιμονοσήμαντες συναρτήσεις

Ορισμός 1.53 (Ενριπτική συνάρτηση). Μια συνάρτηση $f : X \to Y$ λέγεται *ενριπτική* (ή *ένα-προς-ένα*, ή 1-1) αν $(x_1, y) \in f$ και $(x_2, y) \in f$ (ή $f(x_1) = f(x_2)$) $\Rightarrow x_1 = x_2$. Δηλαδή μια συνάρτηση λέγεται ενριπτική αν αντιστοιχεί διαφορετικά στοιχεία του πεδίου ορισμού σε διαφορετικές εικόνες στο πεδίο τιμών της.

Ορισμός 1.54 (Επιρριπτική, αμφιμονοσήμαντη συνάρτηση). Μια συνάρτηση $f : X \to Y$ λέγεται *επιρριπτική* (ή *επί*) αν το πεδίο τιμών της είναι όλο το Y ($f(X) = Y$), δηλαδή αν κάθε $y \in Y$ είναι εικόνα *κάποιου* $x \in X$. Λέγεται *αμφιμονοσήμαντη* (ή *αμφιρριπτική*, ή *ένα-προς-ένα και επί*) αν είναι *και* ενριπτική *και* επιρριπτική.

Στο διάγραμμα βελών μιας συνάρτησης $f : X \to Y$ (Σχήμα 1.9): η f είναι ενριπτική αν και μόνο αν κάθε στοιχείο του Y έχει *το πολύ ένα* εισερχόμενο βέλος· επιρριπτική αν και μόνο αν κάθε στοιχείο του Y έχει *τουλάχιστον ένα* εισερχόμενο βέλος· και αμφιμονοσήμαντη αν και μόνο αν κάθε στοιχείο του Y έχει *ακριβώς ένα* εισερχόμενο βέλος. Μια αμφιμονοσήμαντη συνάρτηση «ταιριάζει» τέλεια τα στοιχεία των δύο συνόλων. Γι' αυτό είναι το βασικό εργαλείο όταν θέλουμε να συγκρίνουμε τα «μεγέθη» συνόλων, ακόμη και άπειρων (Κεφάλαιο 2).



(α) ενριπτική, όχι επί (β) επί, όχι ενριπτική (γ) ούτε ενριπτική ούτε επί (δ) αμφιμονοσήμαντη

Σχήμα 1.9. Διαγράμματα βελών τεσσάρων συναρτήσεων. Σε κάθε διάγραμμα, το αριστερό σύνολο είναι το πεδίο ορισμού και το δεξί το πεδίο άφιξης.

Παράδειγμα 1.55 (Μετρώντας συναρτήσεις). Έστω $A = \{a, b, c\}$ και $B = \{1, 2\}$. Πόσες συναρτήσεις $f : A \to B$ υπάρχουν; Πόσες από αυτές είναι ενριπτικές και πόσες επιρριπτικές;

Λύση. Μια συνάρτηση $f : A \to B$ καθορίζεται πλήρως αν επιλέξουμε τις εικόνες $f(a)$, $f(b)$ και $f(c)$. Για καθεμία υπάρχουν 2 επιλογές, ανεξάρτητα από τις άλλες, άρα (πολλαπλασιαστική αρχή) υπάρχουν $2 \cdot 2 \cdot 2 = 2^3 = 8$ συναρτήσεις. Καμία δεν είναι ενριπτική: θα χρειαζόμασταν τρεις *διαφορετικές* εικόνες σε ένα σύνολο με δύο μόνο στοιχεία. Επιρριπτικές είναι όλες εκτός από τις δύο σταθερές συναρτήσεις (αυτή που στέλνει τα πάντα στο 1 και αυτή που στέλνει τα πάντα στο 2), δηλαδή $8 - 2 = 6$. ◊

Με τον ίδιο συλλογισμό, αν $|A| = m$ και $|B| = n$, υπάρχουν n^m συναρτήσεις $f : A \to B$, δηλαδή $|B^A| = |B|^{|A|}$ (αυτό εξηγεί και τον συμβολισμό Y^X). Το πόσες από αυτές είναι ενριπτικές ή επιρριπτικές θα το μετρήσουμε στα Κεφάλαια ?? και ??.

Η ικανή και αναγκαία συνθήκη για να είναι η $f : X \to Y$ επί είναι η αντίστροφη εικόνα μέσω της f κάθε μη κενού υποσυνόλου του Y να είναι μη κενό υποσύνολο του X. Η ικανή και αναγκαία συνθήκη για να είναι η f ενριπτική είναι η αντίστροφη εικόνα μέσω της f κάθε συνόλου $\{y\} \subseteq Y$, με y στοιχείο του πεδίου τιμών της f, να είναι μονοσύνολο, δηλαδή $\{x\} \subseteq X$ για κάποιο $x \in X$.

Αν η τελευταία συνθήκη ικανοποιείται τότε το σύμβολο f^{-1} χρησιμοποιείται για την παρακάτω συνάρτηση: f^{-1} : (πεδίο τιμών της f) $\to X$ με $f^{-1}(y) = x$ αν $f(x) = y$, δηλαδή η τιμή της f^{-1} για κάθε $y \in$ (πεδίο τιμών της f) είναι το μοναδικό $x \in X$ για το οποίο $f(x) = y$. Με άλλα λόγια αν η $f : X \to Y$ είναι ενριπτική τότε $f^{-1}(y) = x \Leftrightarrow f(x) = y$ για κάθε y στο πεδίο τιμών της f. Επίσης

αν η $f : X \to Y$ είναι αμφιμονοσήμαντη, τότε η f^{-1} ορίζεται για κάθε $y \in Y$, $f^{-1} : Y \to X$ και $f(f^{-1}(y)) = y$ για κάθε $y \in Y$. Η f^{-1} λέγεται τότε *αντίστροφη συνάρτηση* της f.

Συνοψίζοντας: αν η $f : X \to Y$ είναι αμφιμονοσήμαντη, η αντίστροφη συνάρτηση $f^{-1} : Y \to X$ ορίζεται από την ισοδυναμία

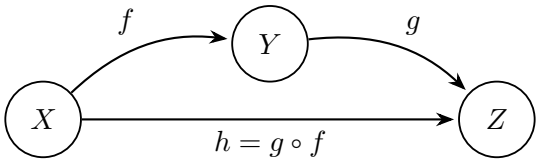
$$f^{-1}(y) = x \iff f(x) = y,$$

και ισχύουν $f(f^{-1}(y)) = y$ για κάθε $y \in Y$ και $f^{-1}(f(x)) = x$ για κάθε $x \in X$. Για να ορίζεται η f^{-1} σε όλο το Y χρειαζόμαστε και την ύπαρξη (η f να είναι επί) και τη μοναδικότητα (η f να είναι ενριπτική) ενός x με $f(x) = y$, για κάθε $y \in Y$. Ο συμβολισμός f^{-1} χρησιμοποιείται λοιπόν με δύο διαφορετικές σημασίες: όταν η f είναι αμφιμονοσήμαντη, το $f^{-1}(y)$ είναι ένα *στοιχείο* του X, ενώ το $f^{-1}(\{y\})$ είναι το *σύνολο* $\{f^{-1}(y)\}$· το $f^{-1}(\{y\})$ όμως ορίζεται για κάθε συνάρτηση f.

Παράδειγμα 1.56. Η $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = 2x + 1$ είναι αμφιμονοσήμαντη: για κάθε $y \in \mathbb{R}$ η εξίσωση $2x + 1 = y$ έχει ακριβώς μία λύση, την $x = (y - 1)/2$. Άρα $f^{-1}(y) = (y - 1)/2$. Αντίθετα, η $g : \mathbb{R} \to \mathbb{R}$ με $g(x) = x^2$ δεν έχει αντίστροφη συνάρτηση: δεν είναι ενριπτική ($g(-1) = g(1)$) ούτε επί (το -1 δεν είναι εικόνα κανενός αριθμού).

1.3.3 Σύνθεση συναρτήσεων

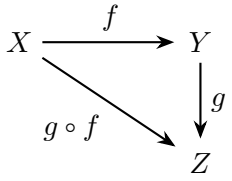
Ορισμός 1.57 (Σύνθεση συναρτήσεων). Έστω τώρα $f : X \to Y$ και $g : Y \to Z$. Κάθε στοιχείο στο πεδίο τιμών της f ανήκει στο πεδίο ορισμού της g και επομένως έχει νόημα το $g(f(x))$ για κάθε $x \in X$. Η συνάρτηση $h : X \to Z$ που ορίζεται με $h(x) = g(f(x))$ καλείται *σύνθεση* των συναρτήσεων f και g και συμβολίζεται με $g \circ f$ (βλέπε Σχήματα 1.10 και 1.11).



Σχήμα 1.10. Η σύνθεση $g \circ f$ των συναρτήσεων f και g.

Προσέξτε τη σειρά: πρώτα εφαρμόζουμε την f και μετά την g, αλλά γράφουμε $g \circ f$, όπως και στον Απειροστικό Λογισμό. Για παράδειγμα, αν $f, g : \mathbb{R} \to \mathbb{R}$ με $f(x) = x + 1$ και $g(x) = x^2$, τότε $(g \circ f)(x) = (x + 1)^2$, ενώ $(f \circ g)(x) = x^2 + 1$· άρα $g \circ f \neq f \circ g$.

Παρατηρούμε ότι η σειρά είναι σπουδαία στη σύνθεση συναρτήσεων. Για να ορισθεί η $g \circ f$ πρέπει το πεδίο τιμών της f να περιέχεται στο πεδίο ορισμού της g, ενώ για να ορισθεί η $f \circ g$ πρέπει το πεδίο τιμών της g να περιέχεται στο πεδίο ορισμού της f.



Σχήμα 1.11. Μεταθετικό διάγραμμα της σύνθεσης $g \circ f$.

Αλλά ακόμα και στην περίπτωση που και οι δύο συνθέσεις $f \circ g$ και $g \circ f$ ορίζονται μπορεί να μην είναι οι ίδιες συναρτήσεις. Με άλλα λόγια η σύνθεση συναρτήσεων δεν είναι αναγκαστικά μεταθετική. Παρόλα αυτά όμως είναι προσεταιριστική. Γιατί αν $f : X \to Y$ και $g : Y \to Z$ και

$h : Z \to W$ τότε για $x \in X$ έχουμε

$$[h \circ (g \circ f)](x) = h[(g \circ f)(x)] = h(g(f(x))) = (h \circ g)(f(x)) = [(h \circ g) \circ f](x).$$

Δηλαδή $h \circ (g \circ f) = (h \circ g) \circ f$.

Η σύνθεση «διατηρεί» τις ιδιότητες που ορίσαμε στην προηγούμενη υποενότητα.

Πρόταση 1.58. *Αν οι $f : X \to Y$ και $g : Y \to Z$ είναι ενριπτικές, τότε και η $g \circ f : X \to Z$ είναι ενριπτική.*

Απόδειξη. Έστω $x_1, x_2 \in X$ με $(g \circ f)(x_1) = (g \circ f)(x_2)$, δηλαδή $g(f(x_1)) = g(f(x_2))$. Αφού η g είναι ενριπτική, έπεται $f(x_1) = f(x_2)$. Αφού η f είναι ενριπτική, έπεται $x_1 = x_2$. Άρα η $g \circ f$ είναι ενριπτική. □

Με παρόμοιο τρόπο αποδεικνύεται ότι η σύνθεση δύο επιρριπτικών συναρτήσεων είναι επιρριπτική (Άσκηση 14), και επομένως η σύνθεση δύο αμφιμονοσήμαντων συναρτήσεων είναι αμφιμονοσήμαντη.

Αν έχουμε δύο αμφιμονοσήμαντες συναρτήσεις $f : X \to Y$ και $g : Y \to Z$ τότε όπως ξέρουμε ορίζονται και οι αντίστροφες $f^{-1} : Y \to X$ και $g^{-1} : Z \to Y$ που είναι και αυτές αμφιμονοσήμαντες, και, όπως είδαμε, η σύνθεση $g \circ f : X \to Z$ είναι επίσης αμφιμονοσήμαντη. Οι ισοδυναμίες

$$\begin{aligned}(g \circ f)(x) = z &\Leftrightarrow g(f(x)) = z \\ &\Leftrightarrow f(x) = g^{-1}(z) \\ &\Leftrightarrow x = f^{-1}(g^{-1}(z))\end{aligned}$$

ισχύουν για κάθε $x \in X$ και $z \in Z$, και μας δείχνουν ότι $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Η σειρά στον τύπο $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ είναι λογική: για να «αναιρέσουμε» την f ακολουθούμενη από την g, αναιρούμε πρώτα το *τελευταίο* βήμα (με την g^{-1}) και μετά το πρώτο (με την f^{-1}), όπως όταν βγάζουμε πρώτα τα παπούτσια και μετά τις κάλτσες, με την αντίστροφη σειρά από αυτή που τα φορέσαμε.

1.3.4 Μερικές ειδικές συναρτήσεις

Η συνάρτηση j που ορίζεται από την $j(x) = x$, για κάθε $x \in X$ (όπου $X \subseteq Y$) λέγεται η *συνάρτηση εγκλεισμού* του X στο Y. Η συνάρτηση εγκλεισμού από το X στο X λέγεται η *ταυτοτική απεικόνιση* του X. Έστω τώρα $f : Y \to Z$ και $X \subseteq Y$ τότε κατασκευάζουμε τη συνάρτηση $g : X \to Z$ τέτοια ώστε $g(x) = f(x)$, για κάθε $x \in X$. Η συνάρτηση g λέγεται ο *περιορισμός* της f στο X, και η f λέγεται μια *επέκταση* της g στο Y. Συνήθως γράφουμε $g = f|X$.

Την ταυτοτική απεικόνιση του X τη συμβολίζουμε id_X· είναι αμφιμονοσήμαντη και ισχύουν $f \circ \mathrm{id}_X = f$ και $\mathrm{id}_Y \circ f = f$ για κάθε $f : X \to Y$. Επίσης, αν η $f : X \to Y$ είναι αμφιμονοσήμαντη, τότε $f^{-1} \circ f = \mathrm{id}_X$ και $f \circ f^{-1} = \mathrm{id}_Y$. Ο περιορισμός $f|X$ συμβολίζεται και $f|_X$: είναι «η ίδια συνάρτηση, με μικρότερο πεδίο ορισμού». Για παράδειγμα, η $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = x^2$ δεν είναι ενριπτική, αλλά ο περιορισμός της $f|_{[0,\infty)}$ είναι (Άσκηση 9).

Έστω X, Y σύνολα. Ορίζουμε μια συνάρτηση $\pi_1 : X \times Y \to X$ με $\pi_1(x, y) = x$. Η συνάρτηση π_1 λέγεται *προβολή* από το $X \times Y$ στο X, ενώ η $\pi_2 : X \times Y \to Y$ με $\pi_2(x, y) = y$ λέγεται η προβολή από το $X \times Y$ στο Y.

Ορισμός 1.59 (Χαρακτηριστική συνάρτηση). Αν $A \subseteq X$, η *χαρακτηριστική συνάρτηση* του A είναι η συνάρτηση $\chi_A : X \to \{0, 1\}$ τέτοια ώστε

$$\chi_A(x) = \begin{cases} 1 & \text{αν } x \in A \\ 0 & \text{αν } x \notin A. \end{cases}$$

Για παράδειγμα, αν $X = \{1,2,3,4\}$ και $A = \{1,3\}$, τότε $\chi_A(1) = \chi_A(3) = 1$ και $\chi_A(2) = \chi_A(4) = 0$. Κάθε υποσύνολο $A \subseteq X$ αντιστοιχεί λοιπόν σε μια συνάρτηση $\chi_A : X \to \{0,1\}$· και αντίστροφα, κάθε συνάρτηση $h : X \to \{0,1\}$ είναι η χαρακτηριστική συνάρτηση ενός υποσυνόλου, του $h^{-1}(\{1\})$. Αν $X = \{a_1, \dots, a_n\}$, η χ_A δεν είναι παρά η ακολουθία δυαδικών ψηφίων $\chi_A(a_1)\chi_A(a_2)\cdots\chi_A(a_n)$ που χρησιμοποιήσαμε στην απόδειξη της Πρότασης 1.21 (βλ. και Άσκηση 17).

Ασκήσεις

1. Ποιες σχέσεις είναι συναρτήσεις;

(α) Έστω $A = \{4,5,6\}$, $B = \{5,6,7\}$ και οι σχέσεις από το A στο B: $R = \{(x,y) \in A \times B : x \geq y\}$, $S = \{(x,y) \in A \times B : \text{ο } x - y \text{ είναι άρτιος}\}$ και $T = \{(4,7),(6,5),(6,7)\}$. Σχεδιάστε τα διαγράμματα βελών τους. Ποιες είναι συναρτήσεις από το A στο B; Για όσες δεν είναι, ποια απαίτηση του ορισμού (ύπαρξη ή μοναδικότητα της εικόνας) παραβιάζεται;

(β) Είναι η $\{(x,y) \in (0,\infty) \times \mathbb{R} : x = y^2\}$ συνάρτηση από το $(0,\infty)$ στο $\mathbb{R}$; Η $\{(x,y) \in (0,\infty) \times (0,\infty) : x = y^2\}$ από το $(0,\infty)$ στο $(0,\infty)$;

(γ) Πόσες σχέσεις υπάρχουν από το $\{a,b\}$ στο $\{x,y\}$; Πόσες από αυτές είναι συναρτήσεις;

(δ) Έστω $f : X \to Y$ συνάρτηση και $f^{-1} = \{(y,x) : (x,y) \in f\}$ η αντίστροφη *σχέση* της (Ορισμός 1.26). Δείξτε ότι η f^{-1} είναι συνάρτηση από το Y στο X αν και μόνο αν η f είναι αμφιμονοσήμαντη.

2. Δείξτε ότι για $A \subseteq X, B \subseteq X$ και $f : X \to Y$,

i) $f(A \cup B) = f(A) \cup f(B)$

ii) $f(A \cap B) \subseteq f(A) \cap f(B)$

(Το i) αποδείχθηκε στην Πρόταση 1.52.) Βρείτε ένα παράδειγμα όπου η ισότητα στο ii) *δεν* ισχύει. Δείξτε ότι αν η f είναι ενριπτική, τότε στο ii) ισχύει ισότητα.

3. Δείξτε ότι για $A \subseteq Y, B \subseteq Y$ και $f : X \to Y$,

i) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$

ii) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$

4. Έστω $f : A \to B$, και $R = \{(a,b) : f(a) = f(b)\} \subseteq A \times A$. Δείξτε ότι η R είναι μια σχέση ισοδυναμίας στο A.

5. – Έστω $f : \mathbb{R} \to \mathbb{R}$, $g : [0,\infty) \to \mathbb{R}$ με $f(x) = x^2 + 1$ και $g(x) = \sqrt{x}$. Βρείτε τη σύνθεση $g \circ f$. Ορίζεται η $f \circ g$; Αν ναι, βρείτε την.

6. Έστω $f, g : \mathbb{R} \to \mathbb{R}$ με $f(x) = x^3$ και $g(x) = x - 1$.

(α) Βρείτε τις $g \circ f$ και $f \circ g$. Είναι ίσες; Για ποια x ισχύει $(g \circ f)(x) = (f \circ g)(x)$;

(β) Δείξτε ότι οι f και g είναι αμφιμονοσήμαντες, και βρείτε τις f^{-1}, g^{-1} και $(g \circ f)^{-1}$. Επαληθεύστε ότι $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$, ενώ $(g \circ f)^{-1} \neq g^{-1} \circ f^{-1}$.

7. – Έστω $A = \{a,b\}$ και $B = \{1,2,3\}$.

(α) Γράψτε όλες τις συναρτήσεις $f : A \to B$, χρησιμοποιώντας τον *συμβολισμό δύο γραμμών* $\left(\begin{smallmatrix} a & b \\ f(a) & f(b) \end{smallmatrix}\right)$. Πόσες είναι;

(β) Πόσες από αυτές είναι ενριπτικές; Πόσες επιρριπτικές;

8. Πόσες συναρτήσεις $f : A \to B$ υπάρχουν αν $|A| = 5$ και $|B| = 7$; Πόσες από αυτές είναι ενριπτικές; Πόσες επιρριπτικές; Εξηγήστε.

9. ⁻ Δείξτε ότι η $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = x^2$ δεν είναι ενριπτική, αλλά ο περιορισμός της $f|_{[0,\infty)}$ είναι. Είναι η $f|_{[0,\infty)} : [0,\infty) \to \mathbb{R}$ επί; Απαντήστε στα ίδια ερωτήματα για την $h(x) = |x|$, και δείξτε ότι η $r : [0,\infty) \to \mathbb{R}$ με $r(x) = \sqrt{x}$ είναι ενριπτική αλλά όχι επί.

10. ⁻ Οι παρακάτω συναρτήσεις έχουν πεδίο ορισμού και πεδίο άφιξης το $\{1,2,3,4,5\}$. Για καθεμία, βρείτε αν είναι ενριπτική, επιρριπτική, αμφιμονοσήμαντη ή τίποτα από αυτά. (Για τα ερωτήματα (β) και (γ) χρησιμοποιούμε τον *συμβολισμό δύο γραμμών* $\left(\begin{smallmatrix} a & b & \cdots \\ f(a) & f(b) & \cdots \end{smallmatrix}\right)$ που είδαμε και στην Άσκηση 7.)

$$\text{(α) } f(x) = \begin{cases} x+2 & \text{αν } x < 4 \\ x & \text{αν } x \geq 4 \end{cases} \qquad \text{(β) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 3 & 1 & 3 & 1 \end{pmatrix} \qquad \text{(γ) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Είναι δυνατόν μια συνάρτηση από το $\{1,2,3,4,5\}$ στον εαυτό του να είναι ενριπτική αλλά όχι επί;

11. Για καθεμία από τις παρακάτω συναρτήσεις βρείτε αν είναι ενριπτική και αν είναι επιρριπτική: (α) $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n + 4$· (β) $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n + 4$· (γ) $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 5n - 8$· (δ) $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n/2$ αν ο n είναι άρτιος και $f(n) = (n+1)/2$ αν ο n είναι περιττός.

12. Έστω $A = \{1, 2, \dots, 10\}$ και $f : \mathcal{P}(A) \to \mathbb{N}$ με $f(B) = |B|$.

(α) Είναι η f ενριπτική; Είναι επιρριπτική;

(β) Βρείτε τα $f^{-1}(\{1\})$, $f^{-1}(\{0\})$ και $f^{-1}(\{12\})$.

13. Έστω $f : X \to Y$ μια συνάρτηση. Ποια από τα παρακάτω είναι δυνατά; Εξηγήστε.

(α) Η f είναι ενριπτική αλλά όχι επιρριπτική.

(β) Η f είναι επιρριπτική αλλά όχι ενριπτική.

(γ) Τα X, Y είναι πεπερασμένα με $|X| = |Y|$, και η f είναι ενριπτική αλλά όχι επιρριπτική.

(δ) Τα X, Y είναι πεπερασμένα με $|X| = |Y|$, και η f είναι επιρριπτική αλλά όχι ενριπτική.

14. Έστω $f : X \to Y$ και $g : Y \to Z$.

(α) Αποδείξτε ότι αν οι f και g είναι επιρριπτικές, τότε και η $g \circ f$ είναι επιρριπτική.

(β) ⋆ Αν η $g \circ f$ είναι ενριπτική, τι μπορείτε να πείτε για τις f και g; Αν η $g \circ f$ είναι επιρριπτική;

15. Έστω $f : A \to B$ και $g : B \to A$ με $g \circ f = \mathrm{id}_A$. Αποδείξτε ότι η f είναι ενριπτική και η g επιρριπτική. Αν επιπλέον $f \circ g = \mathrm{id}_B$, δείξτε ότι η f είναι αμφιμονοσήμαντη και $g = f^{-1}$.

16. ⋆ Έστω $f : X \to Y$, $A \subseteq X$ και $B \subseteq Y$.

(α) Ισχύει πάντα $f^{-1}(f(A)) = A$; Δείξτε ότι πάντα $A \subseteq f^{-1}(f(A))$, και ότι ισχύει ισότητα για κάθε A όταν η f είναι ενριπτική.

(β) Ισχύει πάντα $f(f^{-1}(B)) = B$; Δείξτε ότι πάντα $f(f^{-1}(B)) \subseteq B$, και ότι ισχύει ισότητα για κάθε B όταν η f είναι επιρριπτική.

17. Έστω X ένα σύνολο. Αποδείξτε ότι η συνάρτηση $\Phi : \mathcal{P}(X) \to \{0,1\}^X$ με $\Phi(A) = \chi_A$ είναι αμφιμονοσήμαντη. Αποδείξτε επίσης ότι $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$ και $\chi_{A'}(x) = 1 - \chi_A(x)$ για κάθε $x \in X$ (με $A' = X \setminus A$).

Κεφάλαιο 2

Φυσικοί αριθμοί, επαγωγή και ισοδύναμα σύνολα

2.1 Φυσικοί Αριθμοί. Αρχή της Επαγωγής

Έχουμε γραμματόσημα των 5 και των 8 λεπτών, απεριόριστο πλήθος από το καθένα. Ποια ποσά μπορούμε να πληρώσουμε *ακριβώς*; Με γραμματόσημα των 5 πληρώνουμε τα $5, 10, 15, 20, \dots$, με γραμματόσημα των 8 τα $8, 16, 24, \dots$, και με συνδυασμούς ποσά όπως $5+8 = 13$ ή $5+5+8 = 18$. Αν δοκιμάσουμε ένα-ένα τα ποσά, βρίσκουμε ότι τα μόνα θετικά ποσά που *δεν* μπορούμε να πληρώσουμε είναι τα

$$1, 2, 3, 4, 6, 7, 9, 11, 12, 14, 17, 19, 22, 27.$$

Φαίνεται λοιπόν ότι *κάθε* ποσό $n \geq 28$ μπορεί να πληρωθεί ακριβώς. Πώς όμως θα αποδείξουμε έναν ισχυρισμό για *άπειρα* το πλήθος ποσά, αφού δεν μπορούμε να τα ελέγξουμε ένα-ένα; Το βασικό εργαλείο για τέτοιους ισχυρισμούς είναι η *αρχή της επαγωγής*, το θέμα αυτής της ενότητας. Στο πρόβλημα των γραμματοσήμων θα επιστρέψουμε στην Πρόταση 2.12.

2.1.1 Η αρχή της καλής διάταξης και η αρχή της επαγωγής

Τους αριθμούς $0, 1, 2, \dots$ τους λέμε *φυσικούς*. Το σύνολο των φυσικών το συμβολίζουμε με $\mathbb{N}$. Αυτό έχει την εξής ιδιότητα: αν $n \in \mathbb{N}$, τότε και $n+1 \in \mathbb{N}$. Θα δεχθούμε σαν αξίωμα την παρακάτω, διαισθητικά προφανή ιδιότητα των φυσικών αριθμών:

Αξίωμα 2.1 (Αρχή της καλής διάταξης). *Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο. Δηλαδή για κάθε $X \subseteq \mathbb{N}$, $X \neq \emptyset$ υπάρχει $n \in X$ τέτοιο ώστε για κάθε $m \in X$ ισχύει $n \leq m$.*

Η ιδιότητα αυτή φαίνεται «προφανής», είναι όμως χαρακτηριστική του $\mathbb{N}$: *δεν* ισχύει, για παράδειγμα, στο $\mathbb{Z}$ (το ίδιο το $\mathbb{Z}$ δεν έχει ελάχιστο στοιχείο), ούτε στο σύνολο $\mathbb{Q}_+ = \{x \in \mathbb{Q} : x > 0\}$ των θετικών ρητών, που δεν έχει ελάχιστο στοιχείο, αφού για κάθε $x > 0$ είναι και $0 < x/2 < x$.

Με βάση την αρχή της καλής διάταξης αποδεικνύουμε την αρχή της επαγωγής, που είναι η σημαντικότερη αρχή που αφορά τους φυσικούς. Αυτή η αρχή έχει πολλές διατυπώσεις. Μια από αυτές είναι:

Θεώρημα 2.2 (Αρχή της επαγωγής). *Έστω $X \subseteq \mathbb{N}$ τέτοιο ώστε: (1) $0 \in X$, και (2) για κάθε φυσικό n, αν $n \in X$ τότε $(n+1) \in X$. Τότε το $X = \mathbb{N}$.*

Έστω ότι το $X \subseteq \mathbb{N}$ έχει τις ιδιότητες (1) και (2). Από την (1) βλέπουμε ότι $0 \in X$. Το (2) ισχύει για κάθε φυσικό άρα για τον 0 έχουμε $0 \in X \Rightarrow 1 \in X$. Άρα $1 \in X$. Συνεχίζοντας έτσι βλέπουμε ότι $2 \in X$, $3 \in X$ κ.ο.κ., άρα $X = \mathbb{N}$. Ας αποδείξουμε τώρα αυστηρά την αρχή της επαγωγής από την αρχή της καλής διάταξης.

Απόδειξη. Ας υποθέσουμε ότι $X \subseteq \mathbb{N}$ και ότι το X έχει τις ιδιότητες (1) και (2). Ας υποθέσουμε ότι $X \neq \mathbb{N}$, δηλαδή ότι υπάρχουν φυσικοί που δεν ανήκουν στο X. Αυτό σημαίνει ότι το συμπλήρωμα $\mathbb{N} \setminus X$ δεν είναι κενό. Άρα υπάρχει $n_0 \in \mathbb{N} \setminus X$ που είναι το ελάχιστο στοιχείο του $\mathbb{N} \setminus X$. Επειδή $0 \in X$ έχουμε $n_0 \neq 0$, άρα $n_0 = m+1$ για κάποιο $m \in \mathbb{N}$. Επειδή $m < n_0$ και ο n_0 είναι το ελάχιστο

στοιχείο του $\mathbb{N}\setminus X$, έχουμε $m \notin \mathbb{N}\setminus X$, άρα $m \in X$. Από την ιδιότητα (2) έχουμε όμως ότι $m+1 \in X$. Έπεται ότι $n_0 \in X$ και $n_0 \in \mathbb{N}\setminus X$, άτοπο. Άρα η υπόθεσή μας $X \neq \mathbb{N}$ μας οδήγησε σε άτοπο. □

Ισχύει όμως και το αντίστροφο: αν δεχτούμε την αρχή της επαγωγής, μπορούμε να αποδείξουμε ότι κάθε μη κενό υποσύνολο του $\mathbb{N}$ έχει ελάχιστο στοιχείο (την απόδειξη την παραλείπουμε). Οι δύο αρχές είναι λοιπόν ισοδύναμες, και αρκεί να δεχτούμε τη μία από τις δύο ως αξίωμα· εδώ, όπως και στις διαφάνειες του μαθήματος, δεχτήκαμε την αρχή της καλής διάταξης.

Μια άλλη διατύπωση της αρχής της επαγωγής είναι η ακόλουθη. Έστω P μια ιδιότητα των φυσικών τέτοια ώστε: (1) $P(0)$, δηλαδή ο 0 έχει την ιδιότητα P, και (2) για κάθε φυσικό n: αν $P(n)$ τότε $P(n+1)$, δηλαδή αν το n έχει την ιδιότητα P τότε και το $n+1$ έχει την ιδιότητα P. Τότε όλοι οι φυσικοί έχουν την ιδιότητα P. Μια απόδειξη που στηρίζεται σε αυτή τη διατύπωση της αρχής της επαγωγής λέγεται *επαγωγική απόδειξη*.

Οι δύο διατυπώσεις λένε το ίδιο πράγμα: αρκεί να εφαρμόσουμε το Θεώρημα 2.2 στο σύνολο $X = \{n \in \mathbb{N} : P(n)\}$ των φυσικών που έχουν την ιδιότητα P. Μια χρήσιμη εικόνα είναι μια άπειρη σειρά από ντόμινο: αν πέσει το πρώτο (η (1)) και κάθε ντόμινο που πέφτει ρίχνει το επόμενο (η (2)), τότε πέφτουν *όλα*.

2.1.2 Επαγωγικές αποδείξεις

Μια απόδειξη με επαγωγή ότι η $P(n)$ ισχύει για κάθε $n \geq n_0$ (συνήθως $n_0 = 0$ ή $n_0 = 1$) ακολουθεί πάντα την ίδια «συνταγή»:

1. **Βάση:** δείχνουμε ότι ισχύει η $P(n_0)$.
2. **Επαγωγική υπόθεση:** υποθέτουμε ότι η $P(k)$ ισχύει για *κάποιο* (αυθαίρετο, σταθερό) $k \geq n_0$.
3. **Επαγωγικό βήμα:** χρησιμοποιώντας την επαγωγική υπόθεση, δείχνουμε ότι ισχύει η $P(k+1)$.
4. **Συμπέρασμα:** από την αρχή της επαγωγής, η $P(n)$ ισχύει για κάθε $n \geq n_0$.

Παρατήρηση 2.3. Το σημαντικότερο (και συνήθως το δυσκολότερο) σημείο είναι το βήμα 3: εκεί *πρέπει* να χρησιμοποιήσουμε την επαγωγική υπόθεση. Αν αποδείξουμε την $P(k+1)$ χωρίς αυτήν, τότε απλώς αποδείξαμε την $P(n)$ απευθείας, χωρίς επαγωγή. Προσέξτε επίσης ότι στο βήμα 2 *δεν* υποθέτουμε ότι η $P(k)$ ισχύει για κάθε k (αυτό είναι ακριβώς που θέλουμε να αποδείξουμε), αλλά για ένα συγκεκριμένο k. Αυτό που αποδεικνύουμε στα βήματα 2–3 είναι η συνεπαγωγή «αν $P(k)$, τότε $P(k+1)$», για κάθε $k \geq n_0$.

Παράδειγμα 2.4 (Το άθροισμα $1+2+\cdots+n$). Θα δείξουμε ότι για κάθε $n \geq 1$

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Έστω $P(n)$ η πρόταση «$1+2+\cdots+n = n(n+1)/2$».

Βάση: Για $n=1$ το αριστερό μέλος είναι 1 και το δεξί $1\cdot 2/2 = 1$. Άρα ισχύει η $P(1)$.

Επαγωγική υπόθεση: Έστω ότι για κάποιο $k \geq 1$ ισχύει η $P(k)$, δηλαδή $1+2+\cdots+k = k(k+1)/2$.

Επαγωγικό βήμα: Θέλουμε να δείξουμε την $P(k+1)$, δηλαδή ότι $1+2+\cdots+k+(k+1) = (k+1)(k+2)/2$. Το άθροισμα των πρώτων k όρων είναι, από την επαγωγική υπόθεση, ίσο με $k(k+1)/2$. Άρα

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)\Big(\frac{k}{2}+1\Big) = \frac{(k+1)(k+2)}{2},$$

δηλαδή ισχύει η $P(k+1)$.

Συμπέρασμα: Από την αρχή της επαγωγής, η $P(n)$ ισχύει για κάθε $n \geq 1$.

Η επαγωγή μάς επιτρέπει να *επαληθεύσουμε* έναν τύπο, αλλά δεν μας λέει πώς να τον *βρούμε*. Για το παραπάνω άθροισμα υπάρχει ένα γνωστό τέχνασμα (που αποδίδεται στον Gauss): αν $S = 1 + 2 + \cdots + n$, γράφουμε το άθροισμα και με την αντίστροφη σειρά, $S = n + (n-1) + \cdots + 1$, και προσθέτουμε κατά στήλες. Κάθε στήλη δίνει $n+1$ και οι στήλες είναι n, άρα $2S = n(n+1)$.

Παράδειγμα 2.5. Θα δείξουμε ότι για κάθε $n \in \mathbb{N}$, $n < 2^n$. Έστω $P(n)$ η συνθήκη: $n < 2^n$. Προφανώς $P(0)$, γιατί $0 < 2^0 = 1$, αλλά και $P(1)$, γιατί $1 < 2^1 = 2$ (αυτό το τελευταίο θα είναι η βάση της επαγωγής μας). Για $n \geq 1$, ας υποθέσουμε την $P(n)$, δηλαδή $n < 2^n$. Τότε $2n < 2^{n+1}$ και επειδή $n + 1 \leq 2n$ (για $n \geq 1$) έχουμε

$$n + 1 \leq 2n < 2 \cdot 2^n = 2^{n+1}$$

άρα έχουμε την $P(n+1)$. Επομένως $n < 2^n$ για κάθε $n \in \mathbb{N}$.

Συχνά χρησιμοποιείται μια γενικευμένη μορφή της αρχής της επαγωγής. Όταν θέλουμε να αποδείξουμε ότι μια ιδιότητα P την έχουν όλοι οι φυσικοί $n \geq n_0$, όπου $n_0 \in \mathbb{N}$, αρκεί να αποδείξουμε ότι ο n_0 έχει την ιδιότητα P και ότι για κάθε $n \geq n_0$: «αν $P(n)$ τότε $P(n+1)$». Δηλαδή αν θέλουμε να δείξουμε ότι το σύνολο $X \subseteq \mathbb{N}$ περιέχει το $\{n \in \mathbb{N} : n \geq n_0\}$ τότε

1. Δείχνουμε ότι $n_0 \in X$, και ότι
2. για κάθε $n \geq n_0$, $n \in X \Rightarrow (n+1) \in X$.

Γιατί η επαγωγή «δουλεύει» και από μια βάση $n_0 \neq 0$; Επειδή η πρόταση «$P(n)$ για κάθε $n \geq n_0$» είναι ισοδύναμη με την πρόταση «$Q(\ell)$ για κάθε $\ell \in \mathbb{N}$», όπου $Q(\ell)$ είναι η $P(n_0 + \ell)$. Η βάση $P(n_0)$ είναι η $Q(0)$, και το βήμα «$P(k) \Rightarrow P(k+1)$ για κάθε $k \geq n_0$» είναι το βήμα «$Q(\ell) \Rightarrow Q(\ell+1)$ για κάθε $\ell \in \mathbb{N}$». Έτσι εφαρμόζουμε τη συνηθισμένη αρχή της επαγωγής στην Q.

Παράδειγμα 2.6. Για $n \geq 3$ ισχύει $2n + 1 < n^2$.

Πράγματι για $n = 3$ έχουμε $7 < 9$. Παρατηρούμε ότι

$$2(n+1) + 1 = 2n + 3 = (2n+1) + 2 < n^2 + 2 < n^2 + 2n + 1 = (n+1)^2,$$

δηλαδή ότι για κάθε φυσικό $n \geq 3$ αν $2n + 1 < n^2$ τότε $2(n+1) + 1 < (n+1)^2$. Μαζί με το $2 \cdot 3 + 1 < 3^2$, έχουμε ότι για κάθε φυσικό $n \geq 3$ ισχύει $2n + 1 < n^2$.

Παράδειγμα 2.7. Δείξτε ότι $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$, $n \geq 1$.

i) Το βασικό βήμα: Για $n = 1$ έχουμε $1^2 = \dfrac{1(1+1)(2+1)}{6}$.

ii) Το επαγωγικό βήμα: Έστω ότι για κάποιο $n \geq 1$ ισχύει $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$. Έχουμε ότι

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} = \frac{(n+1)(2n^2+7n+6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} = \frac{(n+1)[(n+1)+1][2(n+1)+1]}{6}. \end{aligned}$$

Άρα η πρόταση $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$ ισχύει για κάθε $n \geq 1$.

2.1.3 Ισχυρή επαγωγή

Η αρχή της επαγωγής μπορεί να διατυπωθεί με μία άλλη μορφή που είναι επίσης ισοδύναμη με την αρχή της καλής διάταξης (αν και φαίνεται πιο ισχυρή από την πρώτη διατύπωση).

Θεώρημα 2.8 (Αρχή της επαγωγής (2η μορφή), ή αρχή της ισχυρής επαγωγής). *Έστω $X \subseteq \mathbb{N}$ και ας υποθέσουμε ότι: (1) $0 \in X$, (2) για κάθε $n \in \mathbb{N}$: $\{0, 1, 2, \dots, n\} \subseteq X \Rightarrow (n+1) \in X$ (δηλαδή από το γεγονός ότι όλοι οι αριθμοί $\leq n$ ανήκουν στο X συνεπάγεται $n+1 \in X$). Τότε $X = \mathbb{N}$.*

Με ιδιότητες: αν (1) ισχύει η $P(0)$ και (2) για κάθε $k \in \mathbb{N}$, από το ότι ισχύουν *όλες* οι $P(0)$, $P(1)$, ..., $P(k)$ έπεται η $P(k+1)$, τότε η $P(n)$ ισχύει για κάθε $n \in \mathbb{N}$. Η διαφορά από την «απλή» επαγωγή είναι ότι στο επαγωγικό βήμα επιτρέπεται να χρησιμοποιήσουμε *όλες* τις προηγούμενες περιπτώσεις και όχι μόνο την αμέσως προηγούμενη. Παρά το όνομά της, η ισχυρή επαγωγή *δεν* αποδεικνύει περισσότερα από την απλή:

Πρόταση 2.9. *Η αρχή της ισχυρής επαγωγής (Θεώρημα 2.8) έπεται από την αρχή της επαγωγής (Θεώρημα 2.2), και αντίστροφα.*

Απόδειξη. Έστω ότι το $X \subseteq \mathbb{N}$ ικανοποιεί τις (1) και (2) του Θεωρήματος 2.8. Θεωρούμε το σύνολο

$$Y = \{n \in \mathbb{N} : \{0, 1, \dots, n\} \subseteq X\}$$

και δείχνουμε με (απλή) επαγωγή ότι $Y = \mathbb{N}$. Από την (1) έχουμε $\{0\} \subseteq X$, άρα $0 \in Y$. Αν $n \in Y$, δηλαδή $\{0, 1, \dots, n\} \subseteq X$, τότε από την (2) έχουμε $n+1 \in X$, άρα $\{0, 1, \dots, n+1\} \subseteq X$, δηλαδή $n+1 \in Y$. Από την αρχή της επαγωγής $Y = \mathbb{N}$. Ειδικά, για κάθε $n \in \mathbb{N}$ έχουμε $n \in Y$, άρα $n \in \{0, 1, \dots, n\} \subseteq X$. Επομένως $X = \mathbb{N}$.

Αντίστροφα, αν το X ικανοποιεί τις υποθέσεις της απλής επαγωγής, τότε ικανοποιεί και αυτές της ισχυρής: αν $\{0, 1, \dots, n\} \subseteq X$, τότε ειδικά $n \in X$, άρα $n+1 \in X$. Επομένως $X = \mathbb{N}$ από την ισχυρή επαγωγή. □

Η ισχυρή επαγωγή είναι απλώς πιο *βολική*, όταν για την $P(k+1)$ χρειαζόμαστε μία ή περισσότερες περιπτώσεις $P(j)$ με $j < k$, όπως στο επόμενο παράδειγμα.

Παράδειγμα 2.10. Θα δείξουμε ότι κάθε φυσικός n έχει την ιδιότητα: «αν $n \neq 0$, τότε είτε $n = 1$ είτε ο n έχει πρώτο διαιρέτη p». Έστω X το σύνολο όλων των φυσικών που ικανοποιούν την πιο πάνω πρόταση (ιδιότητα). Προφανώς $1 \in X$ (και $0 \in X$, αφού η ιδιότητα αφορά μόνο τους $n \neq 0$). Αρκεί λοιπόν να δείξουμε το επαγωγικό βήμα για $n \geq 1$. Ας υποθέσουμε ότι $n \geq 1$ και $\{0, 1, \dots, n\} \subseteq X$· τότε $n+1 \geq 2$. Αν ο αριθμός $n+1$ είναι πρώτος τότε $(n+1) \in X$. Αν ο $n+1$ δεν είναι πρώτος τότε γράφεται σαν γινόμενο $n+1 = m \cdot k$ όπου $1 < k < n+1$ και $1 < m < n+1$. Επειδή $k \in X$ και δεν είναι ίσος με 1 έχουμε ότι ο k έχει πρώτο διαιρέτη. Κάθε διαιρέτης του k είναι και διαιρέτης του $n+1$. Η υπόθεση λοιπόν ότι όλοι οι αριθμοί $\leq n$ ανήκουν στο X συνεπάγεται ότι $(n+1) \in X$. Αυτή η παρατήρηση και το γεγονός ότι $0, 1 \in X$ μας οδηγούν στο συμπέρασμα ότι $X = \mathbb{N}$, με βάση την 2η μορφή της αρχής της επαγωγής.

Στο παραπάνω παράδειγμα η απλή επαγωγή *πάνω στην ίδια ιδιότητα* δεν θα αρκούσε: για να δείξουμε ότι ο $n+1$ έχει πρώτο διαιρέτη χρησιμοποιήσαμε τον διαιρέτη k του $n+1$, που μπορεί να είναι πολύ μικρότερος από τον n, και όχι τον ίδιο τον n (που δεν έχει καμία σχέση με τους διαιρέτες του $n+1$). (Φυσικά, από την Πρόταση 2.9, η απόδειξη μπορεί να ξαναγραφτεί με απλή επαγωγή, για την ιδιότητα «όλοι οι $1, \dots, n$ έχουν την ιδιότητα».)

Παρατήρηση 2.11 (Ισχυρή επαγωγή με πολλές βάσεις). Όπως και η απλή, η ισχυρή επαγωγή μπορεί να ξεκινά από οποιοδήποτε n_0. Συχνά μάλιστα το επαγωγικό βήμα για την $P(k+1)$ χρησιμοποιεί την $P(k+1-r)$ για κάποιο σταθερό $r \geq 1$, δηλαδή «κοιτάζει» r θέσεις πίσω. Τότε η βάση πρέπει να περιέχει ένα ολόκληρο «παράθυρο» r διαδοχικών τιμών: δείχνουμε τις $P(n_0)$, $P(n_0+1)$, ..., $P(n_0+r-1)$ και μετά, για κάθε $k \geq n_0 + r - 1$, δείχνουμε ότι από τις $P(n_0)$, ..., $P(k)$ έπεται η $P(k+1)$. (Για $k+1 \leq n_0 + r - 1$ η $P(k+1)$ είναι μία από τις βάσεις, άρα το επαγωγικό βήμα ισχύει για *κάθε* $k \geq n_0$.)

Είμαστε τώρα έτοιμοι να λύσουμε το πρόβλημα των γραμματοσήμων.

Πρόταση 2.12. *Κάθε ποσό $n \geq 28$ λεπτών μπορεί να πληρωθεί ακριβώς με γραμματόσημα των 5 και των 8 λεπτών.*

Απόδειξη. Με ισχυρή επαγωγή από τη βάση $n_0 = 28$. Το επαγωγικό βήμα θα «κοιτάζει» 5 θέσεις πίσω, γι' αυτό χρειαζόμαστε 5 διαδοχικές βάσεις:

$$28 = 4 \cdot 5 + 8, \quad 29 = 5 + 3 \cdot 8, \quad 30 = 6 \cdot 5, \quad 31 = 3 \cdot 5 + 2 \cdot 8, \quad 32 = 4 \cdot 8.$$

Έστω τώρα $k \geq 32$ και ας υποθέσουμε ότι κάθε ποσό m με $28 \leq m \leq k$ μπορεί να πληρωθεί ακριβώς. Αφού $k+1 \geq 33$, έχουμε $28 \leq (k+1)-5 \leq k$, άρα από την επαγωγική υπόθεση το ποσό $(k+1)-5$ πληρώνεται ακριβώς· προσθέτοντας ένα γραμματόσημο των 5 λεπτών πληρώνουμε ακριβώς το $k+1$. Από την ισχυρή επαγωγή (με την Παρατήρηση 2.11), κάθε ποσό $n \geq 28$ πληρώνεται ακριβώς. □

Το όριο 28 δεν μπορεί να βελτιωθεί: το ποσό 27 *δεν* πληρώνεται, αφού κανένα από τα 27, $27-8=19$, $27-16=11$, $27-24=3$ δεν είναι πολλαπλάσιο του 5. Μια διαφορετική απόδειξη της Πρότασης 2.12, με απλή επαγωγή, ζητείται στην Άσκηση 13.

Ασκήσεις

1. Δείξτε ότι αν το σύνολο A έχει n στοιχεία τότε το $\mathcal{P}(A)$ έχει 2^n στοιχεία. (Αυτή τη φορά με επαγωγή στο n· συγκρίνετε με την απόδειξη της Πρότασης 1.21.)

2. Δείξτε ότι για κάθε $n \in \mathbb{N},\ n \geq 1$

$$(A_1 \cup A_2 \cup \cdots \cup A_n) \times X = (A_1 \times X) \cup (A_2 \times X) \cup \cdots \cup (A_n \times X).$$

3. Δείξτε ότι ο $n^3 + 2n$ είναι πολλαπλάσιο του 3 για όλα τα $n \geq 1$.

4. Δείξτε ότι $n^2 < 2^n$ για $n \geq 5$.

5. ⁻ Δείξτε με επαγωγή ότι για κάθε $n \geq 1$

$$1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

δηλαδή ότι το άθροισμα των πρώτων n περιττών αριθμών είναι n^2.

6. ⁻ Δείξτε ότι για κάθε $n \in \mathbb{N}$ ισχύει $2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.

7. Δείξτε με επαγωγή ότι για κάθε $n \in \mathbb{N}$:

(α) ο $7^n - 1$ είναι πολλαπλάσιο του 6·

(β) ο $7^n - 2^n$ διαιρείται με το 5·

(γ) γενικότερα, αν a, b είναι ακέραιοι με $a \neq b$, ο $a^n - b^n$ διαιρείται με το $a - b$. Ποια είναι τα a, b στα (α) και (β);

8. Δείξτε ότι $2^n < n!$ για κάθε $n \geq 4$. (Θυμηθείτε ότι $n! = 1 \cdot 2 \cdot 3 \cdots n$.)

9. ⁻ Δείξτε ότι για κάθε $n \geq 1$:

(α) $1 + 4 + 7 + \cdots + (3n-2) = \dfrac{n(3n-1)}{2}$.

(β) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

(γ) $\dfrac{1}{1\cdot 3}+\dfrac{1}{3\cdot 5}+\cdots+\dfrac{1}{(2n-1)(2n+1)}=\dfrac{n}{2n+1}$.

10. Χρησιμοποιώντας τον τύπο του Παραδείγματος 2.4, δείξτε ότι για κάθε $n\geq 1$

$$1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2.$$

11. ⁻ Σε ένα δωμάτιο βρίσκονται $n\geq 1$ άτομα και ο καθένας δίνει το χέρι σε όλους τους άλλους ακριβώς μία φορά. Δείξτε με επαγωγή ότι γίνονται συνολικά $n(n-1)/2$ χειραψίες. (*Υπόδειξη:* πόσες νέες χειραψίες γίνονται όταν μπαίνει στο δωμάτιο το άτομο $n+1$;)

12. Τι είναι λάθος σε καθεμία από τις παρακάτω «αποδείξεις»;

(α) «Ισχύει $n+3=n+7$ για κάθε $n\in\mathbb{N}$. Έστω ότι ισχύει $k+3=k+7$. Προσθέτοντας 1 και στα δύο μέλη παίρνουμε $(k+1)+3=(k+1)+7$, που είναι η πρόταση για $k+1$. Από την αρχή της επαγωγής, $n+3=n+7$ για κάθε n.»

(β) «Ο n^2+n είναι περιττός για κάθε $n\in\mathbb{N}$. Έστω ότι ο k^2+k είναι περιττός. Τότε $(k+1)^2+(k+1)=(k^2+k)+(2k+2)$ είναι άθροισμα ενός περιττού και ενός άρτιου, άρα περιττός. Από την αρχή της επαγωγής, ο n^2+n είναι περιττός για κάθε n.»

(γ) «Για κάθε $n\geq 1$, οποιοιδήποτε n αριθμοί $a_1,\dots,a_n$ είναι όλοι ίσοι. Για $n=1$ είναι προφανές. Έστω ότι ισχύει για k αριθμούς, και έστω $a_1,\dots,a_{k+1}$. Από την επαγωγική υπόθεση οι $a_1,\dots,a_k$ είναι ίσοι, και το ίδιο οι $a_2,\dots,a_{k+1}$. Αφού ο a_2 ανήκει και στις δύο ομάδες, όλοι είναι ίσοι με τον a_2.»

Δώστε στη συνέχεια μια σωστή απόδειξη με επαγωγή ότι ο n^2+n είναι *άρτιος* για κάθε $n\in\mathbb{N}$.

13. Γραμματόσημα των 5 και των 8 λεπτών, ξανά.

(α) Αν ένα ποσό πληρώνεται με τουλάχιστον τρία γραμματόσημα των 5 λεπτών, δείξτε ότι πληρώνεται και το ποσό που είναι κατά 1 λεπτό μεγαλύτερο. (*Υπόδειξη:* πόσο είναι το $-3\cdot 5+2\cdot 8$;)

(β) Το ίδιο, αν το ποσό πληρώνεται με τουλάχιστον τρία γραμματόσημα των 8 λεπτών.

(γ) Συμπεράνετε, με *απλή* επαγωγή, ότι κάθε ποσό $n\geq 28$ πληρώνεται ακριβώς.

14. * Ένα τετράγωνο μπορεί να κοπεί σε μικρότερα τετράγωνα, κόβοντας κατά μήκος ευθειών παράλληλων στις πλευρές του (οι τομές δεν χρειάζεται να διασχίζουν όλο το τετράγωνο). Για παράδειγμα, με τις τομές του σχήματος  παίρνουμε 6 τετράγωνα. Αποδείξτε με ισχυρή επαγωγή ότι ένα τετράγωνο μπορεί να κοπεί σε n μικρότερα τετράγωνα για κάθε $n\geq 6$. (*Υπόδειξη:* θα χρειαστείτε τρεις βάσεις.)

15. Ένα παζλ έχει $n\geq 1$ κομμάτια. Σε κάθε κίνηση ενώνουμε δύο κομμάτια, ή δύο ήδη συναρμολογημένα τμήματα, σε ένα. Δείξτε με ισχυρή επαγωγή ότι, όποια σειρά κι αν ακολουθήσουμε, για να ολοκληρωθεί το παζλ χρειάζονται ακριβώς $n-1$ κινήσεις.

16. Δείξτε με ισχυρή επαγωγή ότι κάθε θετικός ακέραιος είτε είναι δύναμη του 2 είτε γράφεται ως άθροισμα *διαφορετικών* δυνάμεων του 2.

17. * Έστω x ένας πραγματικός αριθμός τέτοιος ώστε ο $x+\frac{1}{x}$ να είναι ακέραιος. Δείξτε ότι ο $x^n+\frac{1}{x^n}$ είναι ακέραιος για κάθε $n\in\mathbb{N}$. (*Υπόδειξη:* ισχυρή επαγωγή· υπολογίστε το γινόμενο $(x^k+\frac{1}{x^k})(x+\frac{1}{x})$.)

18. * Μια *γωνία* είναι ένα σχήμα από τρία τετραγωνάκια σε σχήμα «Γ». Από μια σκακιέρα $2^n\times 2^n$ ($n\geq 1$) αφαιρούμε *ένα οποιοδήποτε* τετραγωνάκι. Δείξτε με επαγωγή στο n ότι τα υπόλοιπα τετραγωνάκια μπορούν να καλυφθούν με γωνίες, χωρίς επικαλύψεις. Πόσες γωνίες χρειάζονται;

2.2 Ισοδυναμία συνόλων. Αριθμήσιμα και υπεραριθμήσιμα σύνολα

Πόσα στοιχεία έχει το $\mathbb{N} = \{0, 1, 2, 3, \dots\}$; Και πόσα το σύνολο $\{0, 2, 4, 6, \dots\}$ των άρτιων φυσικών; Διαισθητικά, οι άρτιοι είναι «οι μισοί» φυσικοί. Όμως κάθε $n \in \mathbb{N}$ αντιστοιχεί σε *ακριβώς έναν* άρτιο, τον $2n$, και κάθε άρτιος προκύπτει έτσι από *ακριβώς έναν* φυσικό. Σε αυτή την ενότητα θα δούμε πώς συγκρίνουμε αυστηρά τα «μεγέθη» συνόλων, ακόμη και άπειρων, και θα διαπιστώσουμε ότι για τα άπειρα σύνολα η διαίσθησή μας χρειάζεται αναθεώρηση.

2.2.1 Ισοδύναμα σύνολα

Θυμηθείτε ότι με $|X|$ συμβολίζουμε την πληθικότητα (το πλήθος των στοιχείων) ενός πεπερασμένου συνόλου X (Ορισμός 1.20).

Ορισμός 2.13 (Ισοδύναμα σύνολα). Λέμε ότι δύο σύνολα X και Y είναι *ισοδύναμα* και το γράφουμε $X \sim Y$ όταν υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των στοιχείων των συνόλων X και Y, δηλαδή όταν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : X \to Y$.

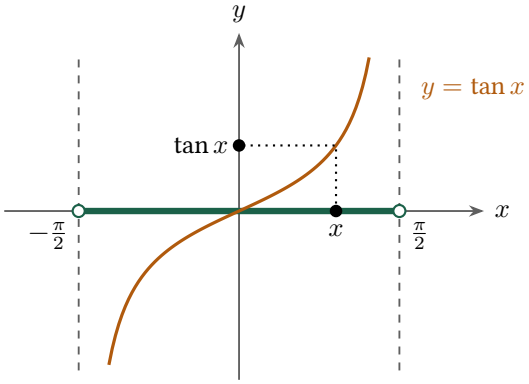
Προφανώς για δύο πεπερασμένα σύνολα A και B έχουμε $A \sim B \Leftrightarrow |A| = |B|$. Η δύναμη του ορισμού είναι ότι *δεν* απαιτεί τα σύνολα να είναι πεπερασμένα.

Παράδειγμα 2.14. 1) Η συνάρτηση που ορίζεται από τον τύπο $f(x) = 2x$ για $x \in \mathbb{N}$ είναι μια αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to \{2x : x \in \mathbb{N}\}$. Βλέπουμε λοιπόν ότι το σύνολο $\mathbb{N}$ και το σύνολο των αρτίων φυσικών είναι ισοδύναμα.

2) Το σύνολο $(-\frac{\pi}{2}, \frac{\pi}{2})$ και το $\mathbb{R}$ είναι ισοδύναμα επειδή έχουμε

$$f : (-\tfrac{\pi}{2}, \tfrac{\pi}{2}) \to \mathbb{R}, \quad f(x) = \tan(x).$$

(Η εφαπτομένη είναι γνησίως αύξουσα στο $(-\frac{\pi}{2}, \frac{\pi}{2})$, άρα ενριπτική, και παίρνει κάθε πραγματική τιμή, άρα είναι επί· βλ. Σχήμα 2.1.)



Σχήμα 2.1. Η $\tan : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ είναι αμφιμονοσήμαντη: κάθε οριζόντια ευθεία $y = c$ τέμνει το γράφημα σε ακριβώς ένα σημείο. Το φραγμένο διάστημα (πράσινο) έχει «τόσα σημεία» όσα ολόκληρη η ευθεία $\mathbb{R}$.

Παρατήρηση 2.15. Το πρώτο από τα παραπάνω παραδείγματα είναι *αδύνατο* για πεπερασμένα σύνολα: ένα γνήσιο υποσύνολο ενός πεπερασμένου συνόλου έχει πάντα λιγότερα στοιχεία, άρα δεν είναι ισοδύναμο με αυτό. Ένα άπειρο σύνολο, αντίθετα, μπορεί να είναι ισοδύναμο με γνήσιο υποσύνολό του (οι άρτιοι φυσικοί είναι γνήσιο υποσύνολο του $\mathbb{N}$). Η ιδιότητα αυτή χρησιμοποιείται μάλιστα και ως ένας τρόπος να *ορίσουμε* τι σημαίνει «άπειρο σύνολο» (ορισμός του Dedekind).

Με τον ίδιο τρόπο, και το διάστημα $(0, 1)$ είναι ισοδύναμο με το $\mathbb{R}$: η $h : (0, 1) \to (-\frac{\pi}{2}, \frac{\pi}{2})$ με $h(x) = \pi x - \frac{\pi}{2}$ είναι αμφιμονοσήμαντη (η αντίστροφή της είναι η $y \mapsto \frac{y}{\pi} + \frac{1}{2}$), οπότε η σύνθεση $\tan \circ h$,

δηλαδή η $x \mapsto \tan(\pi x - \frac{\pi}{2})$, είναι αμφιμονοσήμαντη συνάρτηση από το $(0,1)$ στο $\mathbb{R}$ (Πρόταση 1.58 και Άσκηση 14 της Ενότητας 1.3).

Εύκολα μπορούμε να αποδείξουμε τις παρακάτω ιδιότητες:

1. $X \sim X$,
2. $X \sim Y \Rightarrow Y \sim X$,
3. $X \sim Y$ και $Y \sim Z \Rightarrow X \sim Z$.

Πραγματικά η (1) ισχύει επειδή η ταυτοτική απεικόνιση $\mathrm{id}_X : X \to X$ είναι αμφιμονοσήμαντη. Για την (2) αρκεί να παρατηρήσουμε ότι αν η $f : X \to Y$ είναι αμφιμονοσήμαντη, τότε και η $f^{-1} : Y \to X$ είναι αμφιμονοσήμαντη. Ξέρουμε επίσης ότι αν $f : X \to Y$ και $g : Y \to Z$ είναι αμφιμονοσήμαντες, τότε και η $g \circ f : X \to Z$ είναι αμφιμονοσήμαντη (Ενότητα 1.3). Αυτό αποδεικνύει την (3).

Οι (1)–(3) είναι ακριβώς οι ιδιότητες μιας σχέσης ισοδυναμίας (Ορισμός 1.36): η αυτοπαθής, η συμμετρική και η μεταβατική. Για παράδειγμα, αν $\mathcal{U}$ είναι ένα σύνολο, τότε η $\sim$ είναι σχέση ισοδυναμίας στο $\mathcal{P}(\mathcal{U})$, και κάθε κλάση ισοδυναμίας της αποτελείται από υποσύνολα του $\mathcal{U}$ με «το ίδιο πλήθος στοιχείων». (Προσέξτε ότι *δεν* μιλάμε για σχέση στο «σύνολο όλων των συνόλων»: τέτοιο σύνολο δεν υπάρχει, όπως είδαμε με το παράδοξο του Russell στην Ενότητα 1.1.)

2.2.2 Πεπερασμένα και αριθμήσιμα σύνολα

Ορισμός 2.16 (Πεπερασμένο σύνολο). Έστω $\mathbb{N}_k = \{1, 2, 3, \dots, k\}$ για $k \in \mathbb{N}$, $k > 0$. Τα σύνολα $\mathbb{N}_k$ είναι *αρχικά τμήματα* του συνόλου των φυσικών. Ένα σύνολο λέγεται *πεπερασμένο* όταν είναι ισοδύναμο με κάποιο από τα σύνολα $\mathbb{N}_k$ ή είναι το κενό σύνολο.

Εύκολα βλέπουμε ότι $X \sim \mathbb{N}_k \Leftrightarrow |X| = k$. Το σύνολο $\mathbb{N}$ των φυσικών δεν είναι πεπερασμένο. Τα σύνολα που δεν είναι πεπερασμένα τα λέμε *άπειρα*.

Ας δικαιολογήσουμε γιατί το $\mathbb{N}$ δεν είναι πεπερασμένο. Προφανώς $\mathbb{N} \neq \emptyset$. Αν $f : \mathbb{N}_k \to \mathbb{N}$ είναι *οποιαδήποτε* συνάρτηση, τότε το πεδίο τιμών της $\{f(1), \dots, f(k)\}$ είναι ένα πεπερασμένο, μη κενό σύνολο φυσικών, άρα έχει μέγιστο στοιχείο M. Ο φυσικός $M + 1$ δεν είναι τιμή της f, άρα η f δεν είναι επί. Επομένως δεν υπάρχει αμφιμονοσήμαντη συνάρτηση $\mathbb{N}_k \to \mathbb{N}$, ούτε (από την ιδιότητα (2) παραπάνω) αμφιμονοσήμαντη συνάρτηση $\mathbb{N} \to \mathbb{N}_k$, για κανένα k.

Μεταξύ των απείρων συνόλων θα ξεχωρίσουμε αυτά τα σύνολα που δέχονται μια «αρίθμηση» με τη βοήθεια των φυσικών.

Ορισμός 2.17 (Αριθμήσιμο σύνολο). Ένα σύνολο X λέγεται *αριθμήσιμο* όταν $X \sim \mathbb{N}$, δηλαδή όταν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : X \to \mathbb{N}$. Ένα σύνολο λέγεται *το πολύ αριθμήσιμο* αν είναι πεπερασμένο ή αριθμήσιμο, και *υπεραριθμήσιμο* αν δεν είναι το πολύ αριθμήσιμο.

Αν το X είναι αριθμήσιμο τότε γράφουμε $|X| = \aleph_0$.

(Το $\aleph$, «άλεφ», είναι το πρώτο γράμμα του εβραϊκού αλφαβήτου.) Ισοδύναμα, το X είναι αριθμήσιμο αν υπάρχει αμφιμονοσήμαντη συνάρτηση $g : \mathbb{N} \to X$ (η f^{-1}), δηλαδή αν μπορούμε να γράψουμε *όλα* τα στοιχεία του X σε μια άπειρη λίστα $g(0), g(1), g(2), \dots$, χωρίς επαναλήψεις.

Παράδειγμα 2.18. 1) Το $\mathbb{N}$ είναι αριθμήσιμο.

2) Το σύνολο A των περιττών φυσικών είναι αριθμήσιμο. Πράγματι η συνάρτηση $f(x) = 2x + 1$ δίνει την ισοδυναμία του A με το $\mathbb{N}$.

3) Η συνάρτηση $f : \mathbb{N} \to \mathbb{Z}$ που ορίζεται από το

$$f(n) = \begin{cases} k & \text{αν } n = 2k \\ -k & \text{αν } n = 2k - 1 \end{cases}$$

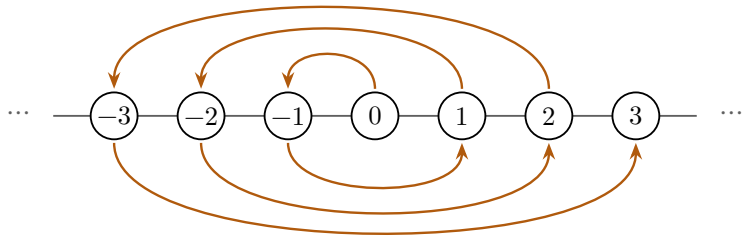
είναι αμφιμονοσήμαντη. Άρα έχουμε $\mathbb{N} \sim \mathbb{Z}$, δηλαδή το $\mathbb{Z}$ είναι αριθμήσιμο.

4) Το σύνολο $\mathbb{N} \times \mathbb{N}$ είναι αριθμήσιμο αφού η συνάρτηση $g(n, m) = 2^n \cdot (2m + 1) - 1$ είναι αμφιμονοσήμαντη από το $\mathbb{N} \times \mathbb{N}$ στο $\mathbb{N}$.

Ας δούμε τα δύο τελευταία παραδείγματα πιο προσεκτικά. Η f του 3) «τυλίγει» τους ακεραίους γύρω από το 0, εναλλάσσοντας αρνητικούς και θετικούς:

n	0	1	2	3	4	5	6	⋯
$f(n)$	0	-1	1	-2	2	-3	3	⋯

(Σχήμα 2.2). Κάθε ακέραιος εμφανίζεται στη δεύτερη γραμμή ακριβώς μία φορά: ο $k > 0$ ως $f(2k)$, ο $-k < 0$ ως $f(2k - 1)$, και ο 0 ως $f(0)$.

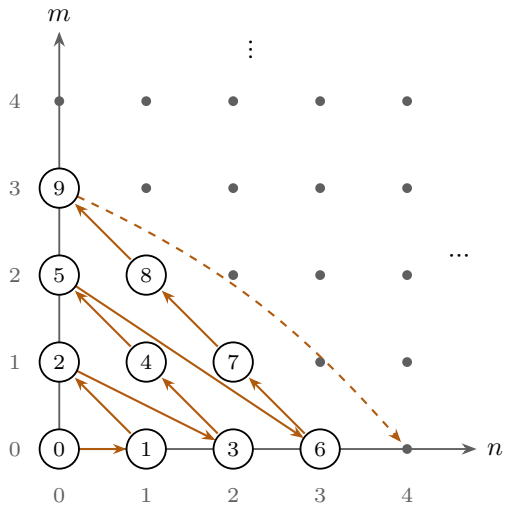


Σχήμα 2.2. Η απαρίθμηση $0, -1, 1, -2, 2, -3, 3, \ldots$ του $\mathbb{Z}$: ακολουθώντας τα βέλη συναντάμε κάθε ακέραιο ακριβώς μία φορά.

Για το $\mathbb{N} \times \mathbb{N}$ υπάρχει και ένας πιο «οπτικός» τρόπος να απαριθμήσουμε τα στοιχεία του: τα τοποθετούμε σε ένα πλέγμα και τα διατρέχουμε κατά διαγωνίους (Σχήμα 2.3). Στη διαγώνιο $d = 0, 1, 2, \ldots$ βρίσκονται τα $d + 1$ ζεύγη (n, m) με $n + m = d$, και κάθε ζεύγος βρίσκεται σε ακριβώς μία διαγώνιο. Έτσι παίρνουμε τη λίστα

$$(0,0),\ (1,0),\ (0,1),\ (2,0),\ (1,1),\ (0,2),\ (3,0),\ \ldots$$

στην οποία εμφανίζεται κάθε στοιχείο του $\mathbb{N} \times \mathbb{N}$ ακριβώς μία φορά. (Ένας τύπος για τη θέση του (n, m) σε αυτή τη λίστα ζητείται στην Άσκηση 4.)



Σχήμα 2.3. Η απαρίθμηση του $\mathbb{N} \times \mathbb{N}$ κατά διαγωνίους. Ο αριθμός μέσα σε κάθε κύκλο είναι η θέση του αντίστοιχου ζεύγους στη λίστα.

Όσο για τη συνάρτηση g του 4): κάθε θετικός ακέραιος s γράφεται με μοναδικό τρόπο ως $s = 2^n(2m + 1)$, δηλαδή ως δύναμη του 2 επί έναν περιττό αριθμό. Η *ύπαρξη* αποδεικνύεται με ισχυρή

επαγωγή στο s: αν ο s είναι περιττός, παίρνουμε $n = 0$· αν είναι άρτιος, τότε $s = 2s'$ με $1 \leq s' < s$, και αν $s' = 2^{n'}(2m+1)$, τότε $s = 2^{n'+1}(2m+1)$. Για τη *μοναδικότητα*, αν $2^n a = 2^{n'} b$ με a, b περιττούς και $n < n'$, τότε $a = 2^{n'-n} b$ θα ήταν άρτιος, άτοπο· άρα $n = n'$ και $a = b$. Επομένως η $(n, m) \mapsto 2^n(2m+1)$ είναι αμφιμονοσήμαντη από το $\mathbb{N} \times \mathbb{N}$ στους θετικούς ακεραίους, και η g (που αφαιρεί 1) είναι αμφιμονοσήμαντη από το $\mathbb{N} \times \mathbb{N}$ στο $\mathbb{N}$.

Πρόταση 2.19. *Αν X, Y είναι αριθμήσιμα τότε και το σύνολο $X \times Y$ είναι αριθμήσιμο.*

Απόδειξη. Έστω $f : \mathbb{N} \to X$ και $g : \mathbb{N} \to Y$ αμφιμονοσήμαντες. Τότε μπορούμε να ορίσουμε μια $h : \mathbb{N} \times \mathbb{N} \to X \times Y$ με $h(n, m) = (f(n), g(m))$. Η h είναι ενριπτική: αν $(f(n), g(m)) = (f(n'), g(m'))$, τότε $f(n) = f(n')$ και $g(m) = g(m')$, άρα $n = n'$ και $m = m'$. Είναι και επί: για $(x, y) \in X \times Y$ υπάρχουν n, m με $f(n) = x$ και $g(m) = y$, άρα $h(n, m) = (x, y)$. Άρα $X \times Y \sim \mathbb{N} \times \mathbb{N}$ και επειδή $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ έχουμε $X \times Y \sim \mathbb{N}$. □

Για να δείξουμε ότι ένα σύνολο είναι αριθμήσιμο, αρκεί συχνά να βρούμε μια *ενριπτική* (και όχι αναγκαστικά επί) συνάρτηση από αυτό σε ένα αριθμήσιμο σύνολο. Αυτό βασίζεται στο επόμενο αποτέλεσμα, που στηρίζεται στην αρχή της καλής διάταξης.

Πρόταση 2.20. *Κάθε άπειρο υποσύνολο S του $\mathbb{N}$ είναι αριθμήσιμο.*

Απόδειξη. Θα γράψουμε τα στοιχεία του S σε αύξουσα σειρά. Από την αρχή της καλής διάταξης, το S έχει ελάχιστο στοιχείο· έστω $s_0 = \min S$. Αν έχουμε ορίσει τα $s_0, s_1, \dots, s_n$, το σύνολο $S \setminus \{s_0, \dots, s_n\}$ δεν είναι κενό (αφού το S είναι άπειρο), και ορίζουμε s_{n+1} να είναι το ελάχιστο στοιχείο του. Έτσι ορίζεται (επαγωγικά) μια συνάρτηση $g : \mathbb{N} \to S$ με $g(n) = s_n$. Η g είναι γνησίως αύξουσα: το s_{n+1} ανήκει στο $S \setminus \{s_0, \dots, s_{n-1}\}$, του οποίου ελάχιστο στοιχείο είναι το s_n (για $n = 0$, στο S, του οποίου ελάχιστο είναι το s_0), άρα $s_{n+1} \geq s_n$, και $s_{n+1} \neq s_n$. Επομένως η g είναι ενριπτική.

Η g είναι και επί. Από το ότι είναι γνησίως αύξουσα έπεται με επαγωγή ότι $s_n \geq n$ για κάθε n. Έστω $t \in S$. Το σύνολο $\{n \in \mathbb{N} : s_n > t\}$ δεν είναι κενό (περιέχει το $t+1$), άρα έχει ελάχιστο στοιχείο, έστω n. Αν το t δεν ήταν κάποιο από τα $s_0, \dots, s_{n-1}$, τότε θα είχαμε $t \in S \setminus \{s_0, \dots, s_{n-1}\}$ και άρα $s_n \leq t$, άτοπο. Άρα $t = s_j$ για κάποιο $j < n$, δηλαδή το t είναι τιμή της g. □

Πόρισμα 2.21. *Αν υπάρχει ενριπτική συνάρτηση $\psi : A \to B$ και το B είναι αριθμήσιμο, τότε το A είναι το πολύ αριθμήσιμο. Ειδικά, κάθε υποσύνολο ενός αριθμήσιμου συνόλου είναι το πολύ αριθμήσιμο.*

Απόδειξη. Έστω $f : B \to \mathbb{N}$ αμφιμονοσήμαντη. Η $f \circ \psi : A \to \mathbb{N}$ είναι ενριπτική, άρα αμφιμονοσήμαντη από το A στο πεδίο τιμών της $S = f(\psi(A)) \subseteq \mathbb{N}$, δηλαδή $A \sim S$. Αν το S είναι πεπερασμένο, τότε και το A είναι πεπερασμένο· αν είναι άπειρο, τότε από την Πρόταση 2.20 είναι $A \sim S \sim \mathbb{N}$. Για το δεύτερο μέρος παίρνουμε ως ψ τη συνάρτηση εγκλεισμού $A \to B$. □

Το σύνολο $\mathbb{Q}$ των ρητών αριθμών είναι αριθμήσιμο. Αυτό φαίνεται από την παρακάτω απόδειξη. Η συνάρτηση $f\left(\frac{k}{m}\right) = (k, m)$, όπου $m > 0$ και k, m πρώτοι μεταξύ τους, απεικονίζει το $\mathbb{Q}$ στο $\mathbb{Z} \times \mathbb{N}$ και είναι ενριπτική. Επειδή όμως $\mathbb{Z} \times \mathbb{N} \sim \mathbb{N}$, το $\mathbb{Q}$ θα είναι το πολύ αριθμήσιμο (Πόρισμα 2.21) και αφού είναι άπειρο θα έχουμε $\mathbb{Q} \sim \mathbb{N}$.

Το αποτέλεσμα είναι εντυπωσιακό: οι ρητοί *φαίνονται* πολύ «πυκνότεροι» από τους φυσικούς (ανάμεσα σε δύο οποιουσδήποτε ρητούς υπάρχουν άπειροι άλλοι), έχουν όμως «το ίδιο πλήθος».

Με την ίδια τεχνική (ενριπτική συνάρτηση στο $\mathbb{N} \times \mathbb{N}$ και το Πόρισμα 2.21) αποδεικνύεται και το επόμενο αποτέλεσμα.

Παράδειγμα 2.22 (Αριθμήσιμη ένωση αριθμήσιμων συνόλων). Έστω $X_0, X_1, X_2, \dots$ αριθμήσιμα σύνολα. Θα δείξουμε ότι η ένωσή τους $X = \bigcup_{n \in \mathbb{N}} X_n$ είναι αριθμήσιμη.

Λύση. Για κάθε n, αφού το X_n είναι αριθμήσιμο, επιλέγουμε μια αμφιμονοσήμαντη συνάρτηση $e_n : \mathbb{N} \to X_n$, δηλαδή μια απαρίθμηση $X_n = \{e_n(0), e_n(1), e_n(2), \dots\}$.[1] Ένα στοιχείο $y \in X$ μπορεί να ανήκει σε περισσότερα από ένα X_n. Γι' αυτό ορίζουμε

$$n(y) = \min\{n \in \mathbb{N} : y \in X_n\},$$

που υπάρχει από την αρχή της καλής διάταξης, και $m(y)$ τον μοναδικό φυσικό με $e_{n(y)}(m(y)) = y$. Η συνάρτηση $\psi : X \to \mathbb{N} \times \mathbb{N}$ με $\psi(y) = (n(y), m(y))$ είναι ενριπτική: αν $\psi(y) = \psi(y') = (n, m)$, τότε $y = e_n(m) = y'$. Επειδή το $\mathbb{N} \times \mathbb{N}$ είναι αριθμήσιμο, από το Πόρισμα 2.21 το X είναι το πολύ αριθμήσιμο. Τέλος, το X περιέχει το άπειρο σύνολο X_0, άρα είναι άπειρο, και επομένως αριθμήσιμο. ◊

2.2.3 Υπεραριθμήσιμα σύνολα

Παραπάνω γνωρίσαμε πολλά άπειρα σύνολα που είναι αριθμήσιμα. Δεν είναι όλα τα άπειρα σύνολα αριθμήσιμα! Για παράδειγμα το ανοικτό διάστημα $(0, 1) \subseteq \mathbb{R}$. Θα δείξουμε ότι το σύνολο των πραγματικών αριθμών μεταξύ 0 και 1 δεν είναι αριθμήσιμο. Η απόδειξη, που δόθηκε από τον G. Cantor το 1891, είναι γνωστή ως το *διαγώνιο επιχείρημα* του Cantor. Ας υποθέσουμε ότι το $(0, 1)$ είναι αριθμήσιμο (για να καταλήξουμε σε άτοπο). Τότε θα είχαμε όλα τα στοιχεία του $(0, 1)$ σε μια λίστα $a_0, a_1, a_2, \dots, a_n, \dots$ που θα μας δινόταν από την ισοδυναμία $(0, 1) \sim \mathbb{N}$.

Συνεπώς θα μπορούσαμε να εξαντλήσουμε όλους τους πραγματικούς μεταξύ 0 και 1 σ' αυτή τη λίστα, δηλαδή κάθε πραγματικός $a \in \mathbb{R}$ με $0 < a < 1$ θα ήταν κάποιος a_i με $i \in \mathbb{N}$. Θα είχαμε λοιπόν τη λίστα:

$$\begin{aligned} a_0 &= 0, a_{00}\, a_{01}\, a_{02}\, a_{03} \cdots \\ a_1 &= 0, a_{10}\, a_{11}\, a_{12}\, a_{13} \cdots \\ a_2 &= 0, a_{20}\, a_{21}\, a_{22}\, a_{23} \cdots \\ a_n &= 0, a_{n0}\, a_{n1}\, a_{n2}\, a_{n3} \cdots a_{nn} \cdots \end{aligned}$$

γράφοντας σαν δεκαδικό κάθε a_i, $i \in \mathbb{N}$, όπου a_{ij} είναι το j-οστό ψηφίο του i-οστού αριθμού στη λίστα. Ας θεωρήσουμε τώρα τον αριθμό

$$0, b_0\, b_1\, b_2\, b_3 \cdots \quad \text{όπου} \quad b_i = \begin{cases} 5 & \text{αν } a_{ii} \neq 5 \\ 4 & \text{αν } a_{ii} = 5 \end{cases} \text{ για όλα τα } i \in \mathbb{N}.$$

Προφανώς, ο αριθμός $0, b_0\, b_1\, b_2 \cdots$ είναι ένας πραγματικός μεταξύ 0 και 1, ο οποίος είναι διαφορετικός από τον κάθε αριθμό στη λίστα. Αυτό συμβαίνει γιατί διαφέρει από τον a_0 στο μηδενικό ψηφίο, από τον a_1 στο πρώτο ψηφίο, από τον a_2 στο δεύτερο ψηφίο κ.ο.κ., δηλαδή διαφέρει από τον a_i στο i-οστό ψηφίο γιατί $b_i \neq a_{ii}$. (Αφού ο b έχει μόνο ψηφία 4 και 5, έχει μία μόνο δεκαδική παράσταση, οπότε ένα διαφορετικό ψηφίο σημαίνει πράγματι διαφορετικό αριθμό· βλ. Παρατήρηση 2.23.) Άρα ο αριθμός $b = 0, b_0\, b_1\, b_2 \cdots$ δεν είναι στη λίστα. Άτοπο, γιατί στη λίστα βρίσκεται κάθε πραγματικός μεταξύ 0 και 1. Συνεπώς το διάστημα $(0, 1) \subseteq \mathbb{R}$ δεν είναι αριθμήσιμο.

Παρατήρηση 2.23 (Γιατί μόνο τα ψηφία 4 και 5;). Το Σχήμα 2.4 δείχνει την κατασκευή σε ένα παράδειγμα. Ο περιορισμός στα ψηφία 4 και 5 χρειάζεται επειδή ορισμένοι πραγματικοί αριθμοί έχουν *δύο* δεκαδικές παραστάσεις: για παράδειγμα $0{,}2000\ldots = 0{,}1999\ldots$ (γενικά, δύο διαφορετικές δεκαδικές παραστάσεις παριστάνουν τον ίδιο αριθμό μόνο αν η μία τελειώνει σε άπειρα 0 και η άλλη σε άπειρα 9). Έτσι, δύο παραστάσεις που διαφέρουν σε ένα ψηφίο δεν παριστάνουν απαραίτητα διαφορετικούς αριθμούς. Ένας «φυσικός» κανόνας όπως ο $b_i = 9 - a_{ii}$ (και $b_i = 1$ αν $a_{ii} = 9$), δεν το αποκλείει: αν $a_{ii} = 0$ για όλα τα i από κάποιο σημείο και μετά, τότε ο b τελειώνει σε άπειρα 9 και μπορεί να είναι ίσος με κάποιον a_j γραμμένο με την άλλη παράστασή του (ή ακόμη και με τον

[1] Η ταυτόχρονη επιλογή απαριθμήσεων για άπειρα το πλήθος σύνολα είναι ένα σημείο που, στην αξιωματική θεωρία συνόλων, απαιτεί μια ασθενή μορφή του *αξιώματος της επιλογής*. Εδώ τη δεχόμαστε χωρίς σχόλια.

θέση:	0	1	2	3	4	
$a_0 = 0,$	3	4	1	5	9	$\cdots$
$a_1 = 0,$	2	7	1	8	2	$\cdots$
$a_2 = 0,$	5	5	0	2	7	$\cdots$
$a_3 = 0,$	1	4	1	5	2	$\cdots$
$a_4 = 0,$	8	1	0	4	9	$\cdots$
			$\vdots$			
$b = 0,$	5	5	5	4	5	$\cdots$

Σχήμα 2.4. Η διαγώνιος κατασκευή σε ένα παράδειγμα. Το ψηφίο b_i του b προκύπτει από το διαγώνιο ψηφίο a_{ii} (σκιασμένο): $b_i = 5$ αν $a_{ii} \neq 5$ και $b_i = 4$ αν $a_{ii} = 5$. Εδώ $a_{33} = 5$, άρα $b_3 = 4$, ενώ $b_i = 5$ στις άλλες θέσεις. Ο b διαφέρει από κάθε a_i στη θέση i.

$1 = 0{,}999\ldots$). Με ψηφία μόνο 4 και 5 έχουμε $0 < b < 1$, και ο b έχει μία μόνο δεκαδική παράσταση· αφού αυτή διαφέρει στη θέση i από την παράσταση του a_i στη λίστα, έχουμε $b \neq a_i$ για κάθε i. (Οποιαδήποτε δύο ψηφία εκτός από το 0 και το 9 θα έκαναν την ίδια δουλειά.)

Ούτε το $\mathbb{R}$ είναι αριθμήσιμο. Το $(0,1) \sim \mathbb{R}$ το είδαμε στην αρχή της ενότητας, με τη συνάρτηση $x \mapsto \tan(\pi x - \frac{\pi}{2})$. Αν το $\mathbb{R}$ ήταν αριθμήσιμο, τότε από τη μεταβατική ιδιότητα της $\sim$ θα ήταν και το $(0,1)$. Υπάρχουν λοιπόν (τουλάχιστον) δύο διαφορετικά «μεγέθη» απείρων συνόλων: το $\aleph_0$ των $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, και το «μέγεθος» του $\mathbb{R}$, που είναι αυστηρά μεγαλύτερο: το $\mathbb{R}$ περιέχει το $\mathbb{N}$, αλλά δεν είναι ισοδύναμο με αυτό.

Το διαγώνιο επιχείρημα γενικεύεται εντυπωσιακά, και δείχνει ότι δεν υπάρχει «μεγαλύτερο» άπειρο.

Θεώρημα 2.24 (Θεώρημα του Cantor). *Για κάθε σύνολο X (πεπερασμένο ή άπειρο) ισχύει $X \nsim \mathcal{P}(X)$.*

Για πεπερασμένα σύνολα το θεώρημα είναι γνωστό, αφού $2^n > n$ για κάθε n (Παράδειγμα 2.5 και Πρόταση 1.21). Το ενδιαφέρον είναι ότι ισχύει και για άπειρα σύνολα: το $\mathcal{P}(\mathbb{N})$ δεν είναι αριθμήσιμο, το $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ δεν είναι ισοδύναμο με το $\mathcal{P}(\mathbb{N})$, κ.ο.κ. Υπάρχουν λοιπόν άπειρα πολλά, ολοένα «μεγαλύτερα», μεγέθη απείρου. Η απόδειξη του θεωρήματος είναι η πρώτη άσκηση αυτής της ενότητας· είναι μια κομψή παραλλαγή του διαγώνιου επιχειρήματος. Η ίδια ιδέα εμφανίζεται και ως «αρχή της διαγωνοποίησης» στο Κεφάλαιο 3.

Ασκήσεις

1. Δείξτε ότι δεν υπάρχει σύνολο X τέτοιο ώστε $X \sim \mathcal{P}(X)$. (*Υπόδειξη:* αν $f : X \to \mathcal{P}(X)$ είναι επί, θεωρήστε το σύνολο $D = \{x \in X : x \notin f(x)\}$.)

2. Δείξτε ότι τα παρακάτω ζεύγη συνόλων είναι ισοδύναμα, βρίσκοντας σε κάθε περίπτωση μια αμφιμονοσήμαντη συνάρτηση:

(α) $^-$ $\mathbb{N}$ και $\{n \in \mathbb{N} : n \geq 5\}$·

(β) $^-$ $\mathbb{Z}$ και το σύνολο $2\mathbb{Z}$ των άρτιων ακεραίων·

(γ) $(0,1)$ και (a,b), όπου $a < b$ πραγματικοί αριθμοί·

(δ) * $(0,1)$ και $[0,1)$.

3. Δείξτε ότι το $\mathbb{Z} \times \mathbb{Z}$ είναι αριθμήσιμο. Στη συνέχεια δείξτε με επαγωγή στο k ότι το $\mathbb{N}^k = \mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ (k φορές) είναι αριθμήσιμο για κάθε $k \geq 1$.

4. ⋆ Δείξτε ότι στην απαρίθμηση του Σχήματος 2.3 το ζεύγος (n, m) βρίσκεται στη θέση

$$G(n, m) = \frac{(n + m)(n + m + 1)}{2} + m,$$

και συμπεράνετε ότι η $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ είναι αμφιμονοσήμαντη. (*Υπόδειξη:* πόσα ζεύγη βρίσκονται στις διαγωνίους $0, 1, \dots, d - 1$; Χρησιμοποιήστε το Παράδειγμα 2.4.)

5. Δείξτε ότι το σύνολο $\mathcal{F}$ όλων των *πεπερασμένων* υποσυνόλων του $\mathbb{N}$ είναι αριθμήσιμο. (*Υπόδειξη:* στο πεπερασμένο $S \subseteq \mathbb{N}$ αντιστοιχίστε τον φυσικό $\sum_{i \in S} 2^i$, και θυμηθείτε την Άσκηση 16 της Ενότητας 2.1.)

6. Έστω $A_0, A_1, A_2, \dots$ πεπερασμένα σύνολα. Δείξτε ότι η ένωση $\bigcup_{n \in \mathbb{N}} A_n$ είναι το πολύ αριθμήσιμη.

7. Δείξτε ότι το σύνολο όλων των πεπερασμένων «λέξεων» (δηλαδή ακολουθιών γραμμάτων πεπερασμένου μήκους) από ένα αλφάβητο 24 γραμμάτων είναι αριθμήσιμο.

8. ⋆ Επιρριπτικές εικόνες αριθμήσιμων συνόλων.

(α) Έστω A αριθμήσιμο σύνολο και $g : A \to B$ επιρριπτική. Δείξτε ότι το B είναι το πολύ αριθμήσιμο.

(β) Δείξτε ότι το σύνολο R όλων των πραγματικών ριζών όλων των εξισώσεων $x^2 + bx + c = 0$ με $b, c \in \mathbb{Z}$ είναι αριθμήσιμο.

(γ) Συμπεράνετε ότι υπάρχει πραγματικός αριθμός που δεν είναι ρίζα καμιάς τέτοιας εξίσωσης.

9. Δείξτε ότι για οποιαδήποτε σύνολα A, B:

(α) $A \times B \sim B \times A$·

(β) αν $A \sim B$, τότε $\mathcal{P}(A) \sim \mathcal{P}(B)$.

10. ⁻ Δείξτε ότι το σύνολο $\mathbb{R} \setminus \mathbb{Q}$ των άρρητων αριθμών είναι υπεραριθμήσιμο.

11. ⋆ Έστω $\{0, 1\}^{\mathbb{N}}$ το σύνολο όλων των άπειρων ακολουθιών $(x_0, x_1, x_2, \dots)$ με $x_i \in \{0, 1\}$.

(α) Δείξτε, με διαγώνιο επιχείρημα, ότι το $\{0, 1\}^{\mathbb{N}}$ είναι υπεραριθμήσιμο.

(β) Δείξτε ότι $\{0, 1\}^{\mathbb{N}} \sim \mathcal{P}(\mathbb{N})$. (*Υπόδειξη:* χαρακτηριστικές συναρτήσεις, Ορισμός 1.59.)

Συγκρίνετε με το Θεώρημα 2.24.

Κεφάλαιο 3

Λογική

3.1 Γενικά

Μια οδηγία για να κάνουμε κάτι αν μια πρόταση είναι αληθής και να κάνουμε κάτι άλλο διαφορετικά, λέγεται *υποθετική οδηγία*. Η δύναμη των υπολογιστών εν μέρει οφείλεται στην ικανότητά τους να πραγματοποιούν υποθετικές οδηγίες. Για να πραγματοποιήσει μια υποθετική οδηγία ένας υπολογιστής θα χρειασθεί να αποφασίσει την αλήθεια ή το ψεύδος μιας πρότασης. Συνεπώς στα διακριτά μαθηματικά είναι χρήσιμο να μελετήσουμε τις προτάσεις, πώς συνδυάζονται μεταξύ τους και πώς αποφασίζουμε ότι μια πρόταση είναι ισοδύναμη με μια άλλη.

Ας ξεκινήσουμε με δύο επιχειρήματα που, με μια πρώτη ματιά, μοιάζουν πολύ:

Αν η Ανθή φάει το φαγητό της, θα πάρει ένα γλυκό.
Η Ανθή έφαγε το φαγητό της.

Άρα, η Ανθή πήρε γλυκό.

Για να πάρει γλυκό, ο Νίκος πρέπει να φάει το φαγητό του.
Ο Νίκος έφαγε το φαγητό του.

Άρα, ο Νίκος πήρε γλυκό.

Πάνω από τη γραμμή βρίσκονται οι *προκείμενες* κάθε επιχειρήματος και κάτω από αυτήν το *συμπέρασμα*. Είναι και τα δύο επιχειρήματα *έγκυρα*, δηλαδή είναι το συμπέρασμα αναγκαστικά αληθές όταν οι προκείμενες είναι αληθείς; Το πρώτο ναι. Το δεύτερο όχι: το ότι το φαγητό είναι *απαραίτητο* για το γλυκό δεν σημαίνει ότι είναι και *αρκετό*· ίσως ο Νίκος χρειάζεται και κάτι άλλο (για παράδειγμα, να έχει διαβάσει τα μαθήματά του). Για να εξηγήσουμε με ακρίβεια τη διαφορά χρειαζόμαστε μια ακριβή γλώσσα για τις προτάσεις και για τους τρόπους με τους οποίους αυτές συνδυάζονται. Στα δύο επιχειρήματα θα επιστρέψουμε στο Παράδειγμα 3.15.

Ορισμός 3.1 (Πρόταση). Όταν χρησιμοποιούμε τη λέξη *πρόταση*, θα εννοούμε από δω και μπρος μια μη αντιφατική αποφαντική πρόταση. Δηλαδή μια πρόταση είναι μια δηλωτική έκφραση που είναι *είτε αληθής είτε ψευδής* (και όχι και τα δύο).

Για παράδειγμα έστω οι εκφράσεις

- «Πέντε και τρία μας κάνει οκτώ»
- «Τρία και δύο μας κάνει επτά»
- «Το πέντε και δύο είναι μεγάλο»
- «Αυτό το βιβλίο είναι μεγάλο»
- «Πήγες πουθενά χθες βράδυ;»

Οι δύο πρώτες είναι προτάσεις. Η τρίτη δεν είναι, γιατί δεν ξέρουμε ως προς τι είναι μεγάλο. Το ίδιο και για την τέταρτη. Ως προς την πέμπτη: δεν είναι αποφαντική.

Εκφράσεις όπως «$x > 3$» ή «ο x είναι πρώτος» δεν είναι προτάσεις: η αλήθειά τους εξαρτάται από την τιμή της μεταβλητής x. Γίνονται όμως προτάσεις μόλις δώσουμε στο x μια συγκεκριμένη τιμή (η «$5 > 3$» είναι αληθής πρόταση και η «$2 > 3$» ψευδής). Τέτοιες εκφράσεις θα τις μελετήσουμε στις Ενότητες 3.3 και 3.4. Ο χαρακτηρισμός «μη αντιφατική» στον ορισμό αποκλείει εκφράσεις όπως η «Αυτή η πρόταση είναι ψευδής»: αν ήταν αληθής, θα ήταν ψευδής, και αν ήταν ψευδής, θα ήταν

αληθής· δεν μπορεί λοιπόν να είναι ούτε το ένα ούτε το άλλο (θυμηθείτε το παράδοξο του Russell, Παρατήρηση 1.7). Από την άλλη, μια πρόταση δεν χρειάζεται να ξέρουμε *ποια* τιμή αλήθειας έχει: η «κάθε άρτιος αριθμός μεγαλύτερος του 2 είναι άθροισμα δύο πρώτων» (η εικασία του Goldbach) είναι πρόταση, αν και κανείς δεν γνωρίζει μέχρι σήμερα αν είναι αληθής ή ψευδής.

3.2 Προτασιακός Λογισμός

3.2.1 Η γλώσσα του προτασιακού λογισμού

Θα μελετήσουμε τη γλώσσα $\mathcal{L}$ του προτασιακού λογισμού. Η $\mathcal{L}$ είναι φτωχή σε σύγκριση με τη φυσική γλώσσα. Δεν έχει γράμματα με τα οποία φτιάχνονται λέξεις, αλλά μόνο σύμβολα-προτάσεις που με τη χρήση μερικών συνδετικών συμβόλων-λέξεων μας δίνουν νέες προτάσεις. Το σύνολο των συμβόλων της, που συμβολίζουμε με $\Sigma(\mathcal{L})$, έχει τα εξής στοιχεία:

α) $p_0, p_1, p_2, \ldots$ που λέγονται *προτασιακές μεταβλητές*,

β) $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ που λέγονται *σύνδεσμοι*, αντίστοιχα άρνηση, σύζευξη, διάζευξη, συνεπαγωγή, ισοδυναμία,

γ) $(\ ,\ )$ που λέγονται *παρενθέσεις*, αντίστοιχα αριστερή παρένθεση, δεξιά παρένθεση.

Το σύνολο των προτασιακών μεταβλητών συμβολίζουμε με $M(\Sigma)$. Οι σύνδεσμοι και οι παρενθέσεις λέγονται *λογικά σύμβολα*, γιατί, όπως θα δούμε, έχουν καθορισμένο νόημα, ενώ οι προτασιακές μεταβλητές μπορούν να ερμηνευθούν με διάφορους τρόπους.

Στην ερμηνεία που θα δούμε παρακάτω, οι σύνδεσμοι διαβάζονται ως εξής:

Σύνδεσμος	Όνομα	Διαβάζεται
$\neg$	άρνηση	«δεν», «όχι»
$\wedge$	σύζευξη	«και»
$\vee$	διάζευξη	«ή»
$\rightarrow$	συνεπαγωγή	«αν ... τότε ...»
$\leftrightarrow$	ισοδυναμία	«... αν και μόνον αν ...»

Στα παραδείγματα, αντί για $p_0, p_1, p_2, \ldots$ γράφουμε συχνά και $p, q, s, \ldots$ για τις προτασιακές μεταβλητές.

Ορισμός 3.2. *Έκφραση* της $\mathcal{L}$ ονομάζεται μια πεπερασμένη ακολουθία από σύμβολά της.

Με $E(\mathcal{L})$ συμβολίζουμε το σύνολο των εκφράσεων της $\mathcal{L}$. Βέβαια, μερικές μόνο από τις εκφράσεις της $\mathcal{L}$ θα παίξουν τον ρόλο που παίζουν οι προτάσεις σε μια φυσική γλώσσα. Αυτές περιγράφονται από τον παρακάτω ορισμό.

Ορισμός 3.3. Μια έκφραση φ λέγεται *προτασιακός τύπος* αν και μόνο αν

α) είναι προτασιακή μεταβλητή, ή

β) είναι της μορφής $(\neg\beta), (\beta \wedge \gamma), (\beta \vee \gamma), (\beta \rightarrow \gamma), (\beta \leftrightarrow \gamma)$ όπου β, γ προτασιακοί τύποι ήδη κατασκευασμένοι.

Να μερικοί προτασιακοί τύποι:

$$p_5, \quad p_0 \wedge p_3, \quad (\neg p_1) \vee (p_0 \rightarrow p_2).$$

Το σύνολο των προτασιακών τύπων της $\mathcal{L}$ συμβολίζεται με $T(\mathcal{L})$.

Σύμφωνα με τον ορισμό, κάθε σύνδεσμος φέρνει μαζί του ένα ζεύγος παρενθέσεων, οπότε, αυστηρά, οι δύο τελευταίοι τύποι γράφονται $(p_0 \wedge p_3)$ και $((\neg p_1) \vee (p_0 \to p_2))$. Για να διαβάζονται ευκολότερα οι τύποι, παραλείπουμε τις εξωτερικές παρενθέσεις, καθώς και τις παρενθέσεις γύρω από μια άρνηση: γράφουμε $\neg p_1 \vee (p_0 \to p_2)$ αντί για $((\neg p_1) \vee (p_0 \to p_2))$. Με αυτή τη σύμβαση το $\neg$ «δένει» μόνο με ό,τι ακολουθεί αμέσως· έτσι ο $\neg p \wedge q$ σημαίνει $((\neg p) \wedge q)$ και όχι $(\neg(p \wedge q))$.

Παράδειγμα 3.4. Ο ορισμός μάς λέει και *πώς* ελέγχουμε ότι μια έκφραση είναι προτασιακός τύπος: τη «χτίζουμε» βήμα-βήμα με τους κανόνες α) και β). Για την έκφραση $((\neg p_1) \vee (p_0 \to p_2))$:

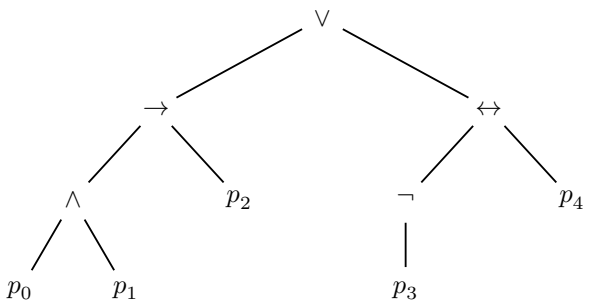
1. οι p_0, p_1, p_2 είναι τύποι, ως προτασιακές μεταβλητές (κανόνας α)·
2. η $(\neg p_1)$ είναι τύπος, από το βήμα 1 και τον κανόνα β)·
3. η $(p_0 \to p_2)$ είναι τύπος, από το βήμα 1 και τον κανόνα β)·
4. η $((\neg p_1) \vee (p_0 \to p_2))$ είναι τύπος, από τα βήματα 2, 3 και τον κανόνα β).

Αντίθετα, εκφράσεις όπως οι $p_0 \wedge \vee p_1$ και $)p_0($ δεν είναι προτασιακοί τύποι: ένας τύπος που δεν είναι προτασιακή μεταβλητή προκύπτει από τον κανόνα β), άρα γραμμένος αυστηρά αρχίζει με «(», ενώ αυτές οι εκφράσεις δεν είναι προτασιακές μεταβλητές και δεν αρχίζουν με «(». (Ούτε με τη σύμβαση για τις παρενθέσεις: η $p_0 \wedge \vee p_1$ θα έπρεπε να είναι η $(p_0 \wedge \gamma)$ με $\gamma = \vee p_1$, που δεν είναι τύπος, αφού δεν είναι μεταβλητή και δεν αρχίζει ούτε με «(» ούτε με «¬».)

Είναι προφανές ότι σε κάθε προτασιακό τύπο αντιστοιχεί ένα *δενδροδιάγραμμα*, ένα διάγραμμα δηλαδή που δείχνει πώς κατασκευάζεται ο τύπος αυτός από προτασιακές μεταβλητές με τη βοήθεια των λογικών συμβόλων, π.χ., στον προτασιακό τύπο

$$((p_0 \wedge p_1) \to p_2) \vee (\neg p_3 \leftrightarrow p_4)$$

αντιστοιχεί το διάγραμμα του Σχήματος 3.1.



Σχήμα 3.1. Το δενδροδιάγραμμα του τύπου $((p_0 \wedge p_1) \to p_2) \vee (\neg p_3 \leftrightarrow p_4)$.

Επειδή το $T(\mathcal{L})$ ορίσθηκε αναδρομικά, όταν θέλουμε να δείξουμε ότι όλοι οι προτασιακοί τύποι έχουν μια ιδιότητα, μπορούμε να το κάνουμε επαγωγικά όπως φαίνεται από το ακόλουθο θεώρημα.

Θεώρημα 3.5 (Αρχή της επαγωγής για το $T(\mathcal{L})$). *Αν $A \subseteq T(\mathcal{L})$ τέτοιο που*

1) $M(\Sigma) \subseteq A$,

2) για κάθε $\varphi, \psi \in A$ οι $(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi), (\varphi \leftrightarrow \psi)$ ανήκουν στο A,

τότε $A = T(\mathcal{L})$.

Το θεώρημα είναι το ανάλογο, για τους προτασιακούς τύπους, της αρχής της επαγωγής για τους φυσικούς (Θεώρημα 2.2): η 1) παίζει τον ρόλο της βάσης και η 2) τον ρόλο του επαγωγικού βήματος. Μάλιστα αποδεικνύεται με ισχυρή επαγωγή (Θεώρημα 2.8) στο πλήθος n των συνδέσμων ενός τύπου: ένας τύπος χωρίς συνδέσμους είναι προτασιακή μεταβλητή, άρα ανήκει στο A από την 1)· ένας τύπος

με $n > 0$ συνδέσμους είναι της μορφής $(\neg\beta)$ ή $(\beta \wedge \gamma)$ κ.λπ., όπου οι β, γ έχουν λιγότερους από n συνδέσμους, άρα ανήκουν στο A από την επαγωγική υπόθεση, οπότε και ο τύπος ανήκει στο A από την 2).

Παράδειγμα 3.6. Θα δείξουμε ότι κάθε προτασιακός τύπος (γραμμένος αυστηρά, με όλες τις παρενθέσεις) έχει το ίδιο πλήθος αριστερών και δεξιών παρενθέσεων. Έστω A το σύνολο των τύπων με αυτή την ιδιότητα. Μια προτασιακή μεταβλητή δεν έχει καθόλου παρενθέσεις, άρα $M(\Sigma) \subseteq A$. Αν $\varphi, \psi \in A$, με k αριστερές και k δεξιές παρενθέσεις ο φ και l αριστερές και l δεξιές ο ψ, τότε ο $(\neg\varphi)$ έχει $k+1$ αριστερές και $k+1$ δεξιές, και καθένας από τους $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$ έχει $k+l+1$ αριστερές και $k+l+1$ δεξιές. Άρα ικανοποιούνται οι 1) και 2) του θεωρήματος, οπότε $A = T(\mathcal{L})$.

3.2.2 Αποτιμήσεις και πίνακες αλήθειας

Μια *ερμηνεία* της $\mathcal{L}$ είναι η εξής:

α) Οι προτασιακές μεταβλητές αντιστοιχούν σε στοιχειώδεις προτάσεις της ελληνικής γλώσσας, προτάσεις δηλαδή που (i) δεν περιέχουν μικρότερες, και (ii) είναι αληθείς ή ψευδείς.

β) Οι σύνδεσμοι αντιστοιχούν στις φράσεις δεν, και, ή, αν...τότε..., αν και μόνον αν...

γ) Οι παρενθέσεις αντιστοιχούν σε σημεία στίξεως που υποδηλώνουν την αρχή και το τέλος μιας πρότασης.

Μ' αυτή την ερμηνεία οι προτασιακοί τύποι της $\mathcal{L}$ αντιστοιχούν στις προτάσεις της ελληνικής γλώσσας.

Ορισμός 3.7. *Αποτίμηση* καλείται μια συνάρτηση $u : M(\Sigma) \to \{A, \Psi\}$, όπου τα A, Ψ καλούνται *τιμές αλήθειας* και αντιστοιχούν στις έννοιες αληθής, ψευδής.

Η απόδοση μιας τιμής αλήθειας σε κάθε προτασιακό τύπο της $\mathcal{L}$, δηλαδή η εύρεση μιας συνάρτησης $\bar{u} : T(\mathcal{L}) \to \{A, \Psi\}$, όταν έχει δοθεί μια αποτίμηση u, γίνεται σύμφωνα με τους κανόνες-πίνακες παρακάτω. Οι πίνακες αυτοί καλούνται *πίνακες αλήθειας* και υποβάλλονται από την ερμηνεία της $\mathcal{L}$. Δοσμένης μιας αποτίμησης u, υπάρχει μία και μόνο επέκταση $\bar{u}$ της u που υπακούει στους κανόνες-πίνακες που ακολουθούν.

φ	ψ	$\neg\varphi$	$\varphi \wedge \psi$	$\varphi \vee \psi$	$\varphi \to \psi$	$\varphi \leftrightarrow \psi$
A	A	Ψ	A	A	A	A
A	Ψ	Ψ	Ψ	A	Ψ	Ψ
Ψ	A	A	Ψ	A	A	Ψ
Ψ	Ψ	A	Ψ	Ψ	A	A

Οι πίνακες της άρνησης, της σύζευξης και της διάζευξης συμφωνούν με τη διαίσθησή μας. (Η διάζευξη είναι *εγκλειστική*: η $\varphi \vee \psi$ είναι αληθής και όταν είναι αληθείς και οι δύο.) Η $\varphi \leftrightarrow \psi$ είναι αληθής ακριβώς όταν οι φ και ψ έχουν την *ίδια* τιμή αλήθειας. Τη συνεπαγωγή όμως πρέπει να την προσέξουμε:

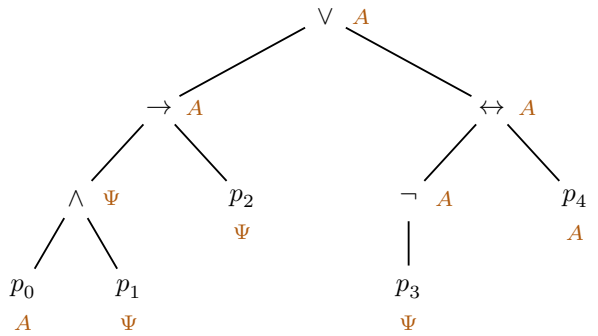
$\varphi \to \psi$ είναι ψευδής ακριβώς όταν η φ είναι αληθής και η ψ ψευδής.

Ειδικότερα, όταν η υπόθεση φ είναι ψευδής, η $\varphi \to \psi$ είναι αληθής, ό,τι κι αν ισχύει για την ψ· λέμε τότε ότι είναι *κενά αληθής*. Μπορούμε να σκεφτόμαστε τη συνεπαγωγή σαν μια υπόσχεση: η «Αν η Ανθή φάει το φαγητό της, θα πάρει γλυκό» παραβιάζεται μόνο αν η Ανθή φάει το φαγητό της και *δεν* πάρει γλυκό. Αν δεν το φάει, η υπόσχεση δεν έχει παραβιαστεί, όποια κι αν είναι η συνέχεια.

Η συνεπαγωγή $\varphi \to \psi$ εκφράζεται στα ελληνικά με πολλούς τρόπους: «αν φ, τότε ψ», «ψ, αν φ», «φ μόνο αν ψ», «η φ είναι *ικανή* (αρκετή) συνθήκη για την ψ», «η ψ είναι *αναγκαία* (απαραίτητη) συνθήκη για την φ», «για να ισχύει η φ, πρέπει να ισχύει η ψ». Έτσι, η πρόταση «για να πάρει γλυκό, ο Νίκος πρέπει να φάει το φαγητό του» της Ενότητας 3.1 είναι της μορφής $q \to p$, με q: «ο Νίκος παίρνει γλυκό» και p: «ο Νίκος τρώει το φαγητό του», και *όχι* της μορφής $p \to q$. Αντίστοιχα, η $\varphi \leftrightarrow \psi$ διαβάζεται και «η φ είναι αναγκαία και ικανή συνθήκη για την ψ».

Όταν έχουμε μια αποτίμηση u, για να βρούμε την $\bar{u}(\varphi)$ χρησιμοποιούμε το δενδροδιάγραμμα του φ. Προφανώς η $\bar{u}(\varphi)$ εξαρτάται μόνο από τις τιμές αλήθειας που η u αντιστοιχεί στις πεπερασμένες το πλήθος προτασιακές μεταβλητές που εμφανίζονται στο φ.

Παράδειγμα 3.8. Έστω u μια αποτίμηση με $u(p_0) = A$, $u(p_1) = \Psi$, $u(p_2) = \Psi$, $u(p_3) = \Psi$ και $u(p_4) = A$ (οι τιμές της στις υπόλοιπες μεταβλητές δεν παίζουν ρόλο). Υπολογίζουμε την τιμή του τύπου του Σχήματος 3.1 από τα φύλλα προς τη ρίζα (Σχήμα 3.2): $\bar{u}(p_0 \wedge p_1) = \Psi$, άρα $\bar{u}((p_0 \wedge p_1) \to p_2) = A$, αφού η υπόθεση είναι ψευδής· $\bar{u}(\neg p_3) = A$, άρα $\bar{u}(\neg p_3 \leftrightarrow p_4) = A$. Τελικά, ως διάζευξη δύο αληθών τύπων, ο τύπος παίρνει την τιμή A.



Σχήμα 3.2. Υπολογισμός της τιμής αλήθειας $\bar{u}(\varphi)$ στο δενδροδιάγραμμα του Σχήματος 3.1, από τα φύλλα προς τη ρίζα, για την αποτίμηση του Παραδείγματος 3.8.

3.2.3 Ταυτολογίες, ταυτολογική συνεπαγωγή και ισοδυναμία

Ορισμός 3.9. Έστω $T \subseteq T(\mathcal{L})$ και $\varphi \in T(\mathcal{L})$. Θα λέμε ότι:

α) η αποτίμηση u *ικανοποιεί* τον φ αν και μόνον αν $\bar{u}(\varphi) = A$ και η αποτίμηση u ικανοποιεί το T αν και μόνον αν η u ικανοποιεί κάθε στοιχείο του T.

β) το T είναι *ικανοποιήσιμο* αν και μόνον αν υπάρχει αποτίμηση που το ικανοποιεί.

γ) ο φ είναι *ταυτολογία* αν και μόνον αν κάθε αποτίμηση ικανοποιεί τον φ.

δ) ο φ είναι *αντίφαση* αν ο $\neg\varphi$ είναι ταυτολογία.

Παράδειγμα 3.10. Ο τύπος $p \vee \neg p$ είναι ταυτολογία και ο $p \wedge \neg p$ αντίφαση: σε κάθε αποτίμηση ακριβώς ένας από τους p, $\neg p$ είναι αληθής. Ο $p \to q$ δεν είναι ούτε ταυτολογία ούτε αντίφαση: η αποτίμηση με $u(p) = A$, $u(q) = \Psi$ τον κάνει ψευδή, ενώ κάθε αποτίμηση με $u(q) = A$ τον ικανοποιεί. Το σύνολο $\{p \to q,\ p,\ \neg q\}$ δεν είναι ικανοποιήσιμο, αφού μια αποτίμηση που ικανοποιεί τους p και $\neg q$ κάνει ψευδή τον $p \to q$.

Παρατηρούμε ότι ο φ είναι αντίφαση αν και μόνον αν *καμία* αποτίμηση δεν τον ικανοποιεί, δηλαδή αν και μόνον αν το $\{\varphi\}$ δεν είναι ικανοποιήσιμο. Επίσης, ο φ είναι ταυτολογία αν και μόνον αν ο $\neg\varphi$ είναι αντίφαση.

Ορισμός 3.11. Έστω $T \subseteq T(\mathcal{L})$ και $\varphi \in T(\mathcal{L})$. Θα λέμε ότι το T *ταυτολογικά συνεπάγεται* τον φ, και θα γράφουμε $T \vDash \varphi$, αν κάθε αποτίμηση που ικανοποιεί το T ικανοποιεί και τον φ. Προφανώς $T \vDash \varphi$ για κάθε $\varphi \in T$.

Η ταυτολογική συνεπαγωγή είναι ακριβώς η έννοια του *έγκυρου επιχειρήματος*: ένα επιχείρημα με προκείμενες τους τύπους του T και συμπέρασμα τον φ είναι έγκυρο αν το συμπέρασμα είναι αληθές *κάθε φορά* που είναι αληθείς όλες οι προκείμενες, δηλαδή αν $T \vDash \varphi$. Η εγκυρότητα εξαρτάται μόνο από τη *μορφή* του επιχειρήματος, όχι από το περιεχόμενο των προτάσεων· θα επανέλθουμε σε αυτό στην Ενότητα 3.5. Γράφουμε $T \not\vDash \varphi$ όταν δεν ισχύει $T \vDash \varphi$, δηλαδή όταν υπάρχει αποτίμηση που ικανοποιεί το T αλλά όχι τον φ.

Παρατηρήσεις:

i) $\emptyset \vDash \varphi$ αν και μόνο αν ο φ είναι ταυτολογία, αφού κάθε αποτίμηση ικανοποιεί το $\emptyset$· τότε γράφουμε και απλώς $\vDash \varphi$.

ii) Αν το T δεν είναι ικανοποιήσιμο, τότε προφανώς $T \vDash \varphi$, για κάθε φ.

iii) Αν $T = \{\psi\}$ και $T \vDash \varphi$, τότε γράφουμε $\psi \vDash \varphi$ και λέμε ότι ο ψ ταυτολογικά συνεπάγεται τον φ.

iv) Αν $\varphi \vDash \psi$ και $\psi \vDash \varphi$, τότε γράφουμε $\varphi \equiv \psi$ και λέμε ότι οι φ, ψ είναι *ταυτολογικά ισοδύναμοι.*

Ισοδύναμα, $\varphi \equiv \psi$ αν και μόνον αν οι φ και ψ έχουν τον *ίδιο* πίνακα αλήθειας, δηλαδή $\bar{u}(\varphi) = \bar{u}(\psi)$ για κάθε αποτίμηση u. Τότε μπορούμε να αντικαταστήσουμε τον έναν τύπο με τον άλλο, ακόμη και ως κομμάτι (υποτύπο) ενός μεγαλύτερου τύπου, χωρίς να αλλάξει η τιμή αλήθειας του μεγαλύτερου τύπου (αυτό αποδεικνύεται εύκολα με το Θεώρημα 3.5). Έτσι μπορούμε να «ξαναγράφουμε» τύπους σε απλούστερη μορφή, όπως θα δούμε στο Παράδειγμα 3.17. Τέλος, $\varphi \equiv \psi$ αν και μόνον αν ο $\varphi \leftrightarrow \psi$ είναι ταυτολογία, και $\varphi \vDash \psi$ αν και μόνον αν ο $\varphi \to \psi$ είναι ταυτολογία (Άσκηση 16).

Θα δούμε τώρα ένα αλγόριθμο με βάση τον οποίο αποφασίζουμε αν ένα πεπερασμένο σύνολο προτασιακών τύπων ταυτολογικά συνεπάγεται ένα προτασιακό τύπο ή όχι. Έστω λοιπόν ότι έχουμε ένα πεπερασμένο $T \subseteq T(\mathcal{L})$ και ένα τύπο φ. Μας ενδιαφέρουν μόνο οι τιμές αλήθειας που μια αποτίμηση αντιστοιχεί στις προτασιακές μεταβλητές που εμφανίζονται στα στοιχεία του $T \cup \{\varphi\}$. Έστω ότι n διαφορετικές προτασιακές μεταβλητές εμφανίζονται στα στοιχεία του $T \cup \{\varphi\}$. Κατασκευάζουμε ένα πίνακα αλήθειας με 2^n σειρές και m στήλες, όπου m ο αριθμός των διαφορετικών προτασιακών τύπων που εμφανίζονται στα δενδροδιαγράμματα των στοιχείων του $T \cup \{\varphi\}$. Αφού προσδιορίσουμε τις τιμές αλήθειας σ' όλες τις στήλες, εξετάζουμε τις σειρές για να δούμε αν κάθε αποτίμηση που ικανοποιεί το T ικανοποιεί και τον φ ή όχι.

Παράδειγμα 3.12. Θα δείξουμε ότι $(p \wedge q) \to s \vDash p \to (q \to s)$.

p	q	s	$p \wedge q$	$q \to s$	$(p \wedge q) \to s$	$p \to (q \to s)$
A	A	A	A	A	A	A
A	A	Ψ	A	Ψ	Ψ	Ψ
A	Ψ	A	Ψ	A	A	A
A	Ψ	Ψ	Ψ	A	A	A
Ψ	A	A	Ψ	A	A	A
Ψ	A	Ψ	Ψ	Ψ	A	A
Ψ	Ψ	A	Ψ	A	A	A
Ψ	Ψ	Ψ	Ψ	A	A	A

Από τις δύο τελευταίες στήλες βλέπουμε ότι ο $p \to (q \to s)$ παίρνει την τιμή αλήθειας A κάθε φορά που ο $(p \wedge q) \to s$ παίρνει την τιμή A, οπότε έχουμε το ζητούμενο.

Παράδειγμα 3.13. Θα δείξουμε ότι ο τύπος $p \to (q \to p)$ είναι ταυτολογία:

p	q	$q \to p$	$p \to (q \to p)$
A	A	A	A
A	Ψ	A	A
Ψ	A	Ψ	A
Ψ	Ψ	A	A

Από την τελευταία στήλη βλέπουμε ότι ο προτασιακός μας τύπος παίρνει πάντα την τιμή A. Άρα είναι ταυτολογία.

Παράδειγμα 3.14 (Modus ponens και modus tollens). Ο κανόνας «$p \to q$ και p, άρα q», γνωστός ως modus ponens, είναι έγκυρος, δηλαδή $\{p \to q,\ p\} \vDash q$: η μόνη γραμμή του πίνακα αλήθειας της συνεπαγωγής όπου είναι αληθείς και η $p \to q$ και η p είναι η πρώτη, με $u(p) = u(q) = A$, και εκεί η q είναι αληθής. Το ίδιο ισχύει και για τον κανόνα «$p \to q$ και $\neg q$, άρα $\neg p$», γνωστό ως modus tollens, δηλαδή $\{p \to q,\ \neg q\} \vDash \neg p$:

p	q	$p \to q$	$\neg q$	$\neg p$
A	A	A	Ψ	Ψ
A	Ψ	Ψ	A	Ψ
Ψ	A	A	Ψ	A
Ψ	Ψ	A	A	A

Η μόνη γραμμή όπου είναι αληθείς και η $p \to q$ και η $\neg q$ είναι η τελευταία, και εκεί η $\neg p$ είναι αληθής.

Παράδειγμα 3.15 (Τα επιχειρήματα της Ενότητας 3.1). Στο πρώτο επιχείρημα, έστω p: «η Ανθή τρώει το φαγητό της» και q: «η Ανθή παίρνει γλυκό». Οι προκείμενες είναι οι $p \to q$ και p, και το συμπέρασμα η q· το επιχείρημα είναι έγκυρο, από το modus ponens. Στο δεύτερο, έστω p: «ο Νίκος τρώει το φαγητό του» και q: «ο Νίκος παίρνει γλυκό». Όπως είδαμε μετά τους πίνακες αλήθειας, η πρώτη προκείμενη είναι η $q \to p$, η δεύτερη η p και το συμπέρασμα η q. Αυτό το επιχείρημα *δεν* είναι έγκυρο: $\{q \to p,\ p\} \not\vDash q$, αφού η αποτίμηση με $u(p) = A$ και $u(q) = \Psi$ ικανοποιεί και τις δύο προκείμενες αλλά όχι το συμπέρασμα. (Ο Νίκος έφαγε το φαγητό του, αλλά ίσως δεν πήρε γλυκό.)

Μερικές γνωστές ταυτολογικές ισοδυναμίες είναι οι εξής:

$$\begin{aligned}
\varphi \wedge \psi &\equiv \psi \wedge \varphi && \text{(αντιμεταθετικότητα)}\\
\varphi \vee \psi &\equiv \psi \vee \varphi && \text{(αντιμεταθετικότητα)}\\
\varphi \wedge (\psi \wedge \chi) &\equiv (\varphi \wedge \psi) \wedge \chi && \text{(προσεταιριστικότητα)}\\
\varphi \vee (\psi \vee \chi) &\equiv (\varphi \vee \psi) \vee \chi && \text{(προσεταιριστικότητα)}\\
\varphi \wedge (\psi \vee \chi) &\equiv (\varphi \wedge \psi) \vee (\varphi \wedge \chi) && \text{(επιμεριστικότητα)}\\
\varphi \vee (\psi \wedge \chi) &\equiv (\varphi \vee \psi) \wedge (\varphi \vee \chi) && \text{(επιμεριστικότητα)}\\
\neg(\neg\varphi) &\equiv \varphi && \text{(διπλή άρνηση)}\\
\neg(\varphi \wedge \psi) &\equiv \neg\varphi \vee \neg\psi && \text{(νόμος του De Morgan)}\\
\neg(\varphi \vee \psi) &\equiv \neg\varphi \wedge \neg\psi && \text{(νόμος του De Morgan)}\\
\varphi \vee \neg\varphi &\equiv A && \text{(νόμος της αποκλείσεως του τρίτου)}\\
(\varphi \to \psi) &\equiv (\neg\psi \to \neg\varphi) && \text{(αντιθετοαντιστροφή)}
\end{aligned}$$

Στον νόμο της αποκλείσεως του τρίτου, γράφοντας «$\equiv A$» εννοούμε ότι ο $\varphi \vee \neg\varphi$ είναι ταυτολογία (είναι ταυτολογικά ισοδύναμος με οποιαδήποτε ταυτολογία)· όμοια, γράφουμε $\varphi \equiv \Psi$ όταν ο

φ είναι αντίφαση. Με αυτή τη σύμβαση, μερικοί ακόμη χρήσιμοι νόμοι είναι οι εξής:

$$\begin{aligned}
\varphi \wedge \neg\varphi &\equiv \Psi && && \text{(νόμος της αντίφασης)}\\
\varphi \wedge A &\equiv \varphi, && \varphi \vee \Psi \equiv \varphi && \text{(ουδέτερα στοιχεία)}\\
\varphi \vee A &\equiv A, && \varphi \wedge \Psi \equiv \Psi &&\\
\varphi \to \psi &\equiv \neg\varphi \vee \psi && && \text{(η συνεπαγωγή ως διάζευξη)}\\
\neg(\varphi \to \psi) &\equiv \varphi \wedge \neg\psi && && \text{(άρνηση της συνεπαγωγής)}\\
\varphi \leftrightarrow \psi &\equiv (\varphi \to \psi) \wedge (\psi \to \varphi). && &&
\end{aligned}$$

Κάθε τέτοιος νόμος αποδεικνύεται με έναν πίνακα αλήθειας. Για παράδειγμα, για τον πρώτο νόμο του De Morgan:

φ	ψ	$\varphi \wedge \psi$	$\neg(\varphi \wedge \psi)$	$\neg\varphi$	$\neg\psi$	$\neg\varphi \vee \neg\psi$
A	A	A	Ψ	Ψ	Ψ	Ψ
A	Ψ	Ψ	A	Ψ	A	A
Ψ	A	Ψ	A	A	Ψ	A
Ψ	Ψ	Ψ	A	A	A	A

Η τέταρτη και η τελευταία στήλη είναι ίδιες. (Εδώ οι φ, ψ είναι τυχόντες τύποι, αλλά η τιμή των $\neg(\varphi \wedge \psi)$ και $\neg\varphi \vee \neg\psi$ εξαρτάται μόνο από τις τιμές των φ και ψ, άρα αρκεί να εξετάσουμε τους τέσσερις συνδυασμούς τους.)

Οι νόμοι αυτοί σας θυμίζουν κάτι: είναι ακριβώς οι νόμοι για την ένωση, την τομή και το συμπλήρωμα συνόλων της Ενότητας 1.1, με τα $\vee$, $\wedge$, $\neg$ στη θέση των $\cup$, $\cap$, $'$ και τα A, Ψ στη θέση των $\mathcal{U}$, $\emptyset$. Η εξήγηση θα δοθεί στην Ενότητα 3.3.

Ορισμός 3.16 (Αντίστροφη και αντιθετοαντίστροφη). Για τη συνεπαγωγή $\varphi \to \psi$, η συνεπαγωγή $\psi \to \varphi$ λέγεται *αντίστροφή* της και η $\neg\psi \to \neg\varphi$ *αντιθετοαντίστροφή* της.

Ο νόμος της αντιθετοαντιστροφής λέει ότι μια συνεπαγωγή είναι πάντα ταυτολογικά ισοδύναμη με την αντιθετοαντίστροφή της. Αντίθετα, *δεν* είναι ισοδύναμη με την αντίστροφή της:

p	q	$p \to q$	$q \to p$	$\neg q \to \neg p$
A	A	A	A	A
A	Ψ	Ψ	A	Ψ
Ψ	A	A	Ψ	A
Ψ	Ψ	A	A	A

Στη δεύτερη και την τρίτη γραμμή οι $p \to q$ και $q \to p$ παίρνουν διαφορετικές τιμές. Αυτό ακριβώς είναι το λάθος στο επιχείρημα για τον Νίκο: η προκείμενη ήταν η $q \to p$, αλλά τη χρησιμοποιήσαμε σαν να ήταν η αντίστροφή της $p \to q$.

Παράδειγμα 3.17. Με τους νόμους μπορούμε να απλοποιούμε τύπους χωρίς πίνακες αλήθειας:

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{(De Morgan)}\\
&\equiv \neg p \wedge (\neg\neg p \vee \neg q) && \text{(De Morgan)}\\
&\equiv \neg p \wedge (p \vee \neg q) && \text{(διπλή άρνηση)}\\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{(επιμεριστικότητα)}\\
&\equiv \Psi \vee (\neg p \wedge \neg q) && \text{(αντιμεταθετικότητα, νόμος της αντίφασης)}\\
&\equiv \neg p \wedge \neg q && \text{(αντιμεταθετικότητα, ουδέτερο στοιχείο).}
\end{aligned}$$

Σε κάθε βήμα εφαρμόζουμε έναν νόμο σε έναν *υποτύπο*, όπως εξηγήσαμε μετά τον ορισμό της $\equiv$.

3.2.4 Συναρτήσεις Boole και πλήρη σύνολα συνδέσμων

Ορισμός 3.18. Έστω $k \in \mathbb{N}$. *Συνάρτηση Boole* με k μεταβλητές λέγεται κάθε συνάρτηση $f : \{A, \Psi\}^k \to \{A, \Psi\}$.

Είναι προφανές ότι σε κάθε προτασιακό τύπο με $k+1$ διαφορετικές προτασιακές μεταβλητές αντιστοιχεί μια συνάρτηση Boole με $k+1$ μεταβλητές. Για το αντίστροφο έχουμε το επόμενο θεώρημα.

Θεώρημα 3.19. *Αν f μια συνάρτηση Boole με $k+1$ μεταβλητές, $k \in \mathbb{N}$, τότε υπάρχει προτασιακός τύπος φ στον οποίο εμφανίζονται μόνο οι $p_0, p_1, \dots, p_k$ τέτοιος που για κάθε αποτίμηση u να ισχύει: $\bar{u}(\varphi) = f(u(p_0), u(p_1), \dots, u(p_k))$, δηλαδή ο πίνακας αλήθειας του φ να περιγράφει πλήρως την f.*

Θα δείξουμε με ένα παράδειγμα πώς βρίσκεται ο τύπος φ. Έστω f η συνάρτηση Boole με τρεις μεταβλητές που ορίζεται ως εξής:

$$\begin{aligned} f(A,A,A) &= \Psi \quad f(\Psi,A,A) = A \\ f(A,A,\Psi) &= A \quad f(\Psi,A,\Psi) = \Psi \\ f(A,\Psi,A) &= A \quad f(\Psi,\Psi,A) = A \\ f(A,\Psi,\Psi) &= \Psi \quad f(\Psi,\Psi,\Psi) = \Psi \end{aligned}$$

Προσδιορίζουμε κατ' αρχήν τα στοιχεία του $\{A, \Psi\}^3$ στα οποία η f αντιστοιχεί την τιμή A. Αυτά είναι τα εξής: $(A, A, \Psi), (A, \Psi, A), (\Psi, A, A), (\Psi, \Psi, A)$. Σε κάθε μια απ' αυτές τις διατεταγμένες τριάδες αντιστοιχούμε ένα προτασιακό τύπο στον οποίο εμφανίζονται μόνο οι p_0, p_1, p_2 ως εξής: Αν το πρώτο στοιχείο της τριάδας είναι A, τότε παίρνουμε την p_0, ενώ αν είναι Ψ, παίρνουμε την $\neg p_0$. Όμοια για τα άλλα δύο στοιχεία της τριάδας και τελικά παίρνουμε τη σύζευξη των τριών στοιχειωδών προτασιακών τύπων που προκύπτουν. Έτσι στην (A, A, Ψ) αντιστοιχεί ο προτασιακός τύπος $p_0 \wedge p_1 \wedge \neg p_2$.

Η διάζευξη των προτασιακών τύπων που αντιστοιχούν στις τέσσερις διατεταγμένες τριάδες είναι ο προτασιακός τύπος

$$(p_0 \wedge p_1 \wedge \neg p_2) \vee (p_0 \wedge \neg p_1 \wedge p_2) \vee (\neg p_0 \wedge p_1 \wedge p_2) \vee (\neg p_0 \wedge \neg p_1 \wedge p_2)$$

του οποίου ο πίνακας αλήθειας περιγράφει πλήρως την f.

Η ίδια κατασκευή δουλεύει για κάθε συνάρτηση Boole, και αυτή είναι η απόδειξη του θεωρήματος: για κάθε $(t_0, \dots, t_k)$ με $f(t_0, \dots, t_k) = A$ σχηματίζουμε τη σύζευξη των p_i για τα i με $t_i = A$ και των $\neg p_i$ για τα i με $t_i = \Psi$· αυτή η σύζευξη είναι αληθής ακριβώς στις αποτιμήσεις που δίνουν στις $p_0, \dots, p_k$ τις τιμές $t_0, \dots, t_k$. Η διάζευξη όλων αυτών των συζεύξεων είναι λοιπόν αληθής ακριβώς όταν η f παίρνει την τιμή A. Μία μόνο περίπτωση θέλει προσοχή: αν η f δεν παίρνει *ποτέ* την τιμή A, δεν υπάρχει καμία σύζευξη να πάρουμε. Τότε την f την αντιπροσωπεύει, για παράδειγμα, η αντίφαση $p_0 \wedge \neg p_0 \wedge p_1 \wedge \dots \wedge p_k$.

Όταν ο πίνακας αλήθειας του φ περιγράφει πλήρως τη συνάρτηση Boole f θα λέμε ότι ο φ *αντιπροσωπεύει* την f. Συνήθως υπάρχουν περισσότεροι από ένας προτασιακοί τύποι που αντιπροσωπεύουν την ίδια συνάρτηση Boole f.

Ορισμός 3.20 (Κανονική διαζευκτική μορφή). Θα λέμε ότι ένας προτασιακός τύπος είναι σε *κανονική διαζευκτική μορφή* αν είναι της μορφής $\varphi_0 \vee \varphi_1 \vee \dots \vee \varphi_l$ όπου κάθε φ_i, $i = 0, 1, \dots, l$ είναι σύζευξη προτασιακών μεταβλητών ή αρνήσεων προτασιακών μεταβλητών.

Από την απόδειξη του παραπάνω θεωρήματος έπεται ότι κάθε προτασιακός τύπος είναι ταυτολογικά ισοδύναμος με ένα προτασιακό τύπο σε κανονική διαζευκτική μορφή.

Παράδειγμα 3.21 (Κανονική διαζευκτική μορφή με δύο τρόπους). Ας βρούμε έναν τύπο σε κανονική διαζευκτική μορφή ταυτολογικά ισοδύναμο με τον $\varphi = (p \to q) \wedge \neg(q \wedge r)$.

Πρώτος τρόπος: με τον πίνακα αλήθειας.

p	q	r	$p \to q$	$q \wedge r$	φ
A	A	A	A	A	Ψ
A	A	Ψ	A	Ψ	A
A	Ψ	A	Ψ	Ψ	Ψ
A	Ψ	Ψ	Ψ	Ψ	Ψ
Ψ	A	A	A	A	Ψ
Ψ	A	Ψ	A	Ψ	A
Ψ	Ψ	A	A	Ψ	A
Ψ	Ψ	Ψ	A	Ψ	A

Ο φ είναι αληθής στις γραμμές (A, A, Ψ), (Ψ, A, Ψ), (Ψ, Ψ, A) και (Ψ, Ψ, Ψ). Η κατασκευή της απόδειξης του Θεωρήματος 3.19 δίνει τον τύπο

$$(p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r).$$

Δεύτερος τρόπος: με τους νόμους (χωρίς πίνακα αλήθειας):

$$\begin{aligned}
\varphi &\equiv (\neg p \vee q) \wedge (\neg q \vee \neg r) && \text{(η συνεπαγωγή ως διάζευξη, De Morgan)}\\
&\equiv (\neg p \wedge (\neg q \vee \neg r)) \vee (q \wedge (\neg q \vee \neg r)) && \text{(αντιμεταθετικότητα, επιμεριστικότητα)}\\
&\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r) \vee (q \wedge \neg q) \vee (q \wedge \neg r) && \text{(επιμεριστικότητα)}\\
&\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r) \vee (q \wedge \neg r) && \text{(νόμος της αντίφασης, ουδέτερο στοιχείο).}
\end{aligned}$$

(Τις παρενθέσεις στις διαδοχικές διαζεύξεις τις παραλείπουμε, λόγω της προσεταιριστικότητας.) Και οι δύο τύποι είναι σε κανονική διαζευκτική μορφή και ισοδύναμοι με τον φ: η κανονική διαζευκτική μορφή ενός τύπου *δεν* είναι μοναδική.

Ο πρώτος τρόπος δουλεύει πάντα και δίνει μια κανονική διαζευκτική μορφή στην οποία κάθε σύζευξη περιέχει όλες τις μεταβλητές (μία σύζευξη για κάθε γραμμή όπου ο τύπος είναι αληθής)· για n μεταβλητές όμως ο πίνακας έχει 2^n γραμμές. Ο δεύτερος δίνει συνήθως συντομότερο τύπο και ακολουθεί πάντα τα ίδια βήματα: (1) απαλείφουμε τους $\leftrightarrow$ και $\to$ με τους νόμους $\varphi \leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi)$ και $\varphi \to \psi \equiv \neg\varphi \vee \psi$· (2) με τους νόμους του De Morgan και της διπλής άρνησης «σπρώχνουμε» τις αρνήσεις προς τα μέσα, μέχρι να εφαρμόζονται μόνο σε μεταβλητές· (3) με την επιμεριστικότητα μεταφέρουμε τις συζεύξεις μέσα στις διαζεύξεις· (4) απλοποιούμε, π.χ., διαγράφοντας τις συζεύξεις που περιέχουν μια μεταβλητή μαζί με την άρνησή της.

Ορισμός 3.22. Έστω $O \subseteq \{\wedge, \vee, \neg, \to, \leftrightarrow\}$. Θα λέμε ότι το O είναι *πλήρες* αν κάθε προτασιακός τύπος είναι ταυτολογικά ισοδύναμος με ένα προτασιακό τύπο που περιέχει μόνο συνδέσμους που ανήκουν στο O.

Όπως είδαμε το $\{\neg, \wedge, \vee\}$ είναι πλήρες.

Πράγματι, κάθε τύπος είναι ταυτολογικά ισοδύναμος με έναν τύπο σε κανονική διαζευκτική μορφή, ο οποίος περιέχει μόνο τους συνδέσμους $\neg$, $\wedge$, $\vee$. Το σύνολο αυτό μπορεί να μικρύνει ακόμη.

Πρόταση 3.23. *Το $\{\neg, \wedge\}$ είναι πλήρες.*

Απόδειξη. Αφού το $\{\neg, \wedge, \vee\}$ είναι πλήρες, αρκεί να δείξουμε ότι κάθε τύπος φ που περιέχει μόνο τους $\neg$, $\wedge$, $\vee$ είναι ταυτολογικά ισοδύναμος με έναν τύπο φ' που περιέχει μόνο τους $\neg$, $\wedge$. Αυτό το

δείχνουμε με το Θεώρημα 3.5. Αν ο φ είναι προτασιακή μεταβλητή, παίρνουμε $\varphi' = \varphi$. Αν $\varphi \equiv \varphi'$ και $\psi \equiv \psi'$, όπου οι φ', ψ' περιέχουν μόνο τους $\neg, \wedge$, τότε $\neg\varphi \equiv \neg\varphi'$, $\varphi \wedge \psi \equiv \varphi' \wedge \psi'$ και, από τους νόμους του De Morgan και της διπλής άρνησης,

$$\varphi \vee \psi \equiv \neg\neg(\varphi \vee \psi) \equiv \neg(\neg\varphi \wedge \neg\psi) \equiv \neg(\neg\varphi' \wedge \neg\psi'),$$

και οι τύποι στα δεξιά περιέχουν μόνο τους $\neg, \wedge$. □

Με τον ίδιο τρόπο αποδεικνύεται ότι και τα $\{\neg, \vee\}$ και $\{\neg, \to\}$ είναι πλήρη (Άσκηση 21). Δεν είναι όμως κάθε σύνολο συνδέσμων πλήρες.

Πρόταση 3.24. *Το $\{\wedge, \vee\}$ δεν είναι πλήρες.*

Απόδειξη. Έστω u η αποτίμηση με $u(p_i) = A$ για κάθε i. Δείχνουμε με το Θεώρημα 3.5 ότι κάθε τύπος φ που περιέχει μόνο τους συνδέσμους $\wedge$, $\vee$ έχει $\bar{u}(\varphi) = A$. Αν ο φ είναι προτασιακή μεταβλητή, $\bar{u}(\varphi) = u(\varphi) = A$. Αν $\bar{u}(\varphi) = \bar{u}(\psi) = A$, τότε και $\bar{u}(\varphi \wedge \psi) = \bar{u}(\varphi \vee \psi) = A$. Όμως $\bar{u}(\neg p_0) = \Psi$, άρα ο $\neg p_0$ δεν είναι ταυτολογικά ισοδύναμος με κανέναν τύπο που περιέχει μόνο τους $\wedge$, $\vee$. □

Το ίδιο επιχείρημα δείχνει ότι ούτε το $\{\wedge, \vee, \to, \leftrightarrow\}$ είναι πλήρες (αφού και $A \to A = A$, $A \leftrightarrow A = A$)· χωρίς την άρνηση δεν μπορούμε να εκφράσουμε την άρνηση.

Παρατήρηση 3.25 (Ένας σύνδεσμος αρκεί). Ας ορίσουμε έναν νέο σύνδεσμο, τον $\uparrow$ ("NAND", ή *σύνδεσμο του Sheffer*), με $\varphi \uparrow \psi$ να σημαίνει $\neg(\varphi \wedge \psi)$: ο $\varphi \uparrow \psi$ είναι ψευδής μόνο όταν και οι δύο τύποι είναι αληθείς. Τότε

$$\neg\varphi \equiv \varphi \uparrow \varphi \qquad \text{και} \qquad \varphi \wedge \psi \equiv (\varphi \uparrow \psi) \uparrow (\varphi \uparrow \psi),$$

οπότε, από την Πρόταση 3.23, κάθε τύπος είναι ταυτολογικά ισοδύναμος με έναν τύπο που περιέχει μόνο τον $\uparrow$. (Ο $\uparrow$ δεν ανήκει στα σύμβολα της $\mathcal{L}$, άρα αυτό βγαίνει έξω από τον παραπάνω ορισμό του πλήρους συνόλου.) Γι' αυτό ένα ψηφιακό κύκλωμα που υπολογίζει οποιαδήποτε συνάρτηση Boole μπορεί να κατασκευαστεί μόνο από πύλες NAND. (Βλ. και το Φροντιστήριο 5 για τον σύνδεσμο NOR.)

Ασκήσεις

1. ⁻ Ποιες από τις παρακάτω εκφράσεις είναι προτάσεις; Για όσες είναι, ποια είναι η τιμή αλήθειας τους (αν είναι γνωστή);

(α) «Ο 7 είναι πρώτος αριθμός.»

(β) «$x + 1 = 3$.»

(γ) «Κλείσε την πόρτα!»

(δ) «$2 + 2 = 5$.»

(ε) «Υπάρχουν άπειροι πρώτοι αριθμοί p τέτοιοι ώστε και ο $p + 2$ να είναι πρώτος.»

2. ⁻ Έστω οι προτάσεις p: «ο Γιάννης πέρασε τα Μαθηματικά» και q: «η Μαρία πέρασε τα Μαθηματικά».

(α) Γράψτε συμβολικά την «Και ο Γιάννης και η Μαρία πέρασαν τα Μαθηματικά».

(β) Γράψτε συμβολικά την «Αν ο Γιάννης πέρασε τα Μαθηματικά, τότε η Μαρία δεν τα πέρασε».

(γ) Διατυπώστε στα ελληνικά τους τύπους $p \vee q$ και $\neg(p \wedge q) \to q$.

(δ) Ξέρετε ότι αν ο Γιάννης πέρασε τα Μαθηματικά, τότε τα πέρασε και η Μαρία. Τι μπορείτε να συμπεράνετε αν ξέρετε ότι (i) η Μαρία πέρασε τα Μαθηματικά; (ii) η Μαρία δεν τα πέρασε;

3. Γράψτε καθεμία από τις παρακάτω προτάσεις στη μορφή «Αν ..., τότε ...». (Κάποιες από αυτές μπορεί να είναι ψευδείς· αυτό δεν έχει σημασία εδώ.)

(α) Για να χάσεις βάρος, πρέπει να γυμνάζεσαι.

(β) Για να χάσεις βάρος, αρκεί να γυμνάζεσαι.

(γ) Κάθε Αθηναίος είναι Έλληνας.

(δ) Είσαι Έλληνας μόνο αν είσαι Αθηναίος.

(ε) Το σύνολο των ρητών είναι υποσύνολο του συνόλου των πραγματικών αριθμών.

(στ) Ένας αριθμός είναι πρώτος αν δεν είναι άρτιος.

(ζ) Είτε η ομάδα μας θα κερδίσει τον τελικό, είτε δεν θα παίξει σε αυτόν.

4. ⋆ Δείξτε, με το Θεώρημα 3.5, ότι σε κάθε προτασιακό τύπο το πλήθος των εμφανίσεων προτασιακών μεταβλητών είναι κατά ένα μεγαλύτερο από το πλήθος των εμφανίσεων των συνδέσμων $\wedge, \vee, \to, \leftrightarrow$. (Για παράδειγμα, ο $(p_0 \wedge p_0) \to \neg p_1$ έχει 3 εμφανίσεις μεταβλητών και 2 τέτοιους συνδέσμους.)

5. ⁻ Είναι ο προτασιακός τύπος $((p \to q) \to p) \to p$ μια ταυτολογία; Σχεδιάστε το δενδροδιάγραμμά του και υπολογίστε πάνω σε αυτό την τιμή του για την αποτίμηση με $u(p) = \Psi$, $u(q) = A$, όπως στο Παράδειγμα 3.8.

6. ⁻ Δείξτε ότι $\{p \to q, \neg q \vee s\} \models \neg(p \wedge \neg s)$.

7. Δείξτε ότι $\models (\neg p \to \neg q) \to ((\neg p \to q) \to p)$, δηλαδή ότι ο προτασιακός τύπος είναι ταυτολογία.

8. ⁻ Δείξτε με πίνακα αλήθειας ότι ισχύει ο *υποθετικός συλλογισμός*: $\{p \to q,\ q \to r\} \models p \to r$.

9. Ποιος από τους παρακάτω δύο τύπους ταυτολογικά συνεπάγεται τον άλλο;

$$p \leftrightarrow (q \leftrightarrow s), \quad (p \wedge q) \to s$$

10. Σε ένα νησί κάθε κάτοικος είναι είτε *ιππότης*, που λέει πάντα την αλήθεια, είτε *απατεώνας*, που λέει πάντα ψέματα. Συναντάτε δύο κατοίκους. Ο πρώτος λέει: «Αν είμαστε ξαδέλφια, τότε είμαστε και οι δύο απατεώνες». Ο δεύτερος λέει: «Είμαστε ξαδέλφια ή είμαστε και οι δύο απατεώνες». Μπορεί να είναι και οι δύο ιππότες; Εξηγήστε πώς μπορείτε να βρείτε την απάντηση με πίνακα αλήθειας.

11. Ο Νίκος σάς λέει τι έφαγε χθες το απόγευμα: «Είχα ποπκόρν ή σταφίδες. Επίσης, αν είχα σάντουιτς με αγγούρι, τότε ήπια σόδα. Αλλά δεν ήπια ούτε σόδα ούτε τσάι.» Ξέρετε ότι ο Νίκος είναι ο χειρότερος ψεύτης του κόσμου και ό,τι λέει είναι ψευδές. Τι έφαγε και τι ήπιε τελικά ο Νίκος; Δικαιολογήστε την απάντησή σας γράφοντας τις δηλώσεις του με προτασιακές μεταβλητές, παίρνοντας τις αρνήσεις τους και συμπεραίνοντας από αυτές.

12. ⋆ Ο Χολμς έχει δύο κοστούμια, ένα μαύρο και ένα καρό. Πάντα φοράει είτε το καρό κοστούμι είτε σανδάλια. Όποτε φοράει το καρό κοστούμι μαζί με μοβ πουκάμισο, δεν φοράει ούτε γραβάτα ούτε παπιγιόν. Ποτέ δεν φοράει το καρό κοστούμι, εκτός αν φοράει επίσης είτε μοβ πουκάμισο είτε σανδάλια. Όποτε φοράει σανδάλια, φοράει και μοβ πουκάμισο. Χθες ο Χολμς φορούσε παπιγιόν. Τι άλλο φορούσε;

13. Θεωρήστε την πρόταση «Αν ο Όσκαρ τρώει κινέζικο φαγητό, τότε πίνει γάλα».

(α) Γράψτε την αντίστροφη πρόταση.

(β) Γράψτε την αντιθετοαντίστροφη πρόταση.

(γ) Μπορεί η αντιθετοαντίστροφη να είναι ψευδής; Αν ήταν, τι θα σας έλεγε αυτό;

(δ) Έστω ότι η αρχική πρόταση είναι αληθής και ότι ο Όσκαρ πίνει γάλα. Μπορείτε να συμπεράνετε κάτι για το αν τρώει κινέζικο φαγητό;

(ε) Έστω ότι η αρχική πρόταση είναι αληθής και ότι ο Όσκαρ δεν πίνει γάλα. Μπορείτε να συμπεράνετε κάτι για το αν τρώει κινέζικο φαγητό;

14. ⁻ Χρησιμοποιώντας τους νόμους του De Morgan και της διπλής άρνησης, απλοποιήστε τον τύπο $\neg(\neg p \vee q) \vee (\neg p \wedge q)$. Επιβεβαιώστε το αποτέλεσμα με πίνακα αλήθειας.

15. Απλοποιήστε τους παρακάτω τύπους, ώστε οι αρνήσεις να εμφανίζονται μόνο αμέσως πριν από προτασιακές μεταβλητές, χωρίς διπλές αρνήσεις και χωρίς $\rightarrow$. Γράψτε όλα τα βήματα και ελέγξτε τις απαντήσεις σας με πίνακες αλήθειας.

(α) $\neg((\neg p \wedge q) \vee \neg(r \vee \neg s))$.

(β) $\neg((\neg p \rightarrow \neg q) \wedge (\neg q \rightarrow r))$.

16. Έστω $\varphi, \psi, \varphi_1, \dots, \varphi_n$ προτασιακοί τύποι. Δείξτε ότι:

(α) $\varphi \equiv \psi$ αν και μόνον αν ο $\varphi \leftrightarrow \psi$ είναι ταυτολογία·

(β) $\varphi \models \psi$ αν και μόνον αν ο $\varphi \rightarrow \psi$ είναι ταυτολογία·

(γ) $\{\varphi_1, \dots, \varphi_n\} \models \psi$ αν και μόνον αν ο $(\varphi_1 \wedge \cdots \wedge \varphi_n) \rightarrow \psi$ είναι ταυτολογία.

17. Συναρτήσεις Boole και σύνδεσμοι.

(α) Πόσες συναρτήσεις Boole με k μεταβλητές υπάρχουν;

(β) Δείξτε ότι δύο τύποι στους οποίους εμφανίζονται μόνο οι $p_0, \dots, p_{k-1}$ αντιπροσωπεύουν την ίδια συνάρτηση Boole αν και μόνο αν είναι ταυτολογικά ισοδύναμοι. Συμπεράνετε, με το Θεώρημα 3.19, ότι υπάρχουν 2^{2^k} τέτοιοι τύποι ανά δύο μη ισοδύναμοι, αλλά όχι περισσότεροι.

(γ) Ένας σύνδεσμος δύο θέσεων (όπως οι $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ και ο $\uparrow$ της Παρατήρησης 3.25) καθορίζεται πλήρως από τον πίνακα αλήθειάς του. Πόσους διαφορετικούς συνδέσμους δύο θέσεων θα μπορούσαμε να ορίσουμε; Σε πόσους από αυτούς η τιμή εξαρτάται και από τις δύο μεταβλητές;

18. ⁻ Έστω η συνάρτηση Boole με τρεις μεταβλητές, που ορίζεται από:

$$\begin{aligned} g(A,A,A) &= \Psi \quad g(\Psi,A,A) = \Psi \\ g(A,A,\Psi) &= \Psi \quad g(\Psi,A,\Psi) = A \\ g(A,\Psi,A) &= \Psi \quad g(\Psi,\Psi,A) = \Psi \\ g(A,\Psi,\Psi) &= A \quad g(\Psi,\Psi,\Psi) = A \end{aligned}$$

Βρείτε ένα προτασιακό τύπο φ που αντιπροσωπεύει την g.

19. Βρείτε τύπο σε κανονική διαζευκτική μορφή που να είναι ταυτολογικά ισοδύναμος με τον $(p_0 \rightarrow p_1) \wedge (\neg p_0 \rightarrow p_2)$.

20. Βρείτε τύπο σε κανονική διαζευκτική μορφή ταυτολογικά ισοδύναμο με τον $(p \leftrightarrow q) \vee \neg r$, και με τους δύο τρόπους του Παραδείγματος 3.21.

21. Δείξτε ότι τα σύνολα $\{\neg, \vee\}$ και $\{\neg, \rightarrow\}$ είναι πλήρη σύνολα συνδέσμων (όπως στην απόδειξη της Πρότασης 3.23).

3.3 Πράξεις μεταξύ Συνόλων και Λογικοί σύνδεσμοι

Στην ενότητα αυτή, με τον όρο «πρόταση για τη μεταβλητή x» εννοούμε μια έκφραση που γίνεται πρόταση (με την έννοια του Ορισμού 3.1) μόλις δώσουμε τιμή στο x· στην Ενότητα 3.4 θα τις ονομάσουμε *κατηγορήματα*.

Στην Άλγεβρα μαθαίνουμε για μεταβλητές. Οι εξισώσεις είναι προτάσεις που αφορούν μεταβλητές. Για παράδειγμα η εξίσωση $x^2 + y^2 = 1$ όπου x, y φυσικοί, είναι μια πρόταση για τις μεταβλητές x και y. Ας υποθέσουμε ότι ρίχνουμε δύο κέρματα. Η πρόταση "Το αποτέλεσμα είναι το ίδιο και στα δύο κέρματα" προφανώς είναι μια πρόταση και η λέξη αποτέλεσμα παίζει το ρόλο μεταβλητής.

Το αποτέλεσμα αυτό μπορεί να είναι μια από τις τέσσερις δυνατότητες $ΚΚ, ΚΓ, ΓΚ, ΓΓ$ και μόνο όταν έχουμε $ΚΚ$ ή $ΓΓ$ γίνεται η παραπάνω πρόταση αληθής. Το *σύμπαν* για μια πρόταση ή μια συζήτηση είναι το σύνολο του οποίου τα στοιχεία μελετάμε. Στην προκειμένη περίπτωση με τα κέρματα το σύμπαν είναι το $\{ΚΚ, ΚΓ, ΓΚ, ΓΓ\}$. Αν έχουμε μια πρόταση για μια μεταβλητή x θα συμβολίζουμε την πρόταση με $P(x)$ όπου η μεταβλητή x θα τρέχει σε κάποιο σύμπαν.

Ορισμός 3.26 (Σύνολο αλήθειας). Το σύνολο όλων των τιμών του x στο σύμπαν μας που κάνουν την πρόταση $P(x)$ αληθή λέγεται το *σύνολο αλήθειας* για την P. Δηλαδή το σύνολο αλήθειας της P είναι το $\{x \in \mathcal{U} \,:\, P(x) \text{ αληθής}\}$.

Για παράδειγμα το σύνολο αλήθειας για την πρόταση "Το αποτέλεσμα είναι το ίδιο και στα δύο κέρματα", όταν ρίχνουμε δύο κέρματα, είναι το $\{ΚΚ, ΓΓ\}$.

Έστω ότι το σύμπαν μας είναι οι πραγματικοί αριθμοί, και έστω $P(x)$ η πρόταση "το τετράγωνο του x είναι 4". Τότε το σύνολο αλήθειας της $P(x)$ είναι το $\{-2, 2\}$. Αν τώρα το σύμπαν μας είναι το $\mathbb{Z} \times \mathbb{Z}$ και η πρόταση $P(x, y)$ είναι η "$x^2 + y^2 = 1$" τότε το σύνολο αλήθειας της $P(x, y)$ είναι το

$$\{(0, 1), (1, 0), (-1, 0), (0, -1)\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

Έστω τώρα δύο προτάσεις $P(x)$ και $Q(x)$ όπου το x τρέχει σε κάποιο σύμπαν $\mathcal{U}$. Θα λέμε ότι οι δύο προτάσεις είναι *ισοδύναμες* αν έχουν τα ίδια σύνολα αλήθειας, δηλαδή αν για κάθε $x \in \mathcal{U}$ η $P(x)$ είναι αληθής αν και μόνο αν η $Q(x)$ είναι αληθής. Για παράδειγμα, έστω ότι ρίχνουμε ένα κέρμα τρεις φορές και θέλουμε να βρούμε το σύνολο αλήθειας της πρότασης "Το αποτέλεσμα έχει ακριβώς 2 κορώνες" και το σύνολο αλήθειας της πρότασης "Το αποτέλεσμα έχει ακριβώς μια φορά γράμματα". Το σύμπαν είναι το

$$\{ΚΚΚ, ΚΚΓ, ΚΓΚ, ΚΓΓ, ΓΚΚ, ΓΚΓ, ΓΓΚ, ΓΓΓ\}.$$

Οι δύο παραπάνω προτάσεις έχουν το ίδιο σύνολο αλήθειας $\{ΚΚΓ, ΚΓΚ, ΓΚΚ\}$ και άρα είναι ισοδύναμες.

Αν $p(x)$ και $q(x)$ είναι προτάσεις για τη μεταβλητή x σε ένα σύμπαν $\mathcal{U}$ και P και Q τα σύνολα αλήθειας τους,

τότε μπορούμε να δείξουμε ότι:

1) το σύνολο $P \cap Q$ είναι το σύνολο αλήθειας της $p \wedge q$,

2) το σύνολο $P \cup Q$ είναι το σύνολο αλήθειας της $p \vee q$ και

3) το σύνολο P' είναι το σύνολο αλήθειας της $\neg p$.

Θα δείξουμε μόνο το 1). Τα μέρη 2) και 3) αποδεικνύονται παρόμοια. Πρώτα έστω $x \in P \cap Q$. Έχουμε $x \in P \cap Q \Rightarrow x \in P$ και $x \in Q \Rightarrow$ (το x κάνει την p αληθή) και (το x κάνει την q αληθή) $\Rightarrow$ το x κάνει την $p \wedge q$ αληθή $\Rightarrow$ το x ανήκει στο σύνολο αλήθειας της $p \wedge q$.

Έστω τώρα ότι το y ανήκει στο σύνολο αλήθειας της $p \wedge q$. Τότε το y κάνει αληθή την $p \wedge q$ και επομένως πρέπει να κάνει και την p και την q αληθή. Άρα $y \in P$ και $y \in Q$. Συνεπώς $y \in P \cap Q$.

Δείξαμε λοιπόν ότι το $P \cap Q$ και το σύνολο αλήθειας της $p \wedge q$ έχουν ακριβώς τα ίδια στοιχεία, άρα είναι το ίδιο σύνολο.

Συνοπτικά, αν οι p και q έχουν σύνολα αλήθειας P και Q σε ένα σύμπαν $\mathcal{U}$, τότε:

Λογική		Σύνολα
$p \wedge q$	$\longleftrightarrow$	$P \cap Q$
$p \vee q$	$\longleftrightarrow$	$P \cup Q$
$\neg p$	$\longleftrightarrow$	P'
$p \to q$	$\longleftrightarrow$	$P' \cup Q$
$p \leftrightarrow q$	$\longleftrightarrow$	$(P \cap Q) \cup (P' \cap Q')$

Για τη συνεπαγωγή: η $p(x) \to q(x)$ είναι αληθής αν και μόνον αν η $p(x)$ είναι ψευδής ή η $q(x)$ είναι αληθής, δηλαδή αν και μόνον αν $x \in P'$ ή $x \in Q$. Ειδικότερα, η $p(x) \to q(x)$ είναι αληθής για *κάθε* $x \in \mathcal{U}$ αν και μόνον αν $P' \cup Q = \mathcal{U}$, δηλαδή αν και μόνον αν $P \subseteq Q$ (Άσκηση 2): η συνεπαγωγή αντιστοιχεί στη σχέση του υποσυνόλου. Όμοια, η $p(x) \leftrightarrow q(x)$ είναι αληθής για κάθε x αν και μόνον αν $P = Q$, δηλαδή αν και μόνον αν οι p και q είναι ισοδύναμες με την έννοια που είδαμε παραπάνω. Γι' αυτό κάθε νόμος για τις πράξεις μεταξύ συνόλων «μεταφράζεται» σε έναν νόμο για τους λογικούς συνδέσμους, και αντίστροφα. Για παράδειγμα, ο νόμος του De Morgan $(P \cup Q)' = P' \cap Q'$ λέει ότι οι $\neg(p \vee q)$ και $\neg p \wedge \neg q$ έχουν το ίδιο σύνολο αλήθειας.

Παράδειγμα 3.27. Έστω σύμπαν το $\mathcal{U} = \{1, 2, \dots, 10\}$, $p(x)$: «ο x είναι άρτιος» και $q(x)$: «$x > 6$». Τότε $P = \{2, 4, 6, 8, 10\}$ και $Q = \{7, 8, 9, 10\}$, οπότε το σύνολο αλήθειας της $p \wedge q$ είναι το $\{8, 10\}$, της $\neg p$ το $\{1, 3, 5, 7, 9\}$ και της $p \to q$ το $P' \cup Q = \{1, 3, 5, 7, 8, 9, 10\}$. Η $p(x) \to q(x)$ είναι δηλαδή ψευδής ακριβώς για τους άρτιους που δεν είναι μεγαλύτεροι του 6, για $x = 2, 4, 6$.

Ασκήσεις

1. ⁻ Έστω σύμπαν το $\mathcal{U} = \{1, 2, \dots, 20\}$, $p(x)$: «ο x διαιρείται με το 3» και $q(x)$: «ο x είναι περιττός». Βρείτε τα σύνολα αλήθειας των $p \wedge q$, $p \vee \neg q$, $p \to q$ και $\neg(p \leftrightarrow q)$.

2. Έστω $p(x)$, $q(x)$ με σύνολα αλήθειας P και Q σε ένα σύμπαν $\mathcal{U}$.

   (α) Δείξτε ότι το σύνολο αλήθειας της $p \leftrightarrow q$ είναι το $(P \cap Q) \cup (P' \cap Q')$.

   (β) Δείξτε ότι η $p(x) \to q(x)$ είναι αληθής για κάθε $x \in \mathcal{U}$ αν και μόνον αν $P \subseteq Q$.

3. Ρίχνουμε δύο ζάρια, ένα κόκκινο και ένα μαύρο, οπότε το σύμπαν είναι το $\{1, \dots, 6\} \times \{1, \dots, 6\}$. Έστω $p(x)$: «το άθροισμα των δύο ενδείξεων είναι 7» και $q(x)$: «οι δύο ενδείξεις είναι διαφορετικές». Βρείτε τα σύνολα αλήθειας P και Q και τα πλήθη των στοιχείων τους, και ελέγξτε ότι η $p(x) \to q(x)$ είναι αληθής για κάθε x. Είναι αληθής για κάθε x και η $q(x) \to p(x)$;

3.4 Κατηγορηματική Λογική. Ποσοδείκτες

3.4.1 Κατηγορήματα και ποσοδείκτες

Στην Ενότητα 3.3 είδαμε εκφράσεις όπως η «$x^2 = 4$», που δεν είναι προτάσεις, γιατί η αλήθειά τους εξαρτάται από το x.

Ορισμός 3.28 (Κατηγόρημα). Ένα *κατηγόρημα* $P(x)$ είναι μια έκφραση με μια μεταβλητή x (ή περισσότερες: $P(x, y)$, $P(x, y, z)$, ...) η οποία γίνεται πρόταση μόλις δώσουμε στη μεταβλητή μια συγκεκριμένη τιμή από ένα σύνολο $\mathcal{U}$, το *σύμπαν* (ή *πεδίο ορισμού*) της μεταβλητής.

Για παράδειγμα, με σύμπαν το $\mathbb{R}$, η $P(x)$: «$x^2 = 4$» είναι κατηγόρημα· η $P(1)$ είναι ψευδής πρόταση και η $P(2)$ αληθής. Αυτό που στην Ενότητα 3.3 λέγαμε «πρόταση για τη μεταβλητή x» είναι λοιπόν ένα κατηγόρημα, και το σύνολο αλήθειάς του είναι το σύνολο των $x \in \mathcal{U}$ για τα οποία η $P(x)$ είναι αληθής. Ένας άλλος τρόπος να πάρουμε πρόταση από ένα κατηγόρημα, χωρίς να δώσουμε τιμή στη μεταβλητή, είναι να χρησιμοποιήσουμε έναν *ποσοδείκτη*.

Ας υποθέσουμε ότι θέλουμε να ορίσουμε τη σχέση $A \subseteq B$ για σύνολα A και B. Ξέρουμε ότι η παραπάνω σχέση λέει ότι κάθε x στο A είναι στο B. Μπορούμε να πούμε, για δοσμένο x στο σύμπαν μας, αν το x είναι στο A τότε είναι στο B, ή $x \in A \Rightarrow x \in B$. Αλλιώς, για όλα τα x, $x \in A \Rightarrow x \in B$.

Ορισμός 3.29 (Ποσοδείκτες). Γράφουμε $\forall x[x \in A \Rightarrow x \in B]$ αντί για την "για όλα τα x (στο σύμπαν) αν $x \in A$ τότε $x \in B$". Μια πρόταση του παραπάνω τύπου λέγεται *καθολική πρόταση* και το σύμβολο $\forall$ λέγεται *καθολικός ποσοδείκτης*. Άρα αν $a(x)$ είναι ένα κατηγόρημα, γράφουμε $\forall x\, a(x)$ για την πρόταση "για όλα τα x, $a(x)$". Επίσης γράφουμε $\exists x\, a(x)$ για την πρόταση "υπάρχει x τέτοιο ώστε $a(x)$". Το σύμβολο $\exists$ λέγεται *υπαρξιακός ποσοδείκτης* και λέμε ότι η $\exists x\, a(x)$ είναι μια *υπαρξιακή πρόταση*.

Συχνά ο ποσοδείκτης αναφέρεται μόνο στα στοιχεία ενός υποσυνόλου A του σύμπαντος. Γράφουμε

$$\forall x \in A\ P(x) \ \text{ αντί για } \ \forall x\,(x \in A \to P(x)), \qquad \exists x \in A\ P(x) \ \text{ αντί για } \ \exists x\,(x \in A \wedge P(x)).$$

Προσέξτε ότι στον καθολικό ποσοδείκτη ο περιορισμός γίνεται με $\to$, ενώ στον υπαρξιακό με $\wedge$: η $\exists x\,(x \in A \to P(x))$ θα ήταν αληθής μόλις υπάρχει έστω ένα $x \notin A$, ανεξάρτητα από την P. Με αυτόν τον συμβολισμό, ο ορισμός του υποσυνόλου γράφεται $\forall x \in A\ (x \in B)$. (Μέσα σε τύπους, τα σύμβολα $\Rightarrow$ και $\to$ χρησιμοποιούνται με την ίδια σημασία.)

Παράδειγμα 3.30. Ξαναγράψτε τις παρακάτω προτάσεις με συμβολικό τρόπο, χρησιμοποιώντας τα κάτωθι:

$$\begin{aligned} s(x) &= \text{“}x \text{ είναι άρτιος”} \\ t(x,y) &= \text{“}x = 2y\text{”} \\ p(x) &= \text{“ο } x \text{ είναι πρώτος”} \\ r(x) &= \text{“}x > 2\text{”} \end{aligned}$$

Το σύμπαν μας είναι οι φυσικοί αριθμοί.

α) Αν ο x είναι άρτιος τότε υπάρχει y τέτοιος ώστε $x = 2y$.

β) Υπάρχει πρώτος x τέτοιος ώστε $x = 2y$ για κάποιο y.

γ) Για όλους τους πρώτους x, αν $x > 2$ τότε ο x δεν είναι άρτιος.

Για την α) $\quad s(x) \to \exists y\, t(x,y)$

Για τη β) $\quad \exists x(p(x) \wedge \exists y\, t(x,y))$

Για τη γ) $\quad \forall x(p(x) \to (r(x) \to \neg s(x)))$

Στην α) η μεταβλητή y είναι *δεσμευμένη* από τον ποσοδείκτη $\exists y$, ενώ η x είναι *ελεύθερη*: η α) είναι ένα κατηγόρημα με μεταβλητή το x, όχι πρόταση, και γίνεται πρόταση μόλις δώσουμε τιμή στο x, ή αν τη γράψουμε $\forall x\,(s(x) \to \exists y\, t(x,y))$. Στις β) και γ) όλες οι μεταβλητές είναι δεσμευμένες, οπότε είναι προτάσεις.

Αν $a(x)$ είναι ένα κατηγόρημα, τότε η $\forall x\, a(x)$ είναι αληθής αν η $a(x)$ είναι αληθής για κάθε x στο σύμπαν. Η $\forall x\, a(x)$ είναι ψευδής αν υπάρχει ένα στοιχείο στο σύμπαν για το οποίο η a είναι ψευδής.

Η πρόταση $\exists x\, a(x)$ είναι αληθής αν η $a(x)$ είναι αληθής για τουλάχιστον ένα x στο σύμπαν. Η $\exists x\, a(x)$ είναι ψευδής αν η $a(x)$ είναι ψευδής για όλα τα x.

Με άλλα λόγια, αν P είναι το σύνολο αλήθειας της $a(x)$, τότε η $\forall x\, a(x)$ είναι αληθής αν και μόνον αν $P = \mathcal{U}$, και η $\exists x\, a(x)$ είναι αληθής αν και μόνον αν $P \neq \emptyset$. Για να δείξουμε ότι μια καθολική πρόταση είναι ψευδής αρκεί *ένα* στοιχείο για το οποίο η a είναι ψευδής (ένα *αντιπαράδειγμα*, Ενότητα 3.5), ενώ για να δείξουμε ότι είναι αληθής δεν αρκούν παραδείγματα: πρέπει να εξετάσουμε *κάθε* στοιχείο του σύμπαντος. Αντίθετα, για να δείξουμε ότι μια υπαρξιακή πρόταση είναι αληθής αρκεί ένα παράδειγμα.

Όταν το σύμπαν είναι πεπερασμένο, π.χ., $\mathcal{U} = \{u_1, u_2, \dots, u_n\}$, οι ποσοδείκτες είναι απλώς «μεγάλες» συζεύξεις και διαζεύξεις: η $\forall x\, a(x)$ σημαίνει $a(u_1) \wedge a(u_2) \wedge \cdots \wedge a(u_n)$ και η $\exists x\, a(x)$ σημαίνει $a(u_1) \vee a(u_2) \vee \cdots \vee a(u_n)$.

Παράδειγμα 3.31. Αν p, r και s είναι τα κατηγορήματα του προηγούμενου παραδείγματος, ποιες από τις παρακάτω είναι αληθείς και ποιες ψευδείς;

α) $\forall x\, p(x)$ γ) $\exists x(p(x) \wedge s(x))$

β) $\exists x\, p(x)$ δ) $\exists x(p(x) \wedge s(x) \wedge r(x))$

Η α) είναι ψευδής, γιατί, π.χ., ο $x = 4$ δεν είναι πρώτος. Η β) είναι αληθής, για παράδειγμα ο $x = 3$. Η γ) αληθής για παράδειγμα ο $x = 2$ και η δ) ψευδής, αφού ο μόνος άρτιος πρώτος είναι ο 2, που δεν είναι μεγαλύτερος του 2.

3.4.2 Πολλαπλοί ποσοδείκτες

Όταν ένα κατηγόρημα έχει περισσότερες μεταβλητές, χρειαζόμαστε έναν ποσοδείκτη για καθεμία, και τότε η *σειρά* των ποσοδεικτών έχει σημασία. Με σύμπαν τους φυσικούς, συγκρίνετε τις προτάσεις

$$\forall x\, \exists y\, (y > x) \qquad \text{και} \qquad \exists y\, \forall x\, (y > x).$$

Η πρώτη λέει «για κάθε x υπάρχει y μεγαλύτερος από τον x», και είναι αληθής. Η δεύτερη λέει «υπάρχει y μεγαλύτερος από *κάθε* x», και είναι ψευδής: ένας τέτοιος y θα έπρεπε να είναι μεγαλύτερος και από τον εαυτό του. Στην πρώτη πρόταση ο y επιτρέπεται να *εξαρτάται* από τον x (για $x = 5$ μπορούμε να πάρουμε $y = 6$, για $x = 100$ τον $y = 101$), ενώ στη δεύτερη ο y πρέπει να είναι ο *ίδιος* για όλους τους x. Αντίθετα, δύο διαδοχικοί ποσοδείκτες *του ίδιου* είδους μπορούν να εναλλαχθούν: οι $\forall x\, \forall y\, P(x, y)$ και $\forall y\, \forall x\, P(x, y)$ λένε το ίδιο πράγμα, και το ίδιο ισχύει για τις $\exists x\, \exists y\, P(x, y)$ και $\exists y\, \exists x\, P(x, y)$.

Πρόταση 3.32. $\forall x \in \mathbb{N}\, \exists y \in \mathbb{N}\, (y > x)$.

Απόδειξη. Έστω $x \in \mathbb{N}$ αυθαίρετος. Επιλέγουμε $y = x + 1$. Τότε $y \in \mathbb{N}$ και $y = x + 1 > x$. Αφού ο x ήταν αυθαίρετος, για κάθε $x \in \mathbb{N}$ υπάρχει $y \in \mathbb{N}$ με $y > x$. □

Η απόδειξη ακολουθεί ένα πρότυπο που αξίζει να θυμόμαστε: για να αποδείξουμε μια πρόταση της μορφής $\forall x\, \exists y\, P(x, y)$, «παγώνουμε» ένα αυθαίρετο x και *κατασκευάζουμε* ένα y (συνήθως ως συνάρτηση του x) για το οποίο η $P(x, y)$ είναι αληθής. Γενικότερα:

- για να αποδείξουμε μια πρόταση $\forall x\, P(x)$, παίρνουμε ένα αυθαίρετο στοιχείο x του σύμπαντος, για το οποίο δεν υποθέτουμε τίποτε άλλο, και δείχνουμε ότι ισχύει η $P(x)$·
- για να αποδείξουμε μια πρόταση $\exists x\, P(x)$, αρκεί να βρούμε (ή να δείξουμε ότι υπάρχει) *ένα* x για το οποίο η $P(x)$ είναι αληθής.

Παράδειγμα 3.33. Έστω σύμπαν οι φοιτητές ενός τμήματος και $G(x, y)$: «ο x γνωρίζει τον y». Τότε:

- $\forall x\, \exists y\, G(x, y)$: «καθένας γνωρίζει κάποιον»·
- $\exists y\, \forall x\, G(x, y)$: «υπάρχει κάποιος που τον γνωρίζουν όλοι»·
- $\exists x\, \forall y\, G(x, y)$: «υπάρχει κάποιος που γνωρίζει όλους»·

- $\forall y\, \exists x\, G(x, y)$: «καθένας είναι γνωστός σε κάποιον».

Η δεύτερη πρόταση συνεπάγεται την πρώτη (για κάθε x μπορούμε να πάρουμε ως y αυτόν που τον γνωρίζουν όλοι), και όμοια η τρίτη συνεπάγεται την τέταρτη. Το αντίστροφο όμως δεν ισχύει γενικά: μπορεί καθένας να γνωρίζει κάποιον, χωρίς να υπάρχει κάποιος που να τον γνωρίζουν όλοι.

3.4.3 Άρνηση ποσοδοτημένων προτάσεων

Θα λέμε ότι δύο προτάσεις με ποσοδείκτες είναι *ισοδύναμες*, και θα γράφουμε $\equiv$, αν, όποιο σύμπαν κι αν επιλέξουμε και όποια κατηγορήματα σε αυτό το σύμπαν κι αν βάλουμε στη θέση των συμβόλων (όπως το a) που εμφανίζονται σε αυτές, οι προτάσεις που προκύπτουν έχουν την ίδια τιμή αλήθειας.

Για παράδειγμα οι $\neg\forall x\, a(x)$ και $\exists x\, (\neg a(x))$ είναι ισοδύναμες.

Η ισοδυναμία αυτή, μαζί με τη «δυϊκή» της, είναι ο πιο χρήσιμος κανόνας για τους ποσοδείκτες.

Πρόταση 3.34 (Άρνηση ποσοδεικτών). *Για κάθε κατηγόρημα $a(x)$ ισχύει*

$$\neg\,\forall x\, a(x) \equiv \exists x\, \neg a(x), \qquad \neg\,\exists x\, a(x) \equiv \forall x\, \neg a(x).$$

Απόδειξη. Έστω P το σύνολο αλήθειας της $a(x)$ σε ένα σύμπαν $\mathcal{U}$· τότε το σύνολο αλήθειας της $\neg a(x)$ είναι το P'. Η $\neg\,\forall x\, a(x)$ είναι αληθής αν και μόνον αν η $\forall x\, a(x)$ είναι ψευδής, δηλαδή αν και μόνον αν $P \neq \mathcal{U}$, δηλαδή αν και μόνον αν $P' \neq \emptyset$, δηλαδή αν και μόνον αν η $\exists x\, \neg a(x)$ είναι αληθής. Όμοια, η $\neg\,\exists x\, a(x)$ είναι αληθής αν και μόνον αν $P = \emptyset$, δηλαδή αν και μόνον αν $P' = \mathcal{U}$, δηλαδή αν και μόνον αν η $\forall x\, \neg a(x)$ είναι αληθής. □

«Δεν ισχύει για όλα» σημαίνει «υπάρχει αντιπαράδειγμα», και «δεν υπάρχει κανένα» σημαίνει «για κάθε ένα δεν ισχύει». Σε ένα πεπερασμένο σύμπαν, όπου οι ποσοδείκτες είναι συζεύξεις και διαζεύξεις, η Πρόταση 3.34 είναι απλώς οι νόμοι του De Morgan: $\neg(a(u_1) \wedge \cdots \wedge a(u_n)) \equiv \neg a(u_1) \vee \cdots \vee \neg a(u_n)$. Προσοχή: η άρνηση της «όλοι οι φοιτητές πέρασαν το μάθημα» *δεν* είναι η «κανένας φοιτητής δεν πέρασε», δηλαδή η $\forall x\, \neg a(x)$, αλλά η «κάποιος φοιτητής δεν πέρασε», δηλαδή η $\exists x\, \neg a(x)$. Όμοια ισχύουν και για τους ποσοδείκτες με περιορισμό: $\neg\,\forall x \in A\, P(x) \equiv \exists x \in A\, \neg P(x)$ και $\neg\,\exists x \in A\, P(x) \equiv \forall x \in A\, \neg P(x)$.

Όταν έχουμε πολλούς ποσοδείκτες, η άρνηση «περνάει μέσα» έναν ποσοδείκτη τη φορά, αλλάζοντας το είδος του καθενός:

$$\neg\,\forall x\, \exists y\, P(x, y) \equiv \exists x\, \neg\,\exists y\, P(x, y) \equiv \exists x\, \forall y\, \neg P(x, y).$$

Όταν η άρνηση φτάσει στο «εσωτερικό», προτασιακό κομμάτι του τύπου, συνεχίζουμε με τους νόμους της Ενότητας 3.2.

Παράδειγμα 3.35. Η άρνηση της (αληθούς) πρότασης $\forall x\, \exists y\, (y > x)$, με σύμπαν το $\mathbb{N}$, είναι η $\exists x\, \forall y\, \neg(y > x)$, δηλαδή η $\exists x\, \forall y\, (y \leq x)$: «υπάρχει φυσικός μεγαλύτερος ή ίσος από κάθε φυσικό». Είναι, όπως πρέπει, ψευδής.

Παράδειγμα 3.36. Η πρόταση γ) του Παραδείγματος 3.30, $\forall x\, (p(x) \to (r(x) \to \neg s(x)))$, έχει άρνηση

$$\begin{aligned}
\neg\,\forall x\, (p(x) \to (r(x) \to \neg s(x))) &\equiv \exists x\, \neg(p(x) \to (r(x) \to \neg s(x))) \\
&\equiv \exists x\, (p(x) \wedge \neg(r(x) \to \neg s(x))) \\
&\equiv \exists x\, (p(x) \wedge (r(x) \wedge \neg\neg s(x))) \\
&\equiv \exists x\, (p(x) \wedge r(x) \wedge s(x)),
\end{aligned}$$

όπου χρησιμοποιήσαμε δύο φορές την ισοδυναμία $\neg(\varphi \to \psi) \equiv \varphi \wedge \neg\psi$ και στο τέλος τη διπλή άρνηση. Η άρνηση είναι λοιπόν η δ) του Παραδείγματος 3.31, «υπάρχει άρτιος πρώτος μεγαλύτερος του 2», που είναι ψευδής· αυτό συμφωνεί με το ότι η γ) είναι αληθής.

Ασκήσεις

1. Αν το σύμπαν μας είναι όλα τα πράγματα και

- $P(x)$ σημαίνει "ο x είναι πρόσωπο"
- $T(x)$ σημαίνει "ο x είναι χρόνος"
- $F(x, y)$ σημαίνει "μπορείς να κοροϊδέψεις τον x την y στιγμή"

γράψτε συμβολικά τις προτάσεις

α) Μπορείς να κοροϊδέψεις μερικούς ανθρώπους όλες τις φορές.

β) Μπορείς να κοροϊδέψεις όλους τους ανθρώπους μερικές φορές.

γ) Δεν μπορείς να κοροϊδέψεις όλους τους ανθρώπους όλες τις φορές.

2. Αν το σύμπαν μας είναι όλα τα πράγματα και

- $N(x)$ σημαίνει "ο x είναι αριθμός"
- $I(x)$ σημαίνει "ο x είναι ενδιαφέρων"
- $L(x, y)$ σημαίνει "ο x είναι μικρότερος του y"

και 0 είναι μια σταθερά και σημαίνει το μηδέν, γράψτε συμβολικά τις παρακάτω προτάσεις:

α) Το μηδέν είναι μικρότερο κάθε αριθμού.

β) Αν κάθε αριθμός είναι ενδιαφέρων, τότε και το μηδέν είναι ενδιαφέρον.

γ) Κανένας αριθμός δεν είναι μικρότερος του μηδενός.

δ) Δεν υπάρχει αριθμός τέτοιος ώστε όλοι οι αριθμοί να είναι μικρότεροι από αυτόν.

ε) Δεν υπάρχει αριθμός τέτοιος ώστε κανένας αριθμός να μην είναι μικρότερος από αυτόν.

3. ⁻ Με σύμπαν το $\mathbb{R}$, είναι αληθής η πρόταση $\forall x \, \exists y \, (xy = 1)$; Γράψτε την άρνησή της, ώστε να μην υπάρχει $\neg$ μπροστά από ποσοδείκτη, και αποφασίστε αν η άρνηση είναι αληθής.

4. ⁻ Σύμπαν: οι φοιτητές μιας τάξης, και $G(x, y)$: «ο x γνωρίζει τον y». Γράψτε συμβολικά την πρόταση «Υπάρχει φοιτητής που γνωρίζει όλους τους άλλους». Στη συνέχεια γράψτε την άρνησή της, συμβολικά και στα ελληνικά.

5. Σύμπαν: όλοι οι άνθρωποι, $C(x)$: «ο x είναι κωμικός» και $F(x)$: «ο x είναι αστείος». Διατυπώστε στα ελληνικά τις προτάσεις:

(α) $\forall x \, (C(x) \to F(x))$

(β) $\forall x \, (C(x) \wedge F(x))$

(γ) $\exists x \, (C(x) \to F(x))$

(δ) $\exists x \, (C(x) \wedge F(x))$

Γιατί η (γ) είναι μια πολύ «αδύναμη» πρόταση;

6. Σύμπαν: οι μαθητές μιας τάξης, $C(x)$: «ο x έχει γάτα», $D(x)$: «ο x έχει σκύλο» και $F(x)$: «ο x έχει κουνάβι». Γράψτε συμβολικά τις προτάσεις:

(α) Ένας μαθητής της τάξης έχει γάτα, σκύλο και κουνάβι.

(β) Όλοι οι μαθητές της τάξης έχουν γάτα, σκύλο ή κουνάβι.

(γ) Κάποιος μαθητής της τάξης έχει γάτα και κουνάβι, αλλά όχι σκύλο.

(δ) Κανένας μαθητής της τάξης δεν έχει γάτα, σκύλο και κουνάβι.

(ε) Για καθένα από τα τρία ζώα (γάτα, σκύλο, κουνάβι) υπάρχει ένας μαθητής της τάξης που το έχει.

7. Ξαναγράψτε τις παρακάτω προτάσεις ώστε οι αρνήσεις να εμφανίζονται μόνο αμέσως πριν από κατηγορήματα (δηλαδή να μην υπάρχει άρνηση μπροστά από ποσοδείκτη ή από έκφραση με συνδέσμους):

(α) $\neg\,\exists y\,\exists x\,P(x,y)$

(β) $\neg\,\forall x\,\exists y\,P(x,y)$

(γ) $\neg\,\exists y\,(Q(y)\wedge\forall x\,\neg R(x,y))$

(δ) $\neg\,\exists y\,(\exists x\,R(x,y)\vee\forall x\,S(x,y))$

(ε) $\neg\,\exists y\,(\forall x\,\exists z\,T(x,y,z)\vee\exists x\,\forall z\,U(x,y,z))$

8. Γράψτε συμβολικά τις παρακάτω προτάσεις για ακεραίους, χρησιμοποιώντας τα κατηγορήματα $E(x)$: «ο x είναι άρτιος», $O(x)$: «ο x είναι περιττός», $P(x)$: «ο x είναι πρώτος» και τη σχέση $<$.

(α) Κανένας αριθμός δεν είναι ταυτόχρονα άρτιος και περιττός.

(β) Ο επόμενος κάθε άρτιου αριθμού είναι περιττός.

(γ) Υπάρχει πρώτος αριθμός που είναι άρτιος.

(δ) Ανάμεσα σε δύο οποιουσδήποτε διαφορετικούς αριθμούς υπάρχει ένας τρίτος.

(ε) Δεν υπάρχει αριθμός ανάμεσα σε έναν αριθμό και τον επόμενό του.

Ποιες από αυτές είναι αληθείς για τους ακεραίους;

9. Για καθεμία από τις παρακάτω προτάσεις, βρείτε ένα σύμπαν (ένα σύνολο αριθμών) στο οποίο είναι αληθής και ένα στο οποίο είναι ψευδής.

(α) $\forall x\,\exists y\,(y^2=x)$.

(β) $\forall x\,\forall y\,(x<y\to\exists z\,(x<z\wedge z<y))$.

(γ) ⋆ $\exists x\,\forall y\,\forall z\,(y<z\to(y\le x\wedge x\le z))$.

10. Έστω $P(x)$ ένα κατηγόρημα σε ένα *μη κενό* σύμπαν, για το οποίο η $\forall x\,P(x)$ είναι αληθής. Είναι αληθής και η $\exists x\,P(x)$; Με άλλα λόγια, είναι η $\forall x\,P(x)\to\exists x\,P(x)$ πάντα αληθής; Είναι πάντα αληθής η αντίστροφή της; Τι συμβαίνει αν το σύμπαν είναι κενό;

11. Γράψτε την άρνηση καθεμίας από τις παρακάτω προτάσεις όσο πιο απλά μπορείτε (όχι απλώς «δεν ισχύει ότι ...»).

(α) Κάθε ακέραιος είναι άρτιος ή περιττός.

(β) Για κάθε ακέραιο n, αν ο n είναι πρώτος, τότε ο $n+3$ δεν είναι πρώτος.

(γ) $\forall x\,\forall y\,(x<y\vee y<x)$.

(δ) $\exists x\,P(x)\to\forall y\,P(y)$.

Είναι αληθής η πρόταση (β);

12. ⁻ Έστω $P(x)$ ένα κατηγόρημα. Τι πρέπει να κάνετε για να αποδείξετε ότι

(α) η $\forall x\,P(x)$ είναι αληθής;

(β) η $\forall x\,P(x)$ είναι ψευδής;

(γ) η $\exists x\,P(x)$ είναι αληθής;

(δ) η $\exists x\, P(x)$ είναι ψευδής;

Σε κάθε μία από τις περιπτώσεις, αρκεί ένα παράδειγμα, ή χρειάζεται ένα επιχείρημα για *κάθε* στοιχείο του σύμπαντος;

3.5 Τι είναι απόδειξη

3.5.1 Επιχειρήματα και αποδείξεις

Στα μαθηματικά χρησιμοποιούμε αποδείξεις. Μια *απόδειξη* μιας πρότασης είναι ένα επιχείρημα που μας πείθει ότι η πρόταση είναι αληθής. Η λογική ασχολείται με το τι κάνει τα επιχειρήματα πειστικά.

Ορισμός 3.37 (Επιχείρημα, εγκυρότητα, ορθότητα). Ένα *επιχείρημα* είναι μια ακολουθία προτάσεων· οι πρώτες λέγονται *προκείμενες* και η τελευταία *συμπέρασμα*. Το επιχείρημα είναι *έγκυρο* αν το συμπέρασμα είναι αληθές κάθε φορά που όλες οι προκείμενες είναι αληθείς, και *ορθό* αν είναι έγκυρο *και* όλες οι προκείμενες είναι πράγματι αληθείς.

Για επιχειρήματα του προτασιακού λογισμού, η εγκυρότητα είναι ακριβώς η ταυτολογική συνεπαγωγή $T \models \varphi$ της Ενότητας 3.2. Η εγκυρότητα αφορά μόνο τη *μορφή* του επιχειρήματος, ενώ η ορθότητα και το περιεχόμενό του. Για παράδειγμα, το επιχείρημα

Αν ο 2 είναι πρώτος, τότε ο 2 είναι περιττός.
Ο 2 είναι πρώτος.

Άρα, ο 2 είναι περιττός.

είναι έγκυρο (είναι της μορφής modus ponens, Παράδειγμα 3.14), αλλά δεν είναι ορθό, αφού η πρώτη προκείμενη είναι ψευδής· γι' αυτό και το συμπέρασμά του μπορεί να είναι ψευδές. Το συμπέρασμα ενός ορθού επιχειρήματος, αντίθετα, είναι πάντα αληθές. Μια *απόδειξη* μιας πρότασης είναι λοιπόν ένα ορθό επιχείρημα με συμπέρασμα αυτή την πρόταση.

Μια τεχνική που έχουμε χρησιμοποιήσει και χρησιμοποιείται, είναι η *αρχή της ευθείας απόδειξης*. Αυτή η αρχή είναι ένα παράδειγμα ενός αποδεικτικού κανόνα, και μας λέει ότι αν γνωρίζουμε ότι η p είναι αληθής και ότι η $p \to s$ είναι αληθής, μπορούμε να συμπεράνουμε ότι η s είναι αληθής επίσης (πρόκειται για τον κανόνα modus ponens του Παραδείγματος 3.14). Θα λέμε ότι μια μαθηματική πρόταση είναι *θεώρημα* αν έχουμε μια απόδειξη ότι είναι αληθής. Ένα μαθηματικό θεώρημα είναι μια πρόταση του τύπου:

$$\text{Αν } p, q, \ldots \text{ τότε } t, \quad p \wedge q \wedge \cdots \to t.$$

Οι προτάσεις $p, q, \ldots$ λέγονται *υποθέσεις* και η πρόταση t λέγεται το *συμπέρασμα*.

3.5.2 Ευθεία απόδειξη και αντιπαράδειγμα

Ορισμός 3.38 (Ευθεία απόδειξη). Μια ευθεία απόδειξη του συμπεράσματος από τις υποθέσεις είναι μια πεπερασμένη ακολουθία $s_1, s_2, s_3, \ldots, s_N$ από προτάσεις, όπου $s_N = t$, το συμπέρασμα, και κάθε s_i, $i = 1, \ldots, N$ είναι ή υπόθεση ή κάποια παραδεδεγμένη αλήθεια (αξίωμα ή γνωστό αποδειγμένο θεώρημα) ή είναι το αποτέλεσμα εφαρμογής της αρχής της ευθείας απόδειξης σε δύο προηγούμενες προτάσεις δηλαδή σε s_j και $s_j \to s_i$ με $j < i$ (δηλαδή τόσο η s_j όσο και η $s_j \to s_i$ βρίσκονται ανάμεσα στις $s_1, \ldots, s_{i-1}$).

Στην πράξη δεν γράφουμε τις αποδείξεις ως ακολουθίες τύπων, αλλά σε φυσική γλώσσα· κάθε βήμα όμως πρέπει να προκύπτει από τα προηγούμενα με τον παραπάνω τρόπο. Στα παραδείγματα που ακολουθούν χρησιμοποιούμε τους εξής ορισμούς: ένας ακέραιος n είναι *άρτιος* αν $n = 2k$ για

κάποιο $k \in \mathbb{Z}$, και *περιττός* αν $n = 2k+1$ για κάποιο $k \in \mathbb{Z}$. Δεχόμαστε ως γνωστό ότι κάθε ακέραιος είναι είτε άρτιος είτε περιττός, και όχι και τα δύο.

Παράδειγμα 3.39 (Ευθεία απόδειξη). Θα δείξουμε ότι το άθροισμα δύο άρτιων ακεραίων είναι άρτιος. Έστω m, n άρτιοι. Τότε $m = 2k$ και $n = 2\lambda$ για κάποιους $k, \lambda \in \mathbb{Z}$. Άρα

$$m + n = 2k + 2\lambda = 2(k + \lambda),$$

και αφού $k + \lambda \in \mathbb{Z}$, ο $m+n$ είναι άρτιος. Κάθε βήμα προκύπτει άμεσα από τα προηγούμενα και από τον ορισμό του άρτιου: πρόκειται για μια τυπική ευθεία απόδειξη. Με τον ίδιο τρόπο δείχνουμε ότι το γινόμενο δύο περιττών είναι περιττός: αν $m = 2k+1$ και $n = 2\lambda+1$, τότε $mn = 4k\lambda+2k+2\lambda+1 = 2(2k\lambda + k + \lambda) + 1$.

Ορισμός 3.40 (Αντιπαράδειγμα). Ένα *αντιπαράδειγμα* σε μια πρόταση για κάποιο σύμπαν είναι ένα στοιχείο του σύμπαντος για το οποίο η πρόταση είναι ψευδής. Δηλαδή, για μια πρόταση της μορφής $\forall x\, P(x)$, ένα αντιπαράδειγμα είναι ένα στοιχείο x του σύμπαντος για το οποίο η $P(x)$ είναι ψευδής.

Παράδειγμα 3.41. Είναι η πρόταση "Αν n φυσικός τότε το n είναι το άθροισμα δύο τετραγώνων", θεώρημα των φυσικών αριθμών;

Η απάντηση είναι όχι γιατί για τον 6 δεν υπάρχουν φυσικοί a και b τέτοιοι που $6 = a^2 + b^2$. Άρα το 6 είναι ένα αντιπαράδειγμα και επομένως η πρόταση δεν είναι θεώρημα.

Από την Πρόταση 3.34, η άρνηση της $\forall x\, P(x)$ είναι η $\exists x\, \neg P(x)$: ένα *μόνο* αντιπαράδειγμα αρκεί για να δείξουμε ότι μια καθολική πρόταση είναι ψευδής. Αντίθετα, όσα παραδείγματα κι αν βρούμε, δεν αποδεικνύουν μια καθολική πρόταση. Για παράδειγμα, ο $n^2 + n + 41$ είναι πρώτος για $n = 0, 1, 2, \dots, 39$, αλλά όχι για κάθε φυσικό n: για $n = 40$ έχουμε $40^2 + 40 + 41 = 41^2$.

3.5.3 Αντιθετοαντιστροφή και απαγωγή σε άτοπο

Έχουμε όμως και μη-ευθείες αποδείξεις. Αν θέλουμε να αποδείξουμε ένα θεώρημα που όπως αναφέραμε παραπάνω είναι μια υποθετική πρόταση $s \to t$, όπου $s = p \wedge q \wedge \cdots$, και $p, q, \dots$ είναι οι υποθέσεις, τότε η *αρχή της απόδειξης με αντιθετοαντιστροφή* μας λέει ότι αρκεί να αποδείξουμε την πρόταση $\neg t \to \neg s$. Μπορούμε να εφαρμόσουμε την παραπάνω αρχή γιατί οι προτάσεις $s \to t$ και $\neg t \to \neg s$ είναι ταυτολογικά ισοδύναμες.

Παράδειγμα 3.42 (Απόδειξη με αντιθετοαντιστροφή). Θα δείξουμε ότι για κάθε ακέραιο n: αν ο n^2 είναι άρτιος, τότε ο n είναι άρτιος. Ευθέως αυτό είναι δύσκολο, αφού από την $n^2 = 2k$ δεν προκύπτει άμεσα κάτι για τον n. Η αντιθετοαντίστροφη πρόταση είναι «αν ο n δεν είναι άρτιος, τότε ο n^2 δεν είναι άρτιος», δηλαδή «αν ο n είναι περιττός, τότε ο n^2 είναι περιττός», και αυτή αποδεικνύεται εύκολα: αν $n = 2k + 1$ με $k \in \mathbb{Z}$, τότε

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

και αφού $2k^2 + 2k \in \mathbb{Z}$, ο n^2 είναι περιττός. Άρα ισχύει και η αρχική πρόταση.

Η αντιθετοαντιστροφή βοηθά συνήθως όταν η υπόθεση ή το συμπέρασμα περιέχουν άρνηση, ή όταν η άρνηση του συμπεράσματος δίνει κάτι πιο «χειροπιαστό» (εδώ: «περιττός», δηλαδή $n = 2k + 1$, αντί για «όχι άρτιος»).

Έστω τώρα ότι θέλουμε να αποδείξουμε το θεώρημα $s \to t$. Η *αρχή της απόδειξης μέσω αντίφασης* μας λέει ότι από την s και την $(s \wedge \neg t) \to \neg s$ μπορούμε να συμπεράνουμε την t. Συνεπώς η αρχή της απόδειξης μέσω αντίφασης λέει ότι, αν υποθέτοντας ότι η s και η άρνηση της t είναι αληθείς, μπορέσουμε να δείξουμε την άρνηση της s αληθή, τότε η s συνεπάγεται την t.

Τέλος, αν θέλουμε να αποδείξουμε το θεώρημα $s \to t$, η *αρχή της απαγωγής σε άτοπο* μας λέει ότι από την s και την $(s \wedge \neg t) \to (r \wedge \neg r)$ μπορούμε να συμπεράνουμε την t. Δηλαδή, αν υποθέτοντας την s και την άρνηση της t αληθείς, μπορέσουμε να έχουμε μια αντίφαση, τότε η s συνεπάγεται την t.

Οι δύο τελευταίες αρχές είναι παραλλαγές της ίδιας ιδέας, και στην πράξη τις λέμε και τις δύο *απαγωγή σε άτοπο*: για να αποδείξουμε την t (υπό τις υποθέσεις s), υποθέτουμε την $\neg t$ και καταλήγουμε σε μια αντίφαση, δηλαδή σε μια πρόταση της μορφής $r \wedge \neg r$ ή στην άρνηση μιας υπόθεσης. Η αντίφαση δείχνει ότι η υπόθεση $\neg t$ ήταν λάθος, άρα ισχύει η t. Ότι όλες αυτές οι αρχές είναι έγκυρες ελέγχεται με πίνακες αλήθειας (Άσκηση 3).

Παράδειγμα 3.43. Δείξτε ότι ο $\sqrt{2}$ είναι άρρητος αριθμός. Ας υποθέσουμε ότι ο $\sqrt{2}$ είναι ρητός και μάλιστα $\sqrt{2} = \dfrac{m}{n}$ όπου m, n θετικοί ακέραιοι και πρώτοι προς αλλήλους (δηλαδή δεν έχουν άλλο κοινό διαιρέτη εκτός από τη μονάδα).[1] Τότε $m^2 = 2n^2$. Άρα ο m διαιρείται από το 2 (ο m^2 είναι άρτιος, άρα και ο m, από το Παράδειγμα 3.42) και επομένως $m = 2k$, για $k \in \mathbb{N}$, και $m^2 = 2n^2 \Rightarrow 4k^2 = 2n^2 \Rightarrow 2k^2 = n^2 \Rightarrow n$ είναι πολλαπλάσιο του 2 (για τον ίδιο λόγο), δηλαδή $n = 2\lambda$. Μα τότε οι m, n έχουν κοινό διαιρέτη το 2, άτοπο γιατί υποθέσαμε ότι είναι πρώτοι προς αλλήλους. Επομένως ο $\sqrt{2}$ είναι άρρητος.

Ποια τεχνική να διαλέξουμε; Δεν υπάρχει γενικός κανόνας, αλλά μερικές ενδείξεις είναι οι εξής:

- *ευθεία απόδειξη*, όταν η υπόθεση «ανοίγει τον δρόμο» φυσικά προς το συμπέρασμα, π.χ., με αλγεβρικούς υπολογισμούς (Παράδειγμα 3.39)·
- *αντιθετοαντιστροφή*, όταν η άρνηση του συμπεράσματος είναι πιο «χειροπιαστή» από το ίδιο το συμπέρασμα (Παράδειγμα 3.42)·
- *απαγωγή σε άτοπο*, όταν δεν βλέπουμε πώς να ξεκινήσουμε ευθέως, ιδίως για ισχυρισμούς της μορφής «δεν υπάρχει ...», όπως ο $\sqrt{2} \notin \mathbb{Q}$, που λέει ότι δεν υπάρχουν m, n με $\sqrt{2} = m/n$ (Παράδειγμα 3.43).

Η εμπειρία, δηλαδή οι ασκήσεις, βοηθά να αναγνωρίζουμε ποια τεχνική ταιριάζει καλύτερα.

Ασκήσεις

1. ⁻ Ποια από τα παρακάτω επιχειρήματα είναι έγκυρα, και ποια ορθά;

(α) «Αν βρέχει, ο δρόμος είναι βρεγμένος. Ο δρόμος είναι βρεγμένος. Άρα βρέχει.»

(β) «Κάθε πρώτος αριθμός είναι περιττός. Ο 2 είναι πρώτος. Άρα ο 2 είναι περιττός.»

(γ) «Αν ο 7 είναι άρτιος, τότε ο 8 είναι περιττός. Ο 8 δεν είναι περιττός. Άρα ο 7 δεν είναι άρτιος.»

2. Ένας φίλος σας έδειξε μια «απόδειξη» ότι $1 = 3$: «Ισχυρίζομαι ότι $1 = 3$. Μπορούμε να κάνουμε οτιδήποτε στο ένα μέλος μιας εξίσωσης, αρκεί να το κάνουμε και στο άλλο. Αφαιρούμε λοιπόν το 2 και από τα δύο μέλη: $-1 = 1$. Υψώνουμε στο τετράγωνο και τα δύο μέλη: $1 = 1$. Και όλοι συμφωνούμε ότι αυτό είναι αληθές.» Είναι έγκυρο αυτό το επιχείρημα; Αποδεικνύει ότι $1 = 3$; Εξηγήστε, χρησιμοποιώντας όσα ξέρετε για τις προτάσεις και τις συνεπαγωγές.

3. ⁻ Δείξτε με πίνακες αλήθειας ότι οι αρχές απόδειξης αυτής της ενότητας είναι έγκυρες, δηλαδή ότι:

(α) $\{s,\ (s \wedge \neg t) \to \neg s\} \vDash t$ (απόδειξη μέσω αντίφασης)·

(β) $\{s,\ (s \wedge \neg t) \to (r \wedge \neg r)\} \vDash t$ (απαγωγή σε άτοπο)·

[1] Μια τέτοια γραφή υπάρχει πάντα: από όλες τις γραφές $\sqrt{2} = m/n$ με m, n θετικούς ακεραίους παίρνουμε αυτήν με τον μικρότερο n, που υπάρχει από την αρχή της καλής διάταξης (Αξίωμα 2.1). Αν οι m, n είχαν κοινό διαιρέτη $d > 1$, η $\sqrt{2} = (m/d)/(n/d)$ θα ήταν γραφή με μικρότερο παρονομαστή.

(γ) $(s \wedge \neg t) \to (r \wedge \neg r) \equiv s \to t$.

4. Θεωρήστε την πρόταση «Για κάθε φυσικό αριθμό n, αν ο n είναι πρώτος, τότε ο n είναι *μονήρης*». (Δεν χρειάζεται να ξέρετε τι σημαίνει «μονήρης», μόνο ότι είναι μια ιδιότητα που έχουν κάποιοι αριθμοί και άλλοι όχι.)

(α) Γράψτε την αντίστροφη και την αντιθετοαντίστροφη πρόταση, διευκρινίζοντας ποια είναι ποια.

(β) Γράψτε την άρνηση της αρχικής πρότασης. Τι θα έπρεπε να δείξετε για να αποδείξετε ότι η πρόταση είναι ψευδής;

(γ) Είναι γνωστό ότι ο 8 είναι μονήρης. Τι μπορείτε να συμπεράνετε για την αλήθεια της αρχικής πρότασης, της αντίστροφής της και της αντιθετοαντίστροφής της;

(δ) Υποθέτοντας ότι η αρχική πρόταση είναι αληθής, τι μπορείτε να πείτε για τη σχέση ανάμεσα στο σύνολο P των πρώτων αριθμών και το σύνολο S των μονήρων αριθμών;

(ε) Θέλετε να αποδείξετε την αρχική πρόταση. Γράψτε την *αρχή* και το *τέλος* της απόδειξης (μόνο τις πρώτες και τις τελευταίες γραμμές, ώστε να φαίνεται η λογική της δομή) αν την αποδεικνύατε (i) ευθέως, (ii) με αντιθετοαντιστροφή, (iii) με απαγωγή σε άτοπο.

5. Αποφασίστε ποιες από τις παρακάτω είναι έγκυρες αποδείξεις της πρότασης «Αν ο ab είναι άρτιος, τότε ο a ή ο b είναι άρτιος», για ακεραίους a, b. (Όλη η άλγεβρα είναι σωστή· ελέγξτε μόνο τη λογική δομή.)

(α) Έστω ότι οι a και b είναι περιττοί, δηλαδή $a = 2k + 1$ και $b = 2m + 1$. Τότε $ab = (2k+1)(2m+1) = 4km + 2k + 2m + 1 = 2(2km + k + m) + 1$. Άρα ο ab είναι περιττός.

(β) Έστω ότι ο a ή ο b είναι άρτιος, π.χ., ο $a = 2k$. Τότε $ab = (2k)b = 2(kb)$. Άρα ο ab είναι άρτιος.

(γ) Έστω ότι ο ab είναι άρτιος αλλά οι a και b είναι περιττοί: $ab = 2n$, $a = 2k+1$, $b = 2j+1$. Τότε $2n = 4kj + 2k + 2j + 1$, άρα $n = 2kj + k + j + \frac{1}{2}$. Όμως ο $2kj + k + j$ είναι ακέραιος, οπότε ο ακέραιος n θα ήταν ίσος με έναν μη ακέραιο, άτοπο.

(δ) Έστω ότι ο $ab = 2n$ είναι άρτιος και ο $a = 2k+1$ περιττός. Τότε $2n = (2k+1)b = 2kb+b$, άρα $b = 2(n - kb)$. Άρα ο b είναι άρτιος.

6. Για ακεραίους a, b γράφουμε $a \mid b$ («ο a διαιρεί τον b») αν $b = ka$ για κάποιον ακέραιο k (όπως στο Παράδειγμα 1.44, τώρα για όλους τους ακεραίους). Για καθεμία από τις παρακάτω προτάσεις, αποφασίστε αν είναι αληθής ή ψευδής· αν είναι αληθής, αποδείξτε την ευθέως από τον ορισμό, και αν είναι ψευδής, δώστε ένα αντιπαράδειγμα.

(α) Το άθροισμα τριών διαδοχικών ακεραίων διαιρείται με το 3.

(β) Αναγκαία συνθήκη για να διαιρείται ένας ακέραιος με το 6 είναι να διαιρείται με το 2.

(γ) Για όλους τους ακεραίους a, b: αν $a \mid b$, τότε $a^2 \mid b^2$.

(δ) Για όλους τους ακεραίους a, b, c: αν $a \mid (b + c)$, τότε $a \mid b$ ή $a \mid c$.

(ε) Για όλους τους ακεραίους a, b, c: αν $a \mid bc$, τότε $a \mid b$ ή $a \mid c$.

7. Αποδείξτε ότι για πραγματικούς αριθμούς x, y ισχύει $x = y$ αν και μόνον αν $xy = \dfrac{(x+y)^2}{4}$. (Πρέπει να αποδείξετε δύο συνεπαγωγές.)

8. Θεωρήστε την πρόταση «Για όλους τους ακεραίους a και b, αν ο $a + b$ είναι άρτιος, τότε οι a και b είναι άρτιοι».

(α) Γράψτε την αντιθετοαντίστροφη, την αντίστροφη και την άρνηση της πρότασης.

(β) Ποιες από τις τέσσερις προτάσεις (την αρχική, την αντιθετοαντίστροφη, την αντίστροφη και την άρνηση) είναι αληθείς; Αποδείξτε τις απαντήσεις σας.

9. ⁻ Αποδείξτε ότι αν ο n είναι ακέραιος και ο n^3 είναι περιττός, τότε ο n είναι περιττός. Ποια τεχνική χρησιμοποιήσατε;

10. Θεωρήστε την πρόταση «Για όλα τα πεπερασμένα σύνολα A και B, αν $A \subseteq B$, τότε $|A| \leq |B|$».

(α) Γράψτε την αντιθετοαντίστροφη πρόταση και χρησιμοποιήστε τη για να εξηγήσετε γιατί η αρχική πρόταση είναι αληθής.

(β) Γράψτε την αντίστροφη της αρχικής πρότασης και εξηγήστε γιατί είναι ψευδής.

11. Αποδείξτε ότι ο $\sqrt{3}$ είναι άρρητος. (*Υπόδειξη:* δείξτε πρώτα, με αντιθετοαντιστροφή, ότι αν ο 3 διαιρεί τον n^2 τότε ο 3 διαιρεί τον n· γράψτε $n = 3k + 1$ ή $n = 3k + 2$.)

12. Αποδείξτε ότι η εξίσωση $x^2 = 4y + 3$ δεν έχει ακέραιες λύσεις.

13. Έχουμε γραμματόσημα των 5 και των 8 λεπτών. Στην Ενότητα 2.1 είδαμε ότι κάθε ποσό $n \geq 28$ πληρώνεται ακριβώς (Πρόταση 2.12 και Άσκηση 13).

(α) Ποια ποσά μπορούμε να πληρώσουμε αν χρησιμοποιήσουμε *άρτιο* πλήθος γραμματοσήμων και από τα δύο είδη; Αποδείξτε την απάντησή σας.

(β) Πληρώσαμε ένα άρτιο ποσό. Αποδείξτε ότι από τουλάχιστον ένα από τα δύο είδη χρησιμοποιήσαμε άρτιο πλήθος γραμματοσήμων. Ποια τεχνική απόδειξης ταιριάζει καλύτερα εδώ;

(γ) Πληρώσαμε ακριβώς 72 λεπτά. Αποδείξτε ότι χρησιμοποιήσαμε τουλάχιστον 6 γραμματόσημα από το ένα από τα δύο είδη.

3.6 Δυο θεμελιώδεις τεχνικές απόδειξης

3.6.1 Η αρχή του περιστερώνα

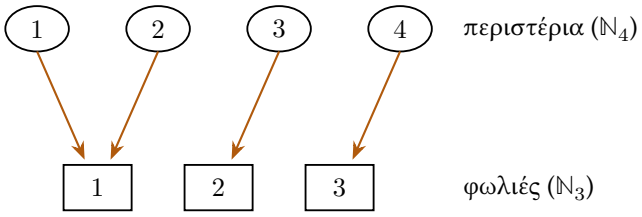
Έχουμε γνωρίσει μια ισχυρή τεχνική για να αποδεικνύουμε καθολικές προτάσεις για τους φυσικούς αριθμούς, την αρχή της επαγωγής (Ενότητα 2.1). Μια άλλη αρχή είναι η *αρχή του περιστερώνα* που διατυπώνεται ως εξής:

Θεώρημα 3.44 (Αρχή του περιστερώνα). *Δεν υπάρχει ενριπτική συνάρτηση από το αρχικό τμήμα $\mathbb{N}_{k+1}$ στο $\mathbb{N}_k$, για κανένα $k \geq 1$.*

Με άλλα λόγια μας λέει ότι (επειδή το τμήμα $\mathbb{N}_{k+1}$ έχει περισσότερα στοιχεία από το $\mathbb{N}_k$ για κάθε $k \geq 1$) για οποιαδήποτε απεικόνιση f από το $\mathbb{N}_{k+1}$ στο $\mathbb{N}_k$ θα υπάρχει τουλάχιστον ένα στοιχείο του $\mathbb{N}_k$ στο οποίο απεικονίζονται τουλάχιστον δύο στοιχεία του $\mathbb{N}_{k+1}$ μέσω της f.

Η ονομασία προέρχεται από την εξής εικόνα: αν $k+1$ περιστέρια μπουν σε k φωλιές, τότε κάποια φωλιά θα πάρει τουλάχιστον δύο περιστέρια (Σχήμα 3.3). Η αρχή του περιστερώνα αποδεικνύεται με επαγωγή στο k (Άσκηση 1). Από αυτήν προκύπτει εύκολα μια γενικότερη μορφή, για οποιαδήποτε πεπερασμένα σύνολα.

Πόρισμα 3.45. *Αν A, B είναι πεπερασμένα σύνολα με $|A| > |B|$, τότε δεν υπάρχει ενριπτική συνάρτηση $f : A \to B$. Ισοδύναμα, για κάθε συνάρτηση $f : A \to B$ υπάρχουν $a \neq a'$ στο A με $f(a) = f(a')$.*



Σχήμα 3.3. Τέσσερα περιστέρια σε τρεις φωλιές: κάθε συνάρτηση $\mathbb{N}_4 \to \mathbb{N}_3$ στέλνει δύο στοιχεία στην ίδια τιμή (εδώ τα 1 και 2 στη φωλιά 1), άρα δεν είναι ενριπτική.

Απόδειξη. Έστω $|A| = n$ και $|B| = k$, οπότε $n > k$. Αν $k = 0$, τότε $B = \emptyset$ και, αφού $A \neq \emptyset$, δεν υπάρχει καμία συνάρτηση $A \to B$. Έστω λοιπόν $k \geq 1$, και ας υποθέσουμε ότι υπάρχει ενριπτική $f : A \to B$. Υπάρχουν αμφιμονοσήμαντες συναρτήσεις $g : \mathbb{N}_n \to A$ και $h : B \to \mathbb{N}_k$. Η σύνθεση $h \circ f \circ g : \mathbb{N}_n \to \mathbb{N}_k$ είναι ενριπτική, ως σύνθεση ενριπτικών (Πρόταση 1.58), άρα και ο περιορισμός της στο $\mathbb{N}_{k+1} \subseteq \mathbb{N}_n$ (αφού $k + 1 \leq n$) είναι ενριπτική συνάρτηση $\mathbb{N}_{k+1} \to \mathbb{N}_k$, που αντιφάσκει με το Θεώρημα 3.44. □

Παρατήρηση 3.46. Η αρχή του περιστερώνα δίνει και μια δεύτερη απόδειξη ότι το $\mathbb{N}$ είναι άπειρο σύνολο (Ενότητα 2.2, μετά τον Ορισμό 2.16): αν υπήρχε αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to \mathbb{N}_k$, ο περιορισμός της στο $\mathbb{N}_{k+1} \subseteq \mathbb{N}$ θα ήταν ενριπτική συνάρτηση $\mathbb{N}_{k+1} \to \mathbb{N}_k$. (Εκεί χρησιμοποιήσαμε μια άλλη ιδέα: ότι κάθε πεπερασμένο, μη κενό σύνολο φυσικών έχει μέγιστο στοιχείο.) Με τον ίδιο τρόπο, αν $\mathbb{N}_n \sim \mathbb{N}_k$ με $n > k \geq 1$, ο περιορισμός μιας αμφιμονοσήμαντης $\mathbb{N}_n \to \mathbb{N}_k$ στο $\mathbb{N}_{k+1}$ θα ήταν ενριπτική συνάρτηση $\mathbb{N}_{k+1} \to \mathbb{N}_k$. Άρα $\mathbb{N}_n \sim \mathbb{N}_k$ μόνο αν $n = k$, και επομένως το πλήθος $|X|$ των στοιχείων ενός πεπερασμένου συνόλου X είναι καλά ορισμένο, όπως δεχτήκαμε στην Ενότητα 2.2.

Παράδειγμα 3.47. Σε κάθε ομάδα 13 ατόμων, τουλάχιστον δύο έχουν γενέθλια τον ίδιο μήνα. Πράγματι, «περιστέρια» είναι τα 13 άτομα και «φωλιές» οι 12 μήνες· η συνάρτηση που αντιστοιχίζει σε κάθε άτομο τον μήνα των γενεθλίων του δεν μπορεί να είναι ενριπτική, από το Πόρισμα 3.45. (Το ίδιο επιχείρημα, ως απαγωγή σε άτοπο: αν κάθε μήνας είχε το πολύ ένα άτομο, θα είχαμε το πολύ 12 άτομα.)

Παράδειγμα 3.48. Από τους αριθμούς $1, 2, \ldots, 2n$ διαλέγουμε $n+1$. Θα δείξουμε ότι δύο από αυτούς είναι διαδοχικοί. Εδώ η δυσκολία είναι να βρούμε τις κατάλληλες «φωλιές»: παίρνουμε τα n ζεύγη $\{1, 2\}, \{3, 4\}, \ldots, \{2n - 1, 2n\}$. Οι $n + 1$ αριθμοί που διαλέξαμε μοιράζονται σε αυτά τα n ζεύγη, άρα δύο από αυτούς ανήκουν στο ίδιο ζεύγος, δηλαδή είναι διαδοχικοί. Το $n + 1$ δεν μπορεί να αντικατασταθεί από n: οι n περιττοί $1, 3, \ldots, 2n - 1$ δεν περιέχουν διαδοχικούς αριθμούς.

3.6.2 Η γενικευμένη αρχή του περιστερώνα

Τι μπορούμε να πούμε αν τα περιστέρια είναι πολύ περισσότερα από τις φωλιές; Για να το διατυπώσουμε, χρειαζόμαστε δύο συναρτήσεις $\mathbb{R} \to \mathbb{Z}$.

Ορισμός 3.49 (Άνω και κάτω ακέραιο μέρος). Για $x \in \mathbb{R}$, το *άνω ακέραιο μέρος* $\lceil x \rceil$ του x είναι ο μικρότερος ακέραιος που είναι μεγαλύτερος ή ίσος του x, και το *κάτω ακέραιο μέρος* $\lfloor x \rfloor$ του x είναι ο μεγαλύτερος ακέραιος που είναι μικρότερος ή ίσος του x.

Για παράδειγμα, $\lceil 2{,}3 \rceil = 3$, $\lfloor 2{,}3 \rfloor = 2$, $\lceil 5 \rceil = \lfloor 5 \rfloor = 5$, $\lceil -1{,}5 \rceil = -1$, $\lfloor -1{,}5 \rfloor = -2$ και $\lceil 100/7 \rceil = 15$, αφού $14 < 100/7 = 14{,}28\ldots \leq 15$. Πάντοτε ισχύει

$$x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1.$$

Για παράδειγμα, αν ήταν $\lceil x \rceil \geq x + 1$, τότε ο ακέραιος $\lceil x \rceil - 1$ θα ήταν μεγαλύτερος ή ίσος του x και μικρότερος από τον $\lceil x \rceil$, άτοπο. Επίσης, $\lfloor x \rfloor = \lceil x \rceil$ αν και μόνον αν ο x είναι ακέραιος.

Θεώρημα 3.50 (Γενικευμένη αρχή του περιστερώνα). *Αν n αντικείμενα κατανεμηθούν σε $k \geq 1$ κουτιά, τότε κάποιο κουτί περιέχει τουλάχιστον $\lceil n/k \rceil$ αντικείμενα.*

Απόδειξη. Με απαγωγή σε άτοπο: έστω ότι κάθε κουτί περιέχει λιγότερα από $\lceil n/k \rceil$ αντικείμενα, δηλαδή, αφού το πλήθος είναι ακέραιος, το πολύ $\lceil n/k \rceil - 1$. Τότε το συνολικό πλήθος των αντικειμένων είναι το πολύ

$$k(\lceil n/k \rceil - 1) < k\left(\frac{n}{k} + 1 - 1\right) = n,$$

αφού $\lceil n/k \rceil < n/k + 1$. Αυτό είναι άτοπο, αφού τα αντικείμενα είναι ακριβώς n. □

Για $n = k + 1$ έχουμε $\lceil (k+1)/k \rceil = 2$, οπότε παίρνουμε ξανά την αρχή του περιστερώνα.

Παράδειγμα 3.51. Ανάμεσα σε 100 οποιαδήποτε άτομα, τουλάχιστον $\lceil 100/7 \rceil = 15$ γεννήθηκαν την ίδια ημέρα της εβδομάδας: εδώ $n = 100$ (τα άτομα) και $k = 7$ (οι ημέρες). Το 15 δεν μπορεί να αντικατασταθεί από 16: αν 15 άτομα έχουν γεννηθεί Δευτέρα, 15 Τρίτη και από 14 καθεμία από τις υπόλοιπες πέντε ημέρες, έχουμε $2 \cdot 15 + 5 \cdot 14 = 100$ άτομα και καμία ημέρα με 16.

Γενικά, ο αριθμός $\lceil n/k \rceil$ του θεωρήματος είναι ο καλύτερος δυνατός (Άσκηση 7).

3.6.3 Η αρχή της διαγωνοποίησης

Η *αρχή της διαγωνοποίησης* διατυπώνεται ως ακολούθως:

Θεώρημα 3.52 (Αρχή της διαγωνοποίησης). *Έστω R μια δυμελής σχέση στο σύνολο A και*

$$D = \{a \in A : (a, a) \notin R\}, \quad R_a = \{b \in A : (a, b) \in R\} \text{ για κάθε } a \in A.$$

Τότε $D \neq R_a$ για κάθε $a \in A$.

Η απόδειξη είναι εύκολη, γιατί αν $(a, a) \in R$ τότε $a \notin D$ και $a \in R_a$, ενώ αν $(a, a) \notin R$ τότε $a \in D$ και $a \notin R_a$. Μάλιστα τα παραπάνω ισχύουν για κάθε $a \in A$.

Το όνομα της αρχής εξηγείται αν φανταστούμε τη σχέση R ως έναν πίνακα, με μια γραμμή και μια στήλη για κάθε στοιχείο του A, όπου στη θέση (a, b) γράφουμε 1 αν $(a, b) \in R$ και 0 αν όχι (Σχήμα 3.4). Η γραμμή του a περιγράφει το σύνολο R_a, ενώ το D περιγράφεται από τη *διαγώνιο* του πίνακα, αφού αλλάξουμε κάθε 0 σε 1 και κάθε 1 σε 0. Έτσι το D διαφέρει από κάθε R_a στη θέση της διαγωνίου, δηλαδή ως προς το στοιχείο a.

	1	2	3	4
R_1:	1	0	1	1
R_2:	0	0	1	0
R_3:	1	1	0	1
R_4:	0	1	0	1
D:	0	1	1	0

Σχήμα 3.4. Η αρχή της διαγωνοποίησης για μια σχέση R στο $A = \{1, 2, 3, 4\}$. Η γραμμή a έχει 1 στη στήλη b αν και μόνον αν $(a, b) \in R$, οπότε $R_1 = \{1, 3, 4\}$, $R_2 = \{3\}$, $R_3 = \{1, 2, 4\}$, $R_4 = \{2, 4\}$. Αλλάζοντας τα διαγώνια στοιχεία (σκιασμένα) παίρνουμε το $D = \{2, 3\}$, που διαφέρει από κάθε R_a στη στήλη a.

Τη διαγωνοποίηση την έχουμε ήδη συναντήσει τρεις φορές, χωρίς να την ονομάσουμε.

- *Το διαγώνιο επιχείρημα* της Ενότητας 2.2 (Σχήμα 2.4): ο αριθμός b κατασκευάστηκε ώστε να διαφέρει από τον a_i στο i-οστό ψηφίο, όπως εδώ το D διαφέρει από το R_a ως προς το a. Η αντιστοιχία είναι ακριβής για τις ακολουθίες από 0 και 1 (Άσκηση 11 της Ενότητας 2.2): αν $s_0, s_1, s_2, \ldots$ είναι μια λίστα τέτοιων ακολουθιών, παίρνουμε $A = \mathbb{N}$ και $(i, j) \in R$ αν και μόνον αν ο j-οστός όρος της s_i είναι 1. Τότε το D αντιστοιχεί στην ακολουθία t με $t_i = 1 - s_{ii}$, που λοιπόν δεν είναι στη λίστα. (Για τους δεκαδικούς αριθμούς χρειάζεται και η προσοχή της Παρατήρησης 2.23, επειδή ένας αριθμός μπορεί να έχει δύο δεκαδικές παραστάσεις.)
- *Το θεώρημα του Cantor* (Θεώρημα 2.24): αν $f : X \to \mathcal{P}(X)$ είναι οποιαδήποτε συνάρτηση, εφαρμόζουμε την αρχή με $A = X$ και $R = \{(a, b) \in X \times X : b \in f(a)\}$, οπότε $R_a = f(a)$. Το σύνολο $D = \{a \in X : a \notin f(a)\}$ είναι στοιχείο του $\mathcal{P}(X)$ διαφορετικό από κάθε $f(a)$, άρα η f δεν είναι επιρριπτική. Αυτή είναι ακριβώς η ιδέα της λύσης της Άσκησης 1 της Ενότητας 2.2.
- *Το παράδοξο του Russell* (Ενότητα 1.1): για ένα σύνολο A (του οποίου τα στοιχεία είναι σύνολα) παίρνουμε $R = \{(a, b) \in A \times A : b \in a\}$, οπότε $R_a = a \cap A$ και $D = \{a \in A : a \notin a\}$. Αν ήταν $D \in A$, τότε για $a = D$ η αρχή θα έδινε $D \neq D \cap A = D$ (αφού $D \subseteq A$), άτοπο. Άρα $D \notin A$. Επομένως *κανένα* σύνολο A δεν περιέχει όλα τα σύνολα (γιατί δεν περιέχει το D), και το σύνολο $\{x : x \notin x\}$ του Russell είναι το «διαγώνιο σύνολο» μιας τέτοιας ανύπαρκτης «συλλογής όλων των συνόλων».

Μία αφηρημένη αρχή, τρεις διαφορετικές εφαρμογές.

Ασκήσεις

1. Αποδείξτε την αρχή του περιστερώνα με τη χρήση της αρχής της επαγωγής (Θεώρημα 2.2). (*Υπόδειξη:* επαγωγή στο $k \geq 1$. Για το επαγωγικό βήμα, αν $f : \mathbb{N}_{k+2} \to \mathbb{N}_{k+1}$ είναι ενριπτική, διακρίνετε περιπτώσεις ανάλογα με το αν υπάρχει $i \leq k + 1$ με $f(i) = k + 1$.)

2. Δείξτε ότι σ' ένα σύνολο ανθρώπων υπάρχουν τουλάχιστον δύο άτομα που έχουν τον ίδιο αριθμό γνωριμιών μέσα στο σύνολο. (Υποθέστε ότι το σύνολο έχει τουλάχιστον δύο άτομα, ότι η γνωριμία είναι αμοιβαία και ότι κανείς δεν μετράει τον εαυτό του. *Υπόδειξη:* αν τα άτομα είναι n, ποιες τιμές μπορεί να πάρει ο αριθμός γνωριμιών ενός ατόμου, και γιατί δεν μπορούν να εμφανιστούν ταυτόχρονα οι τιμές 0 και $n - 1$;)

3. Ρίχνουμε 40 ζάρια (με ενδείξεις 1 έως 6).

(α) Αποδείξτε ότι τουλάχιστον 7 ζάρια φέρνουν την ίδια ένδειξη.

(β) ⋆ Πόσα ζάρια πρέπει να ρίξουμε ώστε να είμαστε βέβαιοι ότι κάποια τέσσερα από αυτά φέρνουν είτε όλα την ίδια ένδειξη είτε όλα διαφορετικές ενδείξεις; Αποδείξτε την απάντησή σας.

4. Υπόλοιπα και αθροίσματα.

(α) Δείξτε ότι ανάμεσα σε $n + 1$ οποιουσδήποτε ακεραίους (όπου $n \geq 1$) υπάρχουν δύο των οποίων η διαφορά διαιρείται με το n. Ισχύει το ίδιο για n ακεραίους;

(β) ⋆ Δείξτε ότι σε κάθε ακολουθία $x_1, x_2, \ldots, x_n$ από n ακεραίους υπάρχουν διαδοχικοί όροι $x_{i+1}, x_{i+2}, \ldots, x_j$, για κάποια $0 \leq i < j \leq n$, των οποίων το άθροισμα διαιρείται με το n.

5. ⋆ Ένας φίλος σας έχει φτιάξει μια λίστα με τα 115 καλύτερα επεισόδια μιας τηλεοπτικής σειράς, κατά σειρά προτίμησης. Από αυτά έχετε δει τα 60. Αποδείξτε ότι υπάρχουν δύο επεισόδια που έχετε δει και απέχουν ακριβώς τέσσερις θέσεις στη λίστα του φίλου σας. (*Υπόδειξη:* χωρίστε τις 115 θέσεις σε ομάδες κατάλληλα.)

6. ⁻ Άνω και κάτω ακέραιο μέρος.

(α) Βρείτε τα $\lfloor -3{,}7 \rfloor$, $\lceil -3{,}7 \rceil$, $\lfloor \sqrt{50} \rfloor$ και $\lceil 1000/13 \rceil$.

(β) Δείξτε ότι $\lceil x \rceil = -\lfloor -x \rfloor$ για κάθε $x \in \mathbb{R}$.

(γ) Δείξτε ότι $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$ για κάθε $n \in \mathbb{Z}$.

7. Δείξτε ότι το Θεώρημα 3.50 δεν μπορεί να βελτιωθεί: για κάθε $n \in \mathbb{N}$ και $k \geq 1$ υπάρχει μια κατανομή n αντικειμένων σε k κουτιά στην οποία κανένα κουτί δεν έχει περισσότερα από $\lceil n/k \rceil$ αντικείμενα. (*Υπόδειξη:* γράψτε $n = qk + r$ με $0 \leq r < k$.)

8. ⋆ Από τους αριθμούς $1, 2, \ldots, 2n$ διαλέγουμε $n + 1$. Δείξτε ότι ένας από αυτούς διαιρεί κάποιον άλλο. (*Υπόδειξη:* γράψτε κάθε αριθμό ως $2^a m$ με m περιττό, όπως στην Ενότητα 2.2, μετά το Σχήμα 2.3.)

9. ⁻ Έστω $A = \{1, 2, 3\}$ και $R = \{(1,1), (1,2), (2,3), (3,1), (3,3)\}$. Βρείτε τα σύνολα R_1, R_2, R_3 και D της αρχής της διαγωνοποίησης και ελέγξτε ότι $D \neq R_a$ για κάθε $a \in A$.

10. Για καθεμία από τις συναρτήσεις $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ με (α) $f(n) = \{0, 1, \ldots, n\}$ και (β) $f(n) = \{m \in \mathbb{N} : m > n\}$, βρείτε το σύνολο $D = \{n \in \mathbb{N} : n \notin f(n)\}$ και εξηγήστε γιατί δεν είναι τιμή της f.

Παράρτημα Α

Απαντήσεις και υποδείξεις

Σε αυτό το παράρτημα δίνονται σύντομες απαντήσεις ή υποδείξεις για τις ασκήσεις στο τέλος κάθε ενότητας και για τις ασκήσεις επανάληψης στο τέλος κάθε μέρους. Δεν αποτελούν πλήρεις λύσεις: για τις αποδείξεις δίνεται συνήθως μόνο η βασική ιδέα, την οποία ο αναγνώστης καλείται να ολοκληρώσει.

Κεφάλαιο 1. Σύνολα, σχέσεις και συναρτήσεις

Ενότητα 1.1

1. Έχει $2^4 = 16$ στοιχεία: το $\emptyset$, τα 4 μονοσύνολα, τα 6 διμελή υποσύνολα $\{a,b\}$, $\{a,c\}$, $\{a,d\}$, $\{b,c\}$, $\{b,d\}$, $\{c,d\}$, τα 4 τριμελή και το $\{a,b,c,d\}$.

2. (α) 13· (β) 198· (γ) 50 (οι περιττοί $1,3,\dots,99$)· (δ) 1· (ε) τέτοιο σύνολο δεν υπάρχει: αν $|E| = 2$, τότε $E = \{2\}$ και $|E| = 1$· αν $|E| \neq 2$, τότε $|E| = 2$.

3. Π.χ., $A = \{1\}$ και $B = \{1, \{1\}\}$ (ή $A = \emptyset$ και $B = \{\emptyset\}$).

4. Όχι. Αν το βιβλίο K αναφέρει τον εαυτό του, τότε, αφού αναφέρει μόνο βιβλία που δεν αναφέρουν τον εαυτό τους, δεν τον αναφέρει· αν δεν τον αναφέρει, τότε είναι ένα από τα βιβλία που οφείλει να αναφέρει. Είναι το επιχείρημα για το $R = \{x : x \notin x\}$, με το «αναφέρει» στη θέση του «ανήκει». (Ένας κατάλογος για τα βιβλία μιας *άλλης* βιβλιοθήκης δεν έχει πρόβλημα: πρβλ. $\{x \in A : x \notin x\}$.)

5. (α) Όχι, αφού $1 \in \mathbb{Z}_+$, $1 \notin 2\mathbb{Z}$· όχι, αφού $0 \in 2\mathbb{Z}$, $0 \notin \mathbb{Z}_+$. (β) $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$, τα πολλαπλάσια του 6. (γ) $2\mathbb{Z} \cup 3\mathbb{Z}$.

6. $AB = \{2,3,4,6,8\}$, άρα $|AB| = 5$ (το 4 προκύπτει δύο φορές)· $|A \times B| = 2 \cdot 3 = 6$.

7. Τα A και $B \setminus A$ είναι ξένα με ένωση $A \cup B$, άρα $|B \setminus A| = |A \cup B| - |A|$ και $|A \cap B| = |B| - |B \setminus A|$: (α) $|A \cap B| = 3$, π.χ., $A = \{1,\dots,5\}$, $B = \{3,\dots,9\}$· (β) $|A \cap B| = 2$, π.χ., $A = \{1,\dots,5\}$, $B = \{4,\dots,9\}$· (γ) όχι, αφού θα έπρεπε $10 = 2|A| - 5$.

8. $|\mathcal{B}_2| = 10 \cdot 9/2 = 45$ (κάθε διμελές υποσύνολο αντιστοιχεί σε δύο διατεταγμένα ζεύγη διαφορετικών στοιχείων). Όμοια $|\mathcal{B}_3| = 12 \cdot 11 \cdot 10/6 = 220$ (κάθε τριμελές υποσύνολο μπορεί να γραφτεί σε 6 διαφορετικές σειρές).

9. Π.χ., (α) $A = \{11,13,15,16,17,18,19,20,21,22\}$· (β) $B = \{10,11,12,13,14\}$· (γ) $C = \{\emptyset, \{10\}, \{11\}, \{12\}, \{13\}\}$· (δ) $D = \{(10,10),(10,11),(10,12),(10,13),(10,14)\}$· (ε) αφού όλα τα στοιχεία του X είναι ≥ 10 και $|E| \leq 10$, πρέπει $|E| = 10$, δηλαδή $E = X$ (μοναδική λύση).

10. $A \cup B = (0,4)$, $A \cap B = [1,2]$, $A' = (-\infty,0] \cup (2,\infty)$, $A \cup C = (0,2] \cup [3,9)$, $A \cap C = \emptyset$, $B' = (-\infty,1) \cup [4,\infty)$, $A' \cap B' = (A \cup B)' = (-\infty,0] \cup [4,\infty)$, $A' \cup B' = (A \cap B)' = (-\infty,1) \cup (2,\infty)$: οι δύο ισότητες είναι οι νόμοι του De Morgan.

11. Π.χ., το $A' \cap B \cap C'$ είναι η περιοχή του B που βρίσκεται έξω από τα A και C, ενώ το $(A \cup B) \setminus C$ είναι η περιοχή της ένωσης $A \cup B$ που βρίσκεται έξω από το C.

12. Αν $x \in A$, τότε $x \in B$, άρα $x \in C$. Παράδειγμα: $A = \{1,2\}$, $B = \{A,3\}$, $C = \{B,4\}$.

13. Διπλός εγκλεισμός· π.χ., για την πρώτη: $A \subseteq A \cup (A \cap B)$ πάντα, και αν $x \in A \cup (A \cap B)$ τότε σε κάθε περίπτωση $x \in A$.

14. Με αλυσίδα ισοδυναμιών, όπως στο κείμενο. Για παράδειγμα, $x \in A \cup (B \cap C) \iff x \in A$ ή ($x \in B$ και $x \in C$) $\iff$ ($x \in A$ ή $x \in B$) και ($x \in A$ ή $x \in C$) $\iff x \in (A \cup B) \cap (A \cup C)$.

15. (α) $x \in A \setminus (B \cup C) \iff x \in A$, $x \notin B$ και $x \notin C \iff x \in (A \setminus B) \cap (A \setminus C)$· όμοια το δεύτερο, με τους νόμους του De Morgan. (β) $x \in A \cap (B \setminus C) \iff x \in A, x \in B, x \notin C$, δηλαδή $x \in A \cap B$ και $x \notin A \cap C$. (γ) Αν $x \in A \cap B$, τότε είτε $x \in C$, οπότε $x \in A \cap C$, είτε $x \in C'$, οπότε $x \in B \cap C'$. (δ) Αν $x \in (A \cup C) \cap (B \cup C')$ και $x \in C$, τότε από το $x \in B \cup C'$ έπεται $x \in B$· αν $x \notin C$, τότε από το $x \in A \cup C$ έπεται $x \in A$.

16. Το $A \subseteq B$ σημαίνει ότι δεν υπάρχει στοιχείο του A εκτός του B, δηλαδή $A \setminus B = A \cap B' = \emptyset$. Για το (β) πάρτε συμπληρώματα στο (α) (νόμοι του De Morgan)· το (γ) είναι μία από τις ιδιότητες του συμπληρώματος.

17. Αν $C \subseteq A$, τότε από τον επιμεριστικό νόμο $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) = A \cap (B \cup C)$, αφού $A \cup C = A$. Αντίστροφα, αν ισχύει η ισότητα, τότε $C \subseteq (A \cap B) \cup C = A \cap (B \cup C) \subseteq A$.

18. $X \in \mathcal{P}(A) \cap \mathcal{P}(B) \iff X \subseteq A$ και $X \subseteq B \iff X \subseteq A \cap B$. Για το δεύτερο: αν $X \subseteq A$ ή $X \subseteq B$, τότε $X \subseteq A \cup B$. Η ισότητα δεν ισχύει πάντα: για $A = \{1\}$, $B = \{2\}$ έχουμε $\{1, 2\} \in \mathcal{P}(A \cup B)$, αλλά $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

19. (α) Ψευδές: για $A = C = \{1\}$, $B = \emptyset$ το αριστερό μέλος είναι $\{1\}$ και το δεξί $\emptyset$. (β) Αληθές: και τα δύο σύνολα αποτελούνται από τα x με $x \in A$, $x \notin B$, $x \notin C$. (γ) Ψευδές: $A = \{1\}$, $B = C = \emptyset$ (το δεξί μέλος είναι πάντα ξένο προς το A). (δ) Αληθές. Αν $x \in A$ και $x \in C$, τότε $x \in A \cap C = B \cap C$· αν $x \notin C$, τότε $x \in A \cup C = B \cup C$· σε κάθε περίπτωση $x \in B$, και συμμετρικά. Μία υπόθεση δεν αρκεί: $A = \{1\}$, $B = C = \emptyset$ (ισχύει η πρώτη) και $A = C = \{1\}$, $B = \emptyset$ (ισχύει η δεύτερη).

20. Και τα δύο σύνολα αποτελούνται από τα στοιχεία που ανήκουν σε ακριβώς ένα από τα A, B. Τα υπόλοιπα έπονται άμεσα από τον ορισμό.

21. Ένα x ανήκει στο $(A \triangle B) \triangle C$ αν και μόνο αν ανήκει σε περιττό πλήθος (ένα ή τρία) από τα A, B, C· το ίδιο ισχύει και για το $A \triangle (B \triangle C)$. Για τον επιμερισμό: $x \in A \cap (B \triangle C)$ αν και μόνο αν $x \in A$ και το x ανήκει σε ακριβώς ένα από τα B, C, δηλαδή σε ακριβώς ένα από τα $A \cap B$, $A \cap C$. Για τη διαγραφή: «προσθέστε» το A και στα δύο μέλη, οπότε $B = (A \triangle A) \triangle B = A \triangle (A \triangle B) = A \triangle (A \triangle C) = C$.

22. $A = \{2, 3\}$ και $B = \{1, 2\}$. (Αν $|B| = 3$, τότε $A = \{3\}$, άρα $B = \{1, 3\}$, άτοπο· αν $|B| = 1$, τότε πρέπει $|A| = 1$, ενώ $A = \{1, 3\}$, άτοπο.)

Ενότητα 1.2

1. Το $A \times A$ έχει 9 στοιχεία: $(a, a), (a, b), (a, c), (b, a), \ldots, (c, c)$. Τα ζεύγη (διμελή υποσύνολα) είναι τα $\{a, b\}$, $\{a, c\}$, $\{b, c\}$.

2. Διπλός εγκλεισμός· π.χ., για το (ii): $(u, v) \in (A \cap B) \times (X \cap Y) \iff u \in A, u \in B, v \in X, v \in Y \iff (u, v) \in A \times X$ και $(u, v) \in B \times Y$.

3. (α) $S = \{(3, 6), (4, 4), (5, 5)\}$, με πεδίο ορισμού $\{3, 4, 5\}$ και πεδίο τιμών $\{4, 5, 6\}$· $S^{-1} = \{(6, 3), (4, 4), (5, 5)\}$, με πεδίο ορισμού $\{4, 5, 6\}$ και πεδίο τιμών $\{3, 4, 5\}$. (β) $R \circ R = \{(1, 3), (2, 4)\}$, $R^{-1} \circ R = \{(1, 1), (2, 2), (3, 3)\}$ (ένα βήμα μπροστά, μετά ένα πίσω), $R \circ R^{-1} = \{(2, 2), (3, 3), (4, 4)\}$. Δεν είναι ίσες, και καμία δεν είναι η ισότητα (λείπει το $(4, 4)$, αντίστοιχα το $(1, 1)$).

4. Είναι αυτοπαθής, μεταβατική και αντισυμμετρική, αλλά όχι συμμετρική. Άρα είναι μερική διάταξη (όχι σχέση ισοδυναμίας)· δεν είναι ολική, αφού το d δεν συγκρίνεται με κανένα άλλο στοιχείο.

5. Π.χ., (α) $\{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (2, 3), (3, 2)\}$ (υπάρχουν τα $(1, 2), (2, 3)$ αλλά όχι το $(1, 3)$)· (β) η $\leq$ στο $\{1, 2, 3, 4\}$· (γ) $\{(1, 1)\}$ (ή ακόμη και η κενή σχέση).

6. Το επιχείρημα υποθέτει σιωπηρά ότι για κάθε a υπάρχει κάποιο b με aRb. Αν ένα a δεν σχετίζεται με κανένα στοιχείο, το επιχείρημα δεν εφαρμόζεται· π.χ., η $R = \{(1, 1)\}$ στο $\{1, 2\}$ είναι συμμετρική και μεταβατική, αλλά όχι αυτοπαθής.

7. Αληθές: αφού $(R^{-1})^{-1} = R$, από την Πρόταση 1.31 η R^{-1} είναι συμμετρική $\iff R^{-1} = R \iff$ η R είναι συμμετρική.

8. (α), (β) Αληθή. (γ) Ψευδές: $R = \{(1, 2)\}$, $S = \{(2, 3)\}$. (δ) Ψευδές: $R = \{(1, 2)\}$, $S = \{(2, 1)\}$.

9. Από τον ορισμό, $(x,z) \in R \circ R$ αν και μόνο αν υπάρχει y με xRy και yRz. Η μεταβατικότητα λέει ακριβώς ότι σε αυτή την περίπτωση xRz.

10. Όπως στο Παράδειγμα 1.41. Οι κλάσεις είναι οι $[0], [1], [2], [3], [4]$, όπου $[r] = \{5k + r \,:\, k \in \mathbb{Z}\}$.

11. (α) Είναι $(a,b) \sim (c,d) \iff a-b = c-d$: δύο ζεύγη σχετίζονται όταν δίνουν την ίδια διαφορά (πρβλ. Άσκηση 4 της Ενότητας 1.3). (β) $[(2,5)] = \{(1,4),(2,5),(3,6),(4,7),(5,8),(6,9)\}$.

12. Μόνο η (γ). Στην (α) το 1 ανήκει σε δύο μερίδια, στη (β) λείπει το 4, και στη (δ) το $7 \notin S$.

13. Υπάρχουν 5 διαμερίσεις: $\{\{1\},\{2\},\{3\}\}$, $\{\{1,2\},\{3\}\}$, $\{\{1,3\},\{2\}\}$, $\{\{2,3\},\{1\}\}$, $\{\{1,2,3\}\}$· άρα, από τα Θεωρήματα 1.39 και 1.40, 5 σχέσεις ισοδυναμίας.

14. Όπως στο Παράδειγμα 1.44, με τη διαφορά ότι τώρα $a \mid 0$ για κάθε a (με $k = 0$), ενώ το 0 διαιρεί μόνο το 0. Για την αντισυμμετρία, αν $a = 0$ και $0 \mid b$, τότε $b = 0$. Δεν είναι ολική ($2 \nmid 3$, $3 \nmid 2$).

15. Αντισυμμετρία και μεταβατικότητα: διακρίνετε τις περιπτώσεις $\alpha < \gamma$ και $\alpha = \gamma$: αν $\alpha < \gamma$, η $(\gamma,\delta) \lhd (\alpha,\beta)$ είναι αδύνατη, ενώ αν $\alpha = \gamma$ όλα ανάγονται στις ιδιότητες της $\leq$. Είναι ολική: αν $\alpha \neq \gamma$, το ζεύγος με τη μικρότερη πρώτη συντεταγμένη είναι «μικρότερο»· αν $\alpha = \gamma$, συγκρίνουμε τα β και δ.

16. $X = \{1,2,3,4,6,9,12,18,36\}$. (α) Ελάχιστο το 1, μέγιστο το 36. (β) Άνω φράγματα του $\{4,6\}$: $12, 36$· κάτω φράγματα: $1, 2$. (γ) Ελάσσονα: $2, 3$· μείζονα: $12, 18$· ούτε ελάχιστο ούτε μέγιστο.

17. (α) Έστω a το μοναδικό ελάσσον στοιχείο και $x \in X$. Το $Y = \{y \in X \,:\, y \preceq x\}$ είναι μη κενό (περιέχει το x) και πεπερασμένο, άρα έχει ελάσσον στοιχείο m. Δείξτε ότι το m είναι ελάσσον στοιχείο και του X. (β) Π.χ., το $\mathbb{Z} \cup \{\star\}$, όπου οι ακέραιοι διατάσσονται με τη $\leq$ και το $\star$ δεν συγκρίνεται με κανέναν ακέραιο: το $\star$ είναι το μόνο ελάσσον στοιχείο, αλλά δεν είναι ελάχιστο.

Ενότητα 1.3

1. (α) Καμία. $R = \{(5,5),(6,5),(6,6)\}$: το 4 δεν έχει εικόνα (και το 6 έχει δύο). $S = \{(4,6),(5,5),(5,7),(6,6)\}$: το 5 έχει δύο εικόνες. T: το 5 δεν έχει εικόνα και το 6 έχει δύο. (β) Η πρώτη όχι ($4 = 2^2 = (-2)^2$)· η δεύτερη ναι, είναι η $x \mapsto \sqrt{x}$. (γ) $2^4 = 16$ σχέσεις· $2 \cdot 2 = 4$ συναρτήσεις. (δ) Η ύπαρξη εικόνας κάθε y μέσω της f^{-1} σημαίνει ότι η f είναι επί· η μοναδικότητά της ότι η f είναι ενριπτική.

2. Για την $f(x) = x^2$, $A = \{-1\}$, $B = \{1\}$ είναι $f(A \cap B) = \emptyset$, ενώ $f(A) \cap f(B) = \{1\}$. Αν η f είναι ενριπτική και $y \in f(A) \cap f(B)$, τότε $y = f(a) = f(b)$ με $a \in A$, $b \in B$, άρα $a = b \in A \cap B$.

3. Αλυσίδα ισοδυναμιών· π.χ., $x \in f^{-1}(A \cap B) \iff f(x) \in A$ και $f(x) \in B \iff x \in f^{-1}(A) \cap f^{-1}(B)$.

4. Οι τρεις ιδιότητες «κληρονομούνται» από την ισότητα: $f(a) = f(a)$· αν $f(a) = f(b)$ τότε $f(b) = f(a)$· αν $f(a) = f(b)$ και $f(b) = f(c)$, τότε $f(a) = f(c)$.

5. $(g \circ f)(x) = \sqrt{x^2+1}$, για κάθε $x \in \mathbb{R}$. $(f \circ g)(x) = x + 1$ για $x \geq 0$, άρα $g \circ f \neq f \circ g$ (δεν έχουν καν το ίδιο πεδίο ορισμού).

6. (α) $(g \circ f)(x) = x^3 - 1$ και $(f \circ g)(x) = (x-1)^3$. Η διαφορά τους είναι $3x(x-1)$, άρα είναι ίσες μόνο για $x = 0$ και $x = 1$· οι συναρτήσεις δεν είναι ίσες. (β) $f^{-1}(y) = \sqrt[3]{y}$, $g^{-1}(y) = y + 1$, $(g \circ f)^{-1}(y) = \sqrt[3]{y+1} = f^{-1}(g^{-1}(y))$· όμως $g^{-1}(f^{-1}(7)) = \sqrt[3]{7} + 1 \neq 2 = \sqrt[3]{8}$.

7. $3^2 = 9$ συναρτήσεις· 6 ενριπτικές (όσες έχουν $f(a) \neq f(b)$)· καμία επιρριπτική ($|A| < |B|$).

8. $7^5 = 16807$ συναρτήσεις· $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520$ ενριπτικές· καμία επιρριπτική, αφού το πεδίο τιμών έχει το πολύ 5 στοιχεία.

9. $f(-1) = f(1)$· αν $x_1, x_2 \geq 0$ και $x_1^2 = x_2^2$, τότε $x_1 = x_2$. Δεν είναι επί του $\mathbb{R}$: οι αρνητικοί αριθμοί δεν είναι τιμές της. Όμοια για την h ($h(-1) = h(1)$). Αν $\sqrt{x_1} = \sqrt{x_2}$, τότε $x_1 = x_2$· το -1 δεν είναι τιμή της r.

10. (α) Ούτε ενριπτική ($f(2) = f(4) = 4$) ούτε επί· (β) ούτε ενριπτική ούτε επί· (γ) αμφιμονοσήμαντη. Όχι: για πεπερασμένα σύνολα με το ίδιο πλήθος στοιχείων, μια συνάρτηση είναι ενριπτική αν και μόνο αν είναι επί.

11. (α) Ενριπτική, όχι επί (τα $0, 1, 2, 3$ δεν είναι τιμές)· (β) αμφιμονοσήμαντη· (γ) ενριπτική, όχι επί (π.χ., το 0 δεν είναι τιμή)· (δ) επί (κάθε m είναι το $f(2m)$), όχι ενριπτική ($f(1) = f(2) = 1$).

12. (α) Δεν είναι ενριπτική ($f(\{1\}) = f(\{2\})$) ούτε επί (το 11 δεν είναι τιμή). (β) $f^{-1}(\{1\})$ είναι τα 10 μονοσύνολα, $f^{-1}(\{0\}) = \{\emptyset\}$ και $f^{-1}(\{12\}) = \emptyset$.

13. Τα (α) και (β) είναι δυνατά (π.χ., η συνάρτηση εγκλεισμού $\mathbb{N} \to \mathbb{Z}$, και η $f : \{1, 2\} \to \{1\}$). Τα (γ) και (δ) είναι αδύνατα: η (γ) θα έδινε πεδίο τιμών με $|X|$ στοιχεία, γνήσιο υποσύνολο του Y· η (δ) θα έδινε πεδίο τιμών με λιγότερα από $|Y|$ στοιχεία.

14. (α) Για $z \in Z$ υπάρχει $y \in Y$ με $g(y) = z$, και για αυτό το y υπάρχει $x \in X$ με $f(x) = y$· τότε $(g \circ f)(x) = z$. (β) Αν η $g \circ f$ είναι ενριπτική, τότε η f είναι ενριπτική· αν η $g \circ f$ είναι επί, τότε η g είναι επί. Η άλλη συνάρτηση δεν χρειάζεται να έχει την ιδιότητα: π.χ., $f : \{1\} \to \{a, b\}$ με $f(1) = a$ και $g : \{a, b\} \to \{5\}$.

15. Αν $f(x_1) = f(x_2)$, τότε $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Για κάθε $a \in A$ έχουμε $a = g(f(a))$, άρα το a είναι τιμή της g. Με εναλλαγή των ρόλων, η f είναι και επί· για $b \in B$, το $g(b)$ ικανοποιεί $f(g(b)) = b$, άρα $g(b) = f^{-1}(b)$.

16. Γενικά όχι: για $f(x) = x^2$ στο $\mathbb{R}$, $f^{-1}(f(\{1\})) = \{-1, 1\}$ και $f(f^{-1}(\{-1, 1\})) = \{1\}$.

17. Αν $\chi_A = \chi_B$, τότε $x \in A \iff \chi_A(x) = 1 \iff \chi_B(x) = 1 \iff x \in B$, άρα $A = B$. Κάθε $h : X \to \{0, 1\}$ είναι η χ_A για $A = h^{-1}(\{1\})$. Οι τύποι: και τα δύο μέλη είναι 1 ακριβώς όταν $x \in A$ και $x \in B$ (αντίστοιχα, όταν $x \notin A$).

Κεφάλαιο 2. Φυσικοί αριθμοί, επαγωγή και ισοδύναμα σύνολα

Ενότητα 2.1

1. Βάση $n = 0$: $\mathcal{P}(\emptyset) = \{\emptyset\}$ έχει $1 = 2^0$ στοιχείο. Βήμα: αν $|A| = n + 1$, διαλέγουμε $a \in A$ και θέτουμε $A' = A \setminus \{a\}$. Τα υποσύνολα του A που δεν περιέχουν το a είναι ακριβώς τα υποσύνολα του A' (2^n από την επαγωγική υπόθεση), και αυτά που περιέχουν το a είναι ακριβώς τα $X \cup \{a\}$ με $X \subseteq A'$ (άλλα 2^n). Σύνολο 2^{n+1}.

2. Για $n = 1$ δεν έχουμε τίποτα να δείξουμε. Στο βήμα γράφουμε $A_1 \cup \cdots \cup A_{n+1} = (A_1 \cup \cdots \cup A_n) \cup A_{n+1}$, εφαρμόζουμε την περίπτωση δύο συνόλων (Άσκηση 2 της Ενότητας 1.2) και μετά την επαγωγική υπόθεση.

3. Βάση: $1 + 2 = 3$. Βήμα: $(n + 1)^3 + 2(n + 1) = (n^3 + 2n) + 3(n^2 + n + 1)$.

4. Βάση: $25 < 32$. Βήμα: για $n \geq 5$, $(n + 1)^2 = n^2 + (2n + 1) < n^2 + n^2 = 2n^2 < 2 \cdot 2^n = 2^{n+1}$, όπου χρησιμοποιήσαμε το Παράδειγμα 2.6.

5. Βάση: $1 = 1^2$. Βήμα: $n^2 + (2n + 1) = (n + 1)^2$.

6. Βάση: $2^0 = 1 = 2^1 - 1$. Βήμα: $(2^{n+1} - 1) + 2^{n+1} = 2^{n+2} - 1$.

7. (α) Βάση: $7^0 - 1 = 0$. Βήμα: $7^{n+1} - 1 = 7(7^n - 1) + 6$. (β) Βάση: $7^0 - 2^0 = 0$. Βήμα: $7^{n+1} - 2^{n+1} = 7(7^n - 2^n) + 5 \cdot 2^n$. (γ) Βάση: $a^0 - b^0 = 0$. Βήμα: $a^{n+1} - b^{n+1} = a(a^n - b^n) + b^n(a - b)$. Τα (α), (β) είναι οι περιπτώσεις $a = 7, b = 1$ και $a = 7, b = 2$.

8. Βάση: $2^4 = 16 < 24 = 4!$. Βήμα: $2^{n+1} = 2 \cdot 2^n < 2 \cdot n! < (n + 1) \cdot n! = (n + 1)!$.

9. (α) Βήμα: $\frac{n(3n-1)}{2} + (3n+1) = \frac{3n^2+5n+2}{2} = \frac{(n+1)(3n+2)}{2}$. (β) Βήμα: $\frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n(n+2)+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2}$. (γ) Βήμα: $\frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} = \frac{2n^2+3n+1}{(2n+1)(2n+3)} = \frac{n+1}{2n+3}$.

10. Έστω $S_n = 1 + 2 + \cdots + n = n(n+1)/2$. Τότε $S_{n+1}^2 = (S_n + (n+1))^2 = S_n^2 + 2(n+1)S_n + (n+1)^2 = S_n^2 + n(n+1)^2 + (n+1)^2 = S_n^2 + (n+1)^3$, και από την επαγωγική υπόθεση $S_n^2 = 1^3 + \cdots + n^3$.

11. Βάση: για $n = 1$ γίνονται 0 χειραψίες. Βήμα: το άτομο $n+1$ δίνει n νέες χειραψίες, και $\frac{n(n-1)}{2} + n = \frac{(n+1)n}{2}$.

12. (α) Λείπει η βάση: η $P(0)$, δηλαδή $3 = 7$, είναι ψευδής (το βήμα είναι σωστό, αλλά δεν αρκεί). (β) Και εδώ λείπει η βάση, και μάλιστα η $P(0)$ είναι ψευδής (0 είναι άρτιος). Σωστή απόδειξη: ο $0^2 + 0 = 0$ είναι άρτιος, και $(k+1)^2 + (k+1) = (k^2 + k) + 2(k+1)$ είναι άθροισμα δύο άρτιων. (γ) Το βήμα αποτυγχάνει για $k = 1$: οι ομάδες $\{a_1\}$ και $\{a_2\}$ δεν έχουν κοινό στοιχείο. Αφού το $P(1) \Rightarrow P(2)$ είναι ψευδές, η αλυσίδα σπάει: το βήμα πρέπει να ισχύει για *κάθε* $k \geq n_0$.

13. (α) $-3\cdot 5 + 2\cdot 8 = 1$: αντικαθιστούμε τρία γραμματόσημα των 5 με δύο των 8. (β) Αντικαθιστούμε τρία γραμματόσημα των 8 (24 λεπτά) με πέντε των 5 (25 λεπτά). (γ) Βάση: $28 = 4 \cdot 5 + 8$. Βήμα: αν το $n \geq 28$ πληρώνεται με a γραμματόσημα των 5 και b των 8 και $a \leq 2$, τότε $8b \geq n - 10 \geq 18$, άρα $b \geq 3$· σε κάθε περίπτωση εφαρμόζεται το (α) ή το (β).

14. Βάσεις: 6 (το σχήμα της εκφώνησης)· 7 (χωρίζουμε το τετράγωνο σε 4 ίσα τετράγωνα και ένα από αυτά πάλι σε 4)· 8 (ένα τετράγωνο πλευράς $3/4$ και 7 τετράγωνα πλευράς $1/4$ κατά μήκος δύο πλευρών). Βήμα: για $n \geq 9$ είναι $n - 3 \geq 6$· χωρίζουμε το τετράγωνο σε $n-3$ τετράγωνα και ένα από αυτά σε 4, οπότε το πλήθος αυξάνεται κατά 3.

15. Βάση: για $n = 1$ δεν χρειάζεται καμία κίνηση. Βήμα: η τελευταία κίνηση ενώνει τμήματα με k και $n-k$ κομμάτια, $1 \leq k \leq n-1$, που (ισχυρή επαγωγική υπόθεση) χρειάστηκαν $k-1$ και $n-k-1$ κινήσεις· συνολικά $(k-1) + (n-k-1) + 1 = n - 1$. (Και χωρίς επαγωγή: κάθε κίνηση μειώνει το πλήθος των τμημάτων κατά 1.)

16. Βάση: $1 = 2^0$. Βήμα: έστω $n \geq 2$ και 2^m η μεγαλύτερη δύναμη του 2 με $2^m \leq n$. Αν $n = 2^m$, τελειώσαμε. Αλλιώς ο $r = n - 2^m$ ικανοποιεί $1 \leq r < 2^m$ (αφού $n < 2^{m+1}$) και $r < n$, άρα από την επαγωγική υπόθεση είναι δύναμη του 2 ή άθροισμα διαφορετικών δυνάμεων του 2, όλες $\leq r < 2^m$. Προσθέτοντας το 2^m παίρνουμε τον n ως άθροισμα διαφορετικών δυνάμεων του 2.

17. Έστω $s_n = x^n + x^{-n}$ (προφανώς $x \neq 0$). Είναι $s_0 = 2$ και ο s_1 είναι ακέραιος από την υπόθεση. Επιπλέον $s_k s_1 = x^{k+1} + x^{-(k+1)} + x^{k-1} + x^{-(k-1)} = s_{k+1} + s_{k-1}$, άρα $s_{k+1} = s_k s_1 - s_{k-1}$, που είναι ακέραιος αν οι s_k, s_{k-1} είναι ακέραιοι (ισχυρή επαγωγή με βάσεις $n = 0, 1$).

18. *Υπόδειξη:* χωρίστε τη σκακιέρα $2^{k+1} \times 2^{k+1}$ σε τέσσερα τεταρτημόρια $2^k \times 2^k$. Τοποθετήστε μία γωνία στο κέντρο, ώστε να καλύπτει ένα τετραγωνάκι από καθένα από τα τρία τεταρτημόρια που *δεν* περιέχουν το αφαιρεμένο, και εφαρμόστε την επαγωγική υπόθεση και στα τέσσερα. (Γι' αυτό η πρόταση πρέπει να αφορά *οποιοδήποτε* αφαιρεμένο τετραγωνάκι.) Γωνίες: $(4^n - 1)/3$.

Ενότητα 2.2

1. Έστω ότι υπάρχει επί συνάρτηση $f : X \to \mathcal{P}(X)$ και έστω $D = \{x \in X : x \notin f(x)\}$. Αφού $D \subseteq X$, υπάρχει $d \in X$ με $f(d) = D$. Αν $d \in D$, τότε $d \notin f(d) = D$· αν $d \notin D = f(d)$, τότε από τον ορισμό του D έχουμε $d \in D$. Και οι δύο περιπτώσεις οδηγούν σε άτοπο, άρα δεν υπάρχει ούτε καν επί συνάρτηση $X \to \mathcal{P}(X)$.

2. (α) $n \mapsto n + 5$. (β) $k \mapsto 2k$. (γ) $x \mapsto a + (b-a)x$. (δ) Στείλτε τα $0, \frac{1}{2}, \frac{1}{3}, \ldots$ στα $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ και κρατήστε τα υπόλοιπα σημεία σταθερά.

3. Από την Πρόταση 2.19 με $X = Y = \mathbb{Z}$. Για το $\mathbb{N}^k$: βάση $k = 1$· στο βήμα, η $(x_1, \ldots, x_k, x_{k+1}) \mapsto ((x_1, \ldots, x_k), x_{k+1})$ δείχνει ότι $\mathbb{N}^{k+1} \sim \mathbb{N}^k \times \mathbb{N}$, που είναι αριθμήσιμο από την επαγωγική υπόθεση και την Πρόταση 2.19.

4. Οι διαγώνιοι $0, 1, \ldots, d-1$ περιέχουν $1 + 2 + \cdots + d = d(d+1)/2$ ζεύγη (Παράδειγμα 2.4), και στη διαγώνιο $d = n + m$ το (n, m) είναι το ζεύγος με αριθμό m (αρχίζοντας από το 0).

5. Η $b(S) = \sum_{i \in S} 2^i$ (με $b(\emptyset) = 0$) είναι αμφιμονοσήμαντη $\mathcal{F} \to \mathbb{N}$. Είναι επί από την Άσκηση 16 της Ενότητας 2.1. Είναι ενριπτική: αν $S \neq T$, έστω j το μεγαλύτερο στοιχείο του $S \triangle T$, π.χ., $j \in S$. Τα στοιχεία που μετρούν στο $b(T)$ αλλά όχι στο $b(S)$ είναι όλα $< j$, άρα συνεισφέρουν το πολύ $2^0 + \cdots + 2^{j-1} = 2^j - 1 < 2^j$ (Άσκηση 6 της Ενότητας 2.1), οπότε $b(S) > b(T)$.

6. Όπως στο Παράδειγμα 2.22: γράφουμε κάθε A_n ως λίστα $e_n(0), \dots, e_n(k_n-1)$ και θέτουμε $\psi(y) = (n(y), m(y))$. Η ψ είναι ενριπτική στο $\mathbb{N}\times\mathbb{N}$, άρα η ένωση είναι το πολύ αριθμήσιμη (μπορεί να είναι και πεπερασμένη, π.χ., αν όλα τα A_n είναι ίσα).

7. Για κάθε $\ell \in \mathbb{N}$ οι λέξεις μήκους ℓ είναι πεπερασμένες (24^ℓ το πλήθος), άρα από την Άσκηση 6 η ένωσή τους είναι το πολύ αριθμήσιμη· είναι και άπειρη (π.χ., οι λέξεις α, αα, ααα, ...), άρα αριθμήσιμη.

8. (α) Έστω $e : \mathbb{N} \to A$ αμφιμονοσήμαντη και $h(b) = \min\{n : g(e(n)) = b\}$ (υπάρχει, αφού η g είναι επί). Η $h : B \to \mathbb{N}$ είναι ενριπτική, αφού $g(e(h(b))) = b$· εφαρμόστε το Πόρισμα 2.21. (β) Το σύνολο D των $(b, c, s) \in \mathbb{Z}\times\mathbb{Z}\times\{0, 1\}$ με $b^2 - 4c \geq 0$ είναι άπειρο υποσύνολο του αριθμήσιμου $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$, άρα αριθμήσιμο. Η $(b, c, s) \mapsto (-b + (-1)^s\sqrt{b^2 - 4c})/2$ είναι επί από το D στο R, άρα το R είναι το πολύ αριθμήσιμο· είναι και άπειρο, αφού κάθε $m \in \mathbb{Z}$ είναι ρίζα της $x^2 - mx = 0$. (γ) Το $\mathbb{R}$ είναι υπεραριθμήσιμο, άρα $R \neq \mathbb{R}$.

9. (α) $(a, b) \mapsto (b, a)$. (β) Αν η $f : A \to B$ είναι αμφιμονοσήμαντη, τότε η $X \mapsto f(X)$ είναι αμφιμονοσήμαντη από το $\mathcal{P}(A)$ στο $\mathcal{P}(B)$, με αντίστροφη την $Y \mapsto f^{-1}(Y)$.

10. Αν το $\mathbb{R}\setminus\mathbb{Q}$ ήταν το πολύ αριθμήσιμο, τότε το $\mathbb{R} = \mathbb{Q}\cup(\mathbb{R}\setminus\mathbb{Q})$ θα ήταν το πολύ αριθμήσιμο: η απόδειξη του Παραδείγματος 2.22 (με $X_0 = \mathbb{Q}$, $X_1 = \mathbb{R}\setminus\mathbb{Q}$ και $X_n = \emptyset$ για $n \geq 2$, γράφοντας κάθε X_n ως λίστα, πεπερασμένη ή άπειρη) δίνει ενριπτική συνάρτηση από το $\mathbb{R}$ στο $\mathbb{N}\times\mathbb{N}$. Αυτό αντιφάσκει με το ότι το $\mathbb{R}$ είναι υπεραριθμήσιμο.

11. (α) Αν $s_0, s_1, s_2, \dots$ ήταν μια απαρίθμηση του $\{0, 1\}^{\mathbb{N}}$ και $s_i = (s_{i0}, s_{i1}, \dots)$, τότε η ακολουθία t με $t_i = 1 - s_{ii}$ διαφέρει από κάθε s_i στη θέση i, άτοπο. (Εδώ δεν υπάρχει το πρόβλημα των δύο παραστάσεων της Παρατήρησης 2.23: διαφορετικές ακολουθίες είναι διαφορετικά στοιχεία.) (β) Η $A \mapsto (\chi_A(0), \chi_A(1), \chi_A(2), \dots)$ είναι αμφιμονοσήμαντη (Άσκηση 17 της Ενότητας 1.3). Άρα το $\mathcal{P}(\mathbb{N})$ είναι υπεραριθμήσιμο, όπως προβλέπει το Θεώρημα 2.24.

Κεφάλαιο 3. Λογική

Ενότητα 3.2

1. (α) Πρόταση, αληθής. (β) Όχι: η αλήθειά της εξαρτάται από το x (κατηγόρημα, Ενότητα 3.4). (γ) Όχι: δεν είναι δηλωτική. (δ) Πρόταση, ψευδής. (ε) Πρόταση (η εικασία των δίδυμων πρώτων), της οποίας η τιμή αλήθειας δεν είναι γνωστή.

2. (α) $p \wedge q$. (β) $p \to \neg q$. (γ) «Ο Γιάννης ή η Μαρία (ή και οι δύο) πέρασαν τα Μαθηματικά»· «Αν δεν πέρασαν και οι δύο, τότε η Μαρία πέρασε». (δ) Ξέρουμε την $p \to q$. (i) Τίποτα για τον Γιάννη. (ii) Ο Γιάννης δεν πέρασε (modus tollens).

3. (α) Αν χάσεις βάρος, τότε γυμνάζεσαι. (β) Αν γυμνάζεσαι, τότε θα χάσεις βάρος. (γ) Αν κάποιος είναι Αθηναίος, τότε είναι Έλληνας. (δ) Αν είσαι Έλληνας, τότε είσαι Αθηναίος. (ε) Αν ένας αριθμός είναι ρητός, τότε είναι πραγματικός. (στ) Αν ένας αριθμός δεν είναι άρτιος, τότε είναι πρώτος. (ζ) Αν η ομάδα μας παίξει στον τελικό, τότε θα τον κερδίσει.

4. Έστω $v(\varphi)$ το πλήθος των εμφανίσεων μεταβλητών και $b(\varphi)$ το πλήθος των εμφανίσεων των $\wedge, \vee, \to, \leftrightarrow$. Για μια μεταβλητή, $v = 1$ και $b = 0$. Ο $(\neg\varphi)$ έχει τα ίδια v, b με τον φ. Αν $v(\varphi) = b(\varphi)+1$ και $v(\psi) = b(\psi) + 1$, τότε για τον $(\varphi \wedge \psi)$ έχουμε $v = v(\varphi) + v(\psi) = (b(\varphi) + b(\psi) + 1) + 1 = b + 1$, και όμοια για τους άλλους συνδέσμους.

5. Ναι (νόμος του Peirce). Αν $u(p) = A$, ο τύπος είναι αληθής, αφού το συμπέρασμα p είναι αληθές. Αν $u(p) = \Psi$, τότε $\bar{u}(p \to q) = A$, άρα $\bar{u}((p \to q) \to p) = \Psi$, και ο τύπος είναι πάλι αληθής. Στο δενδροδιάγραμμα η ρίζα είναι ο κύριος σύνδεσμος $\to$, με παιδιά τον $(p \to q) \to p$ και τον p· για $u(p) = \Psi$, $u(q) = A$ βρίσκουμε, από τα φύλλα προς τη ρίζα, $\bar{u}(p \to q) = A$, $\bar{u}((p \to q) \to p) = \Psi$ και στη ρίζα την τιμή A.

6. Έστω ότι η u ικανοποιεί τους $p \to q$ και $\neg q \vee s$, και ότι $\bar{u}(p \wedge \neg s) = A$. Τότε $u(p) = A$ και $u(s) = \Psi$, άρα $u(q) = A$ από τον $p \to q$, οπότε $\bar{u}(\neg q \vee s) = \Psi$, άτοπο.

7. Αν $u(p) = A$, ο $(\neg p \to q) \to p$ είναι αληθής, άρα και ο τύπος. Αν $u(p) = \Psi$ και $u(q) = A$, τότε ο $\neg p \to \neg q$ είναι ψευδής, άρα ο τύπος αληθής. Αν $u(p) = u(q) = \Psi$, τότε ο $\neg p \to q$ είναι ψευδής, άρα ο $(\neg p \to q) \to p$ αληθής, και ο τύπος αληθής.

8. Οι $p \to q$ και $q \to r$ είναι και οι δύο αληθείς μόνο στις γραμμές (A, A, A), (Ψ, A, A), (Ψ, Ψ, A), (Ψ, Ψ, Ψ) των (p, q, r), και σε όλες είναι αληθής και η $p \to r$.

9. Ο πρώτος συνεπάγεται ταυτολογικά τον δεύτερο, αλλά όχι το αντίστροφο. Ο $p \leftrightarrow (q \leftrightarrow s)$ είναι αληθής ακριβώς όταν περιττό πλήθος από τους p, q, s είναι αληθείς, δηλαδή στις αποτιμήσεις AAA, $A\Psi\Psi$, $\Psi A\Psi$, $\Psi\Psi A$ (για τις τιμές των p, q, s με αυτή τη σειρά). Ο $(p \wedge q) \to s$ είναι ψευδής μόνο στην $AA\Psi$, που δεν είναι καμία από αυτές· άρα σε κάθε αποτίμηση που ο πρώτος είναι αληθής, είναι αληθής και ο δεύτερος. Στην $\Psi\Psi\Psi$ όμως ο δεύτερος είναι αληθής (η υπόθεση $p \wedge q$ είναι ψευδής) και ο πρώτος ψευδής, αφού κανένας από τους p, q, s δεν είναι αληθής.

10. Όχι. Έστω C: «είμαστε ξαδέλφια» και K: «είμαστε και οι δύο απατεώνες». Αν ήταν και οι δύο ιππότες, η K θα ήταν ψευδής και οι $C \to K$, $C \vee K$ αληθείς. Στον πίνακα αλήθειας των $C \to K$ και $C \vee K$, όμως, δεν υπάρχει γραμμή με K ψευδή στην οποία να είναι και οι δύο αληθείς: η πρώτη δίνει C ψευδή και η δεύτερη C αληθή.

11. Έστω P: «είχα ποπκόρν», Q: «είχα σάντουιτς με αγγούρι», R: «είχα σταφίδες», S: «ήπια σόδα», T: «ήπια τσάι». Οι δηλώσεις του είναι $P \vee R$, $Q \to S$, $\neg(S \vee T)$, και είναι όλες ψευδείς. Άρα ισχύουν οι αρνήσεις τους: $\neg P \wedge \neg R$, $Q \wedge \neg S$ και $S \vee T$. Από τη δεύτερη, Q και $\neg S$· τότε από την τρίτη, T. Ο Νίκος είχε σάντουιτς με αγγούρι και ήπιε τσάι (και τίποτα άλλο από όσα ανέφερε).

12. Με K: «καρό κοστούμι», Σ: «σανδάλια», M: «μοβ πουκάμισο», Γ: «γραβάτα ή παπιγιόν», έχουμε (1) $K \vee \Sigma$, (2) $(K \wedge M) \to \neg\Gamma$, (3) $K \to (M \vee \Sigma)$, (4) $\Sigma \to M$, και χθες Γ. Από τη (2), χθες ισχύει $\neg(K \wedge M)$. Αν ίσχυε K, τότε $\neg M$, άρα από την (3) Σ, άρα από την (4) M, άτοπο. Άρα $\neg K$· από την (1) Σ και από την (4) M. Ο Χολμς φορούσε το μαύρο κοστούμι, σανδάλια και μοβ πουκάμισο.

13. (α) Αν ο Όσκαρ πίνει γάλα, τότε τρώει κινέζικο φαγητό. (β) Αν ο Όσκαρ δεν πίνει γάλα, τότε δεν τρώει κινέζικο φαγητό. (γ) Ναι· τότε θα ήταν ψευδής και η αρχική (είναι ισοδύναμες), δηλαδή ο Όσκαρ θα έτρωγε κινέζικο χωρίς να πίνει γάλα. (δ) Όχι. (ε) Ναι: δεν τρώει κινέζικο φαγητό.

14. $\neg(\neg p \vee q) \equiv \neg\neg p \wedge \neg q \equiv p \wedge \neg q$, άρα ο τύπος είναι ισοδύναμος με τον $(p \wedge \neg q) \vee (\neg p \wedge q)$: «ακριβώς ένας από τους p, q είναι αληθής», δηλαδή με τον $\neg(p \leftrightarrow q)$.

15. (α) $(p \vee \neg q) \wedge (r \vee \neg s)$. (β) $\neg(\neg p \to \neg q) \vee \neg(\neg q \to r) \equiv (\neg p \wedge q) \vee (\neg q \wedge \neg r)$.

16. (α) $\varphi \equiv \psi$ σημαίνει ότι $\bar{u}(\varphi) = \bar{u}(\psi)$ για κάθε u, δηλαδή ότι $\bar{u}(\varphi \leftrightarrow \psi) = A$ για κάθε u. (β) $\varphi \vDash \psi$ σημαίνει ότι δεν υπάρχει u με $\bar{u}(\varphi) = A$ και $\bar{u}(\psi) = \Psi$, δηλαδή u που να κάνει ψευδή τον $\varphi \to \psi$. (γ) Μια u ικανοποιεί το $\{\varphi_1, \dots, \varphi_n\}$ αν και μόνον αν ικανοποιεί τον $\varphi_1 \wedge \cdots \wedge \varphi_n$· εφαρμόστε το (β).

17. (α) Το $\{A, \Psi\}^k$ έχει 2^k στοιχεία, άρα (Ενότητα 1.3) υπάρχουν 2^{2^k} συναρτήσεις $\{A, \Psi\}^k \to \{A, \Psi\}$, π.χ., 4, 16 και 256 για $k = 1, 2, 3$. (β) Αν ο φ αντιπροσωπεύει την f και ο ψ την g, τότε για κάθε αποτίμηση u έχουμε $\bar{u}(\varphi) = f(u(p_0), \dots, u(p_{k-1}))$ και $\bar{u}(\psi) = g(u(p_0), \dots, u(p_{k-1}))$· άρα $\varphi \equiv \psi$ αν και μόνο αν $f = g$. Από το Θεώρημα 3.19 κάθε συνάρτηση αντιπροσωπεύεται από έναν τύπο, οπότε παίρνουμε 2^{2^k} τύπους ανά δύο μη ισοδύναμους· αν όμως έχουμε περισσότερους από 2^{2^k} τύπους, δύο από αυτούς αντιπροσωπεύουν την ίδια συνάρτηση (αφού οι συναρτήσεις είναι μόνο 2^{2^k}), άρα είναι ισοδύναμοι. (γ) $2^{2^2} = 16$. Από αυτούς 2 είναι σταθεροί (πάντα A ή πάντα Ψ), 2 εξαρτώνται μόνο από την πρώτη μεταβλητή (οι p, $\neg p$) και 2 μόνο από τη δεύτερη, άρα $16 - 6 = 10$ εξαρτώνται και από τις δύο· ανάμεσά τους οι $\wedge$, $\vee$, $\to$, $\leftrightarrow$ και $\uparrow$.

18. Η g παίρνει την τιμή A στις (A, Ψ, Ψ), (Ψ, A, Ψ), (Ψ, Ψ, Ψ), άρα $\varphi = (p_0 \wedge \neg p_1 \wedge \neg p_2) \vee (\neg p_0 \wedge p_1 \wedge \neg p_2) \vee (\neg p_0 \wedge \neg p_1 \wedge \neg p_2)$. (Ισοδύναμα, $\neg p_2 \wedge \neg(p_0 \wedge p_1)$.)

19. Ο $(p_0 \wedge p_1) \vee (\neg p_0 \wedge p_2)$: αν η p_0 είναι αληθής, και οι δύο τύποι έχουν την τιμή της p_1, ενώ αν είναι ψευδής, την τιμή της p_2. (Η κατασκευή του κειμένου δίνει τον $(p_0 \wedge p_1 \wedge p_2) \vee (p_0 \wedge p_1 \wedge \neg p_2) \vee (\neg p_0 \wedge p_1 \wedge p_2) \vee (\neg p_0 \wedge \neg p_1 \wedge p_2)$.)

20. Ο τύπος είναι ψευδής μόνο στις γραμμές (A, Ψ, A) και (Ψ, A, A), άρα ο πίνακας αλήθειας δίνει τη διάζευξη έξι συζεύξεων, μία για καθεμία από τις (A, A, A), (A, A, Ψ), (A, Ψ, Ψ), (Ψ, A, Ψ), (Ψ, Ψ, A), (Ψ, Ψ, Ψ), π.χ., $p \wedge \neg q \wedge \neg r$ για την (A, Ψ, Ψ). Με τους νόμους: $p \leftrightarrow q \equiv (\neg p \vee q) \wedge (\neg q \vee p) \equiv (\neg p \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge \neg q) \vee (q \wedge p) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$, άρα ο τύπος είναι ισοδύναμος με τον $(p \wedge q) \vee (\neg p \wedge \neg q) \vee \neg r$.

21. Όπως στην απόδειξη της Πρότασης 3.23, για το $\{\neg, \vee\}$ αρκεί η $\varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$, και για το $\{\neg, \to\}$, αφού το $\{\neg, \vee\}$ είναι πλήρες, η $\varphi \vee \psi \equiv \neg\varphi \to \psi$. (Αυστηρά, η αντικατάσταση γίνεται σε όλους τους υποτύπους, με επαγωγή, Θεώρημα 3.5.)

Ενότητα 3.3

1. $P = \{3, 6, 9, 12, 15, 18\}$ και Q οι περιττοί. $p \wedge q$: $\{3, 9, 15\}$. $p \vee \neg q$: $\{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20\}$. $p \to q$: $P' \cup Q = \mathcal{U} \setminus \{6, 12, 18\}$. $\neg(p \leftrightarrow q)$: η συμμετρική διαφορά $P \triangle Q = \{1, 5, 6, 7, 11, 12, 13, 17, 18, 19\}$.

2. (α) Η $p(x) \leftrightarrow q(x)$ είναι αληθής αν και μόνον αν ($x \in P$ και $x \in Q$) ή ($x \notin P$ και $x \notin Q$). (β) Αν $P \subseteq Q$, τότε κάθε x είτε δεν ανήκει στο P είτε ανήκει στο Q, άρα $P' \cup Q = \mathcal{U}$. Αντίστροφα, αν $P' \cup Q = \mathcal{U}$ και $x \in P$, τότε $x \notin P'$, άρα $x \in Q$.

3. $P = \{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$, με 6 στοιχεία· το Q περιέχει όλα τα ζεύγη εκτός από τα (i, i), άρα έχει $36 - 6 = 30$ στοιχεία. Αφού $i + i \neq 7$, ισχύει $P \subseteq Q$, άρα η $p(x) \to q(x)$ είναι αληθής για κάθε x (Άσκηση 2). Η $q(x) \to p(x)$ όχι: π.χ., για $x = (1, 2)$.

Ενότητα 3.4

1. (α) $\exists x\,(P(x) \wedge \forall y\,(T(y) \to F(x, y)))$. (β) $\forall x\,(P(x) \to \exists y\,(T(y) \wedge F(x, y)))$· με μια άλλη ανάγνωση («υπάρχει στιγμή που κοροϊδεύεις όλους») $\exists y\,(T(y) \wedge \forall x\,(P(x) \to F(x, y)))$. (γ) $\neg\,\forall x\,\forall y\,((P(x) \wedge T(y)) \to F(x, y))$, ισοδύναμα $\exists x\,\exists y\,(P(x) \wedge T(y) \wedge \neg F(x, y))$.

2. (α) $\forall x\,(N(x) \to L(0, x))$ (ή, αν δεν θέλουμε να απαιτήσουμε $0 < 0$, $\forall x\,((N(x) \wedge \neg(x = 0)) \to L(0, x))$). (β) $\forall x\,(N(x) \to I(x)) \to I(0)$. (γ) $\neg\,\exists x\,(N(x) \wedge L(x, 0))$. (δ) $\neg\,\exists x\,(N(x) \wedge \forall y\,(N(y) \to L(y, x)))$. (ε) $\neg\,\exists x\,(N(x) \wedge \forall y\,(N(y) \to \neg L(y, x)))$.

3. Ψευδής: για $x = 0$ δεν υπάρχει y με $0 \cdot y = 1$. Η άρνηση $\exists x\,\forall y\,(xy \neq 1)$ είναι αληθής, με $x = 0$.

4. $\exists x\,\forall y\,(y \neq x \to G(x, y))$. Άρνηση: $\forall x\,\exists y\,(y \neq x \wedge \neg G(x, y))$, δηλαδή «κάθε φοιτητής έχει κάποιον συμφοιτητή του που δεν γνωρίζει».

5. (α) Κάθε κωμικός είναι αστείος. (β) Όλοι οι άνθρωποι είναι κωμικοί και αστείοι. (γ) Υπάρχει άνθρωπος που, αν είναι κωμικός, είναι αστείος· είναι αληθής μόλις υπάρχει έστω ένας άνθρωπος που δεν είναι κωμικός (κενά αληθής συνεπαγωγή). (δ) Υπάρχει κωμικός που είναι αστείος.

6. (α) $\exists x\,(C(x) \wedge D(x) \wedge F(x))$. (β) $\forall x\,(C(x) \vee D(x) \vee F(x))$. (γ) $\exists x\,(C(x) \wedge F(x) \wedge \neg D(x))$. (δ) $\neg\,\exists x\,(C(x) \wedge D(x) \wedge F(x))$. (ε) $\exists x\,C(x) \wedge \exists x\,D(x) \wedge \exists x\,F(x)$.

7. (α) $\forall y\,\forall x\,\neg P(x, y)$. (β) $\exists x\,\forall y\,\neg P(x, y)$. (γ) $\forall y\,(\neg Q(y) \vee \exists x\,R(x, y))$. (δ) $\forall y\,(\forall x\,\neg R(x, y) \wedge \exists x\,\neg S(x, y))$. (ε) $\forall y\,(\exists x\,\forall z\,\neg T(x, y, z) \wedge \forall x\,\exists z\,\neg U(x, y, z))$.

8. (α) $\neg\,\exists x\,(E(x) \wedge O(x))$. (β) $\forall x\,(E(x) \to O(x + 1))$. (γ) $\exists x\,(P(x) \wedge E(x))$. (δ) $\forall x\,\forall y\,(x < y \to \exists z\,(x < z \wedge z < y))$. (ε) $\forall x\,\neg\,\exists y\,(x < y \wedge y < x + 1)$. Για τους ακεραίους είναι αληθείς όλες εκτός από τη (δ) (για $x = 0$, $y = 1$).

9. (α) Αληθής στο $[0, \infty)$, ψευδής στο $\mathbb{N}$ (για $x = 2$) ή στο $\mathbb{R}$ (για $x = -1$). (β) Αληθής στο $\mathbb{Q}$ (με $z = (x + y)/2$), ψευδής στο $\mathbb{Z}$ (για $x = 0$, $y = 1$). (γ) Αληθής στο $\{0, 1, 2\}$ με $x = 1$ (ελέγξτε τα τρία ζεύγη $y < z$)· ψευδής στο $\mathbb{N}$, αφού για κάθε x τα $y = x + 1$, $z = x + 2$ δεν ικανοποιούν την $y \leq x$.

10. Ναι: αν το σύμπαν περιέχει ένα στοιχείο u, τότε η $P(u)$ είναι αληθής, άρα και η $\exists x\,P(x)$. Η αντίστροφη όχι: με σύμπαν το $\mathbb{N}$ και $P(x)$: «$x = 0$». Σε κενό σύμπαν η $\forall x\,P(x)$ είναι (κενά) αληθής και η $\exists x\,P(x)$ ψευδής, οπότε η συνεπαγωγή είναι ψευδής.

11. (α) Υπάρχει ακέραιος που δεν είναι ούτε άρτιος ούτε περιττός. (β) Υπάρχει πρώτος n τέτοιος ώστε και ο $n+3$ να είναι πρώτος. (γ) $\exists x\,\exists y\,(\neg(x<y)\wedge\neg(y<x))$. (δ) $\exists x\,P(x)\wedge\exists y\,\neg P(y)$. Η (β) είναι ψευδής: για $n=2$ ο $n+3=5$ είναι πρώτος. (Είναι το μόνο αντιπαράδειγμα, αφού για περιττό πρώτο n ο $n+3$ είναι άρτιος μεγαλύτερος του 2.)

12. (α) Ένα επιχείρημα για ένα αυθαίρετο στοιχείο x. (β) Ένα αντιπαράδειγμα: ένα x με την $P(x)$ ψευδή. (γ) Ένα παράδειγμα: ένα x με την $P(x)$ αληθή. (δ) Ένα επιχείρημα ότι η $P(x)$ είναι ψευδής για αυθαίρετο x (δηλαδή απόδειξη της $\forall x\,\neg P(x)$).

Ενότητα 3.5

1. (α) Μη έγκυρο ($\{p\to q,\ q\}\not\vdash p$), άρα ούτε ορθό. (β) Έγκυρο, αλλά όχι ορθό: η πρώτη προκείμενη είναι ψευδής. (γ) Έγκυρο (modus tollens) και ορθό: η πρώτη προκείμενη είναι κενά αληθής, αφού ο 7 δεν είναι άρτιος, και η δεύτερη αληθής.

2. Αυτό που πραγματικά αποδείχτηκε είναι η συνεπαγωγή $(1=3)\to(1=1)$, που είναι πράγματι αληθής (η υπόθεσή της είναι ψευδής, και άλλωστε το συμπέρασμά της είναι αληθές). Από μια αληθή συνεπαγωγή $P\to Q$ με Q αληθή δεν συμπεραίνουμε τίποτα για την P· θα χρειαζόμασταν την αντίστροφη, $(1=1)\to(1=3)$, που είναι ψευδής. Το επιχείρημα δεν αποδεικνύει ότι $1=3$.

3. (α) Αν $u(s)=A$ και $u(t)=\Psi$, τότε ο $s\wedge\neg t$ είναι αληθής και ο $\neg s$ ψευδής, άρα η u δεν ικανοποιεί τον $(s\wedge\neg t)\to\neg s$. (β) Όμοια, αφού ο $r\wedge\neg r$ είναι πάντα ψευδής. (γ) Αφού $r\wedge\neg r\equiv\Psi$ και $\varphi\to\Psi\equiv\neg\varphi$, ο τύπος είναι ισοδύναμος με τον $\neg(s\wedge\neg t)\equiv\neg s\vee t\equiv s\to t$.

4. (α) Αντίστροφη: «για κάθε n, αν ο n είναι μονήρης, τότε είναι πρώτος». Αντιθετοαντίστροφη: «για κάθε n, αν ο n δεν είναι μονήρης, τότε δεν είναι πρώτος». (β) «Υπάρχει πρώτος n που δεν είναι μονήρης»· αρκεί να βρούμε έναν τέτοιο πρώτο (ένα αντιπαράδειγμα). (γ) Τίποτα για την αρχική και την αντιθετοαντίστροφη (ο 8 δεν είναι πρώτος, άρα η συνεπαγωγή για $n=8$ είναι κενά αληθής)· η αντίστροφη όμως είναι ψευδής, με αντιπαράδειγμα τον 8. (δ) $P\subseteq S$ (Ενότητα 3.3), και αφού $8\in S\setminus P$, μάλιστα $P\subsetneq S$. (ε) (i) «Έστω ότι ο n είναι πρώτος. ... Άρα ο n είναι μονήρης.» (ii) «Έστω ότι ο n δεν είναι μονήρης. ... Άρα ο n δεν είναι πρώτος.» (iii) «Έστω ότι ο n είναι πρώτος και δεν είναι μονήρης. ... Άρα ο n δεν είναι πρώτος (ή: άρα ο n είναι μονήρης), άτοπο. Επομένως, αν ο n είναι πρώτος, τότε είναι μονήρης.»

5. Έστω P: «ο ab είναι άρτιος», S: «ο a είναι άρτιος», R: «ο b είναι άρτιος». (α) Έγκυρη: αποδεικνύει την $\neg(S\vee R)\to\neg P$, την αντιθετοαντίστροφη της $P\to(S\vee R)$. (β) Μη έγκυρη: αποδεικνύει την αντίστροφη $(S\vee R)\to P$. (γ) Έγκυρη: απαγωγή σε άτοπο από τις P και $\neg(S\vee R)$. (δ) Έγκυρη: αποδεικνύει την $(P\wedge\neg S)\to R$, που είναι ισοδύναμη με την $P\to(S\vee R)$.

6. (α) Αληθής: $n+(n+1)+(n+2)=3(n+1)$ και $n+1\in\mathbb{Z}$. (β) Αληθής: η πρόταση είναι η «αν $6\mid n$, τότε $2\mid n$» (Ενότητα 3.2), και αν $n=6k$, τότε $n=2(3k)$. (γ) Αληθής: αν $b=ka$, τότε $b^2=k^2a^2$ και $k^2\in\mathbb{Z}$. (δ) Ψευδής: για $a=2$, $b=c=1$ έχουμε $2\mid 1+1$, αλλά $2\nmid 1$. (ε) Ψευδής: για $a=4$, $b=c=2$ έχουμε $4\mid 2\cdot 2$, αλλά $4\nmid 2$ (ή $a=6$, $b=2$, $c=3$). (Η (ε) ισχύει όμως όταν ο a είναι πρώτος.)

7. $\frac{(x+y)^2}{4}-xy=\frac{(x-y)^2}{4}$, που είναι 0 αν και μόνον αν $x=y$.

8. (α) Αντιθετοαντίστροφη: «αν ο a ή ο b είναι περιττός, τότε ο $a+b$ είναι περιττός». Αντίστροφη: «αν οι a, b είναι άρτιοι, τότε ο $a+b$ είναι άρτιος». Άρνηση: «υπάρχουν ακέραιοι a, b με τον $a+b$ άρτιο και τον a ή τον b περιττό». (β) Η αρχική και η αντιθετοαντίστροφη είναι ψευδείς ($a=b=1$)· η αντίστροφη είναι αληθής (Παράδειγμα 3.39), και η άρνηση αληθής ($a=b=1$).

9. Με αντιθετοαντιστροφή: αν ο $n=2k$ είναι άρτιος, τότε $n^3=8k^3=2(4k^3)$ είναι άρτιος.

10. (α) «Αν $|A|>|B|$, τότε $A\not\subseteq B$». Είναι αληθής: αν ήταν $A\subseteq B$, η $a\mapsto a$ θα ήταν ενριπτική συνάρτηση $A\to B$, που αντιφάσκει με την αρχή του περιστερώνα (Πόρισμα 3.45 της επόμενης ενότητας). (β) «Αν $|A|\le|B|$, τότε $A\subseteq B$»· ψευδής, π.χ., για $A=\{1,2\}$, $B=\{3,4,5\}$.

11. Αν ο 3 δεν διαιρεί τον n, τότε $n = 3k+1$ ή $n = 3k+2$, και $n^2 = 3(3k^2+2k)+1$ ή $n^2 = 3(3k^2+4k+1)+1$, οπότε ο 3 δεν διαιρεί τον n^2. Στη συνέχεια όπως για τον $\sqrt{2}$: από $m^2 = 3n^2$ έχουμε $m = 3k$, άρα $n^2 = 3k^2$ και ο 3 διαιρεί και τον n, άτοπο.

12. Αν ο $x = 2k$ είναι άρτιος, $x^2 = 4k^2$· αν $x = 2k+1$, $x^2 = 4(k^2+k)+1$. Άρα $x^2 = 4y+3$ θα έδινε $4(k^2-y) = 3$ ή $4(k^2+k-y) = 2$, αδύνατο για ακεραίους.

13. (α) Με $2j$ γραμματόσημα των 5 και $2k$ των 8 λεπτών το ποσό είναι $10j+16k = 2(5j+8k)$, δηλαδή ακριβώς τα διπλάσια των ποσών $5j+8k$ που πληρώνονται με γραμματόσημα των 5 και των 8 λεπτών. Αυτά είναι όλα τα ποσά από 28 και πάνω (Πρόταση 2.12) και, κάτω από το 28, τα $0, 5, 8, 10, 13, 15, 16, 18, 20, 21, 23, 24, 25, 26$. Άρα πληρώνονται ακριβώς όλα τα άρτια ποσά από 56 και πάνω και τα $0, 10, 16, 20, 26, 30, 32, 36, 40, 42, 46, 48, 50, 52$· το μεγαλύτερο άρτιο ποσό που δεν πληρώνεται έτσι είναι το 54. (β) Με αντιθετοαντιστροφή: αν και τα δύο πλήθη είναι περιττά, $5(2j+1)+8(2k+1) = 2(5j+8k+6)+1$ είναι περιττό. (γ) Με απαγωγή σε άτοπο: με το πολύ 5 από κάθε είδος, το ποσό είναι το πολύ $5\cdot 5+5\cdot 8 = 65 < 72$.

Ενότητα 3.6

1. Βάση ($k=1$): κάθε $f : \mathbb{N}_2 \to \mathbb{N}_1$ έχει $f(1) = f(2) = 1$. Βήμα: έστω ότι δεν υπάρχει ενριπτική $\mathbb{N}_{k+1} \to \mathbb{N}_k$, και έστω ενριπτική $f : \mathbb{N}_{k+2} \to \mathbb{N}_{k+1}$. Αν κανένα $i \le k+1$ δεν έχει $f(i) = k+1$, ο περιορισμός της f στο $\mathbb{N}_{k+1}$ είναι ενριπτική συνάρτηση $\mathbb{N}_{k+1} \to \mathbb{N}_k$, άτοπο. Αλλιώς, $f(i) = k+1$ για κάποιο $i \le k+1$, και $f(k+2) \ne k+1$· η g που προκύπτει από την f ανταλλάσσοντας τις τιμές της στα i και $k+2$ είναι ενριπτική και μας φέρνει στην πρώτη περίπτωση.

2. Αν τα άτομα είναι $n \ge 2$, ο αριθμός γνωριμιών κάθε ατόμου είναι ένας από τους $0, 1, \dots, n-1$. Οι τιμές 0 και $n-1$ δεν μπορούν να εμφανιστούν και οι δύο: αν κάποιος γνωρίζει όλους τους άλλους, κανείς δεν έχει 0 γνωριμίες. Άρα οι n αριθμοί γνωριμιών παίρνουν το πολύ $n-1$ διαφορετικές τιμές, και από την αρχή του περιστερώνα δύο άτομα έχουν τον ίδιο.

3. (α) $\lceil 40/6 \rceil = 7$. (β) 10. Με 9 ζάρια δεν αρκεί: τρία ζάρια με 1, τρία με 2 και τρία με 3. Με 10 ζάρια, αν εμφανίζονται τουλάχιστον τέσσερις διαφορετικές ενδείξεις, παίρνουμε τέσσερα ζάρια με διαφορετικές ενδείξεις· αλλιώς τα 10 ζάρια έχουν το πολύ 3 ενδείξεις, και κάποια ένδειξη εμφανίζεται τουλάχιστον $\lceil 10/3 \rceil = 4$ φορές.

4. (α) Τα δυνατά υπόλοιπα της διαίρεσης με το n είναι τα n στοιχεία $0, 1, \dots, n-1$. Από την αρχή του περιστερώνα (Πόρισμα 3.45), δύο από τους $n+1$ ακεραίους, έστω $x = qn+r$ και $y = q'n+r$, έχουν το ίδιο υπόλοιπο r, άρα $x-y = (q-q')n$. Για n ακεραίους όχι: οι $0, 1, \dots, n-1$ έχουν διαφορές $1, \dots, n-1$ σε απόλυτη τιμή. (β) Θέτουμε $s_0 = 0$ και $s_j = x_1+\cdots+x_j$ για $j = 1, \dots, n$. Από το (α) για τους $n+1$ αριθμούς $s_0, s_1, \dots, s_n$, υπάρχουν $i < j$ με $n \mid s_j - s_i = x_{i+1}+\cdots+x_j$. (Ο s_0 χρειάζεται: χωρίς αυτόν θα είχαμε μόνο n αριθμούς.)

5. Χωρίζουμε τις θέσεις $1, \dots, 115$ σε «αλυσίδες» ανάλογα με το υπόλοιπο της διαίρεσης με το 4 (π.χ., $1, 5, 9, \dots, 113$), και κάθε αλυσίδα σε διαδοχικά ζεύγη $\{1,5\}, \{9,13\}, \dots$. Οι τρεις αλυσίδες με 29 θέσεις δίνουν 14 ζεύγη και μία μεμονωμένη θέση η καθεμία, και η αλυσίδα με 28 θέσεις 14 ζεύγη: συνολικά $3\cdot 15+14 = 59$ «φωλιές». Τα 60 επεισόδια που έχετε δει δίνουν δύο στην ίδια φωλιά, δηλαδή σε θέσεις που απέχουν 4.

6. (α) $-4, -3, 7, 77$. (β) Ο $\lfloor -x \rfloor$ είναι ο μεγαλύτερος ακέραιος $\le -x$, άρα ο $-\lfloor -x \rfloor$ είναι ο μικρότερος ακέραιος $\ge x$. (γ) Για $n = 2k$ έχουμε $k+k$, και για $n = 2k+1$ έχουμε $k+(k+1)$.

7. Έστω $n = qk+r$ με $0 \le r < k$. Βάζουμε $q+1$ αντικείμενα σε r κουτιά και q στα υπόλοιπα $k-r$. Αν $r = 0$ τότε $\lceil n/k \rceil = q$, και αν $r > 0$ τότε $\lceil n/k \rceil = q+1$, αφού $q < n/k < q+1$.

8. Κάθε $x \in \{1, \dots, 2n\}$ γράφεται ως $2^a m$ με m περιττό, και ο m είναι ένας από τους n περιττούς $1, 3, \dots, 2n-1$. Από τους $n+1$ αριθμούς, δύο έχουν το ίδιο m: $2^a m$ και $2^b m$ με $a < b$, και ο πρώτος διαιρεί τον δεύτερο.

9. $R_1 = \{1,2\}$, $R_2 = \{3\}$, $R_3 = \{1,3\}$ και $D = \{2\}$: το 1 ανήκει στο R_1 αλλά όχι στο D, το 2 ανήκει στο D αλλά όχι στο R_2, και το 3 ανήκει στο R_3 αλλά όχι στο D.

10. (α) $n \in f(n)$ για κάθε n, άρα $D = \emptyset$, που δεν είναι τιμή της f αφού κάθε $f(n)$ περιέχει το 0. (β) $n \notin f(n)$ για κάθε n, άρα $D = \mathbb{N}$, που δεν είναι τιμή της f αφού κανένα $f(n)$ δεν περιέχει το 0.

??. $\omega^2 - \omega - 12 = (\omega - 4)(\omega + 3) = 0$, με ρίζες 4 και -3. Για $r \neq 0$, η r^n ικανοποιεί τη σχέση αν και μόνο αν $r^2 = r + 12$ (διαιρώντας με r^{n-2}), δηλαδή αν το r είναι ρίζα: οι ακολουθίες 4^n και $(-3)^n$.

??. (α) Ναι, για κάθε n: $3 \cdot 2^{n-1} - 2 \cdot 2^{n-2} = 3 \cdot 2^{n-1} - 2^{n-1} = 2^n$. (Το ότι οι πρώτοι όροι ταιριάζουν δεν αρκεί· πρέπει να ελέγξουμε τη σχέση για κάθε n.) (β) Ρίζες 1, 2· $a_n = A + B\,2^n$ με $A + B = 1$, $A + 2B = 5$, άρα $a_n = 4 \cdot 2^n - 3$. (γ) Βάση $a_0 = a_1 = 1$· για $n \geq 2$, αν $a_{n-1} = a_{n-2} = 1$, τότε $a_n = 3 - 2 = 1$.

??. Ρίζες $4, -1$: $a_n = a \cdot 4^n + b(-1)^n$, με $a+b = 2$ και $4a-b = 3$. Άρα $a = b = 1$ και $a_n = 4^n + (-1)^n$.

??. (α) $2, 2, 6, 10, 22, 42, 86, \ldots$ (β) Έστω L_n και M_n τα μεγάλα και τα μικρά κουνελάκια την ημέρα n, και $T_n = L_n + M_n$. Τότε $L_n = L_{n-1} + M_{n-1} = T_{n-1}$ και $M_n = 2L_{n-1} = 2T_{n-2}$, άρα $T_n = T_{n-1} + 2T_{n-2}$, με $T_0 = T_1 = 2$. (γ) Ρίζες $2, -1$: $T_n = \frac{1}{3}(2^{n+2} + 2(-1)^n)$.

??. (α) $F_1^2 + \cdots + F_n^2 = F_n\,F_{n+1}$: $1 = 1 \cdot 1$, $2 = 1 \cdot 2$, $6 = 2 \cdot 3$, $15 = 3 \cdot 5$, $40 = 5 \cdot 8$. (β) Βήμα: $F_nF_{n+1} + F_{n+1}^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1}F_{n+2}$. (γ) Το ορθογώνιο $8 \times 13 = F_6 \times F_7$ χωρίζεται σε τετράγωνα με πλευρές $1, 1, 2, 3, 5, 8$, δηλαδή $F_1, \ldots, F_6$: κάθε φορά που προσθέτουμε ένα τετράγωνο πλευράς F_{n+1} στη μεγάλη πλευρά ενός ορθογωνίου $F_n \times F_{n+1}$, παίρνουμε ένα ορθογώνιο $F_{n+1} \times F_{n+2}$.

??. Για $n = 1, 2$ ελέγχουμε απευθείας ($\varphi^{-1} \leq 1 \leq 1$ και $1 \leq 1 \leq \varphi$). Για $n \geq 3$, $F_n = F_{n-1} + F_{n-2} \leq \varphi^{n-2} + \varphi^{n-3} = \varphi^{n-3}(\varphi + 1) = \varphi^{n-1}$, και όμοια $F_n \geq \varphi^{n-3} + \varphi^{n-4} = \varphi^{n-2}$. Άρα $\log_{10} F_n$ είναι περίπου $n \log_{10} \varphi \approx 0{,}209\,n$.

??. Έστω s_n το πλήθος. Τα υποσύνολα που δεν περιέχουν το n είναι s_{n-1}· αυτά που το περιέχουν δεν περιέχουν το $n-1$, και προκύπτουν από ένα υποσύνολο του $\{1, \ldots, n-2\}$: s_{n-2}. Άρα $s_n = s_{n-1} + s_{n-2}$, με $s_0 = 1$, $s_1 = 2$, και $s_n = F_{n+2}$. (Το χαρακτηριστικό διάνυσμα ενός τέτοιου υποσυνόλου είναι ακριβώς μια λέξη 0-1 χωρίς δύο διαδοχικούς άσσους.)

??. (α) Αν αγνοήσουμε το πρώτο γράμμα, οι λέξεις που αρχίζουν με 0 (όπως και αυτές που αρχίζουν με 1) σχηματίζουν ένα αντίγραφο του Q_{n-1}, και κάθε λέξη $0w$ είναι γειτονική με ακριβώς μία λέξη του άλλου αντιγράφου, την $1w$. Άρα $e_n = 2e_{n-1} + 2^{n-1}$. (β) Ειδική λύση $Bn2^n$ με $B = \frac{1}{2}$, και από την $e_1 = 1$ προκύπτει $e_n = n\,2^{n-1}$. Από το Λήμμα των Χειραψιών: 2^n κορυφές βαθμού n, άρα $n2^n/2$ ακμές. (γ) Διμερές: οι λέξεις με άρτιο και με περιττό πλήθος άσσων. Για τον κύκλο του Hamilton: για $n = 2$ είναι ο C_4· αν $w_1, \ldots, w_N$ ($N = 2^{n-1}$) είναι ένας κύκλος του Hamilton του Q_{n-1}, τότε ο $0w_1, 0w_2, \ldots, 0w_N, 1w_N, 1w_{N-1}, \ldots, 1w_1, 0w_1$ είναι κύκλος του Hamilton του Q_n.

??. Για $\beta \neq c$: ειδική λύση $B\beta^n$ με $B = \frac{d\beta}{\beta - c}$, και $y_n = (y_0 - B)\,c^n + B\beta^n$. Για $\beta = c$: ειδική λύση Bnc^n με $B = d$, και $y_n = (y_0 + dn)\,c^n$. Στο Παράδειγμα **??** ($c = \beta = 2$, $d = 1$, $y_0 = 0$) παίρνουμε $k\,2^k$· στην Άσκηση **??** ($c = 4$, $\beta = 3$, $d = 1$, $y_0 = 1$) $B = -3$ και $a_n = 4 \cdot 4^n - 3 \cdot 3^n$.

Βιβλιογραφία

[BM] J. A. Bondy, U. S. R. Murty, *Graph Theory with Applications*, North-Holland, 1976.

[Epp] S. S. Epp, *Discrete Mathematics with Applications*, 4th edition, Brooks/Cole (Cengage Learning), 2011.

[GKP] R. L. Graham, D. E. Knuth, O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd edition, Addison-Wesley, 1994.

[Lev] O. Levin, *Discrete Mathematics: An Open Introduction*, 4η έκδοση, 2025 (έντυπη έκδοση: CRC Press). Ελεύθερα διαθέσιμο, με την άδεια CC BY-NC-SA 4.0, στη διεύθυνση `https://discrete.openmathbooks.org`.

[LL] S. Lipschutz, M. Lipson, *Schaum's Outline of Discrete Mathematics*, 3rd edition, McGraw-Hill, 2007.

[Liu] C. L. Liu, *Elements of Discrete Mathematics*, McGraw-Hill International Editions, Computer Science Series.

[LPV] L. Lovász, J. Pelikán, K. Vesztergombi, *Discrete Mathematics: Elementary and Beyond*, Undergraduate Texts in Mathematics, Springer, 2003.

[MAA] R. J. McEliece, R. B. Ash, C. Ash, *Introduction to Discrete Mathematics*, McGraw-Hill International Editions, Computer Science Series.

[Pól] G. Pólya, *Πώς να το λύσω*, Εκδόσεις Καρδαμίτσα, 1998 (μετάφραση του *How to Solve It*, 1945).

[Ros] K. H. Rosen, *Discrete Mathematics and its Applications*, 6th edition, McGraw-Hill (International Edition), 2007.

[Vel] D. J. Velleman, *How to Prove It: A Structured Approach*, 3rd edition, Cambridge University Press, 2019.

[Χαρ] Χ. Χαραλαμπίδης, *Συνδυαστική*.