Σημειώσεις του Μαθήματος

ΜΕΜ 103
Θεμέλια των Μαθηματικών

Βασισμένες στο βιβλίο των I.Stewart και D.Tall

Χρήστος Κουρουνιώτης

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

2018

Εισαγωγή

Αρχίζοντας τη μελέτη των μαθηματικών στο Πανεπιστήμιο, ας προσπαθήσουμε να αναλογιστούμε πώς δημιουργούνται τα μαθηματικά. Τα μαθηματικά είναι δραστηριότητα του ανθρώπινου μυαλού. Ενας υπολογιστής στον οποίο θα είχαμε καταγράψει όλους τους κανόνες της λογικής, θα μπορούσε να δημιουργήσει, με τυχαίο τρόπο, προτάσεις και να ελέγξει εάν αυτές είναι αληθείς ή όχι. Το ανθρώπινο μυαλό όμως, αν και μπορεί να ελέγξει ένα-ένα τα λογικά βήματα, δουλεύει κυρίως με άλλο τρόπο. Επιδιώκει μια συνολική εικόνα, από την οποία μπορεί να κατανοήσει όλο το επιχείρημα, συνθέτοντας τις ιδέες σε μια γενικώτερη δομή και συνδέοντας αυτές με άλλες ιδέες. Ο συνδυασμός της λογικής ανάλυσης και της συνολικής προσέγγισης δίδει τα καλύτερα αποτελέσματα.

Καθώς ένας άνθρωπος αποκτά μαθηματικές πληροφορίες, τις συνθέτει σε μια **μαθηματική έννοια**. Αργότερα μπορεί να εμφανιστούν νέες πληροφορίες, που να μην ταιριάζουν με τη μαθηματική έννοια που έχει δημιουργηθεί στο μυαλό του. Οταν συμβεί αυτό, και αφού ελεγχθεί η ορθότητα των νέων στοιχείων, μπορεί να χρειαστεί να τροποποιηθεί η αρχική συνολική εικόνα, αναμορφώνοντας ή δημιουργώντας μια νέα, πιο εκλεπτυσμένη μαθηματική έννοια. Οσο συμβαίνει αυτό, προκαλείται σύγχυση. Για να προχωρήσει η διαδικασία ο μαθηματικός πρέπει να μην χάσει την εμπιστοσύνη ώστε να ξεπεράσει τη σύγχυση.

Η διαδικασία με την οποία δημιουργούνται μαθηματικές έννοιες δεν είναι λογική και ευθύγραμμη. Ο μαθηματικός ψάχνει στις γνώσεις και τις εμπειρίες του, για να πιαστεί κάπου. Σε κάποια φάση, οι διάφορες ιδέες μπορεί να αρχίσουν να ταιριάζουν. Στο τέλος, μπορεί όλες οι βασικές ιδέες να συνδυαστούν σε μια σύντομη, στρωτή και λογική απόδειξη.

Σαν απόφοιτοι Λυκείου, γνωρίζετε ήδη πολλές μαθηματικές έννοιες. Στόχος των σπουδών σας στο Πανεπιστήμιο είναι να κτίσετε σε αυτές τις έννοιες και να τις εκλεπτύνετε σε ένα ανώτερο επίπεδο μαθηματικής ωριμότητας. Για να το πετύχουμε αυτό πρέπει να ξεκινήσουμε από παραδείγματα που βασίζονται σε γνωστές έννοιες, και στη βάση αυτών να κατασκευάσουμε νέες έννοιες.

Αυτή η διαδικασία δεν έχει καμία σχέση με μια αξιωματική κατασκευή όλων των μαθηματικών από το κενό, η οποία είναι εφικτή και μπορεί να έχει φιλοσοφικό ενδιαφέρον, αλλά δεν έχει ιδιαίτερη διδακτική χρησιμότητα.

Μεγάλο μέρος της μαθησιακής διαδικασίας συνίσταται στην ανακατασκευή πρότερων μαθηματικών εννοιών, για να προσαρμοστούν σε νέες ιδέες. Αυτή η διαδικασία είναι που προκαλεί σύγχυση. Πρέπει να περιμένετε οτι θα συναντήσετε περιόδους σύγχυσης στις σπουδές σας. Οταν αυτές δεν οφείλονται σε ελλειπή εξήγηση εκ μέρους των διδασκόντων ή απλώς παρερμηνεία, πρέπει να τις θεωρείτε χρήσιμες και ευπρόσδεκτες. Είναι ένδειξη οτι συντελείται πρόοδος στις γνώσεις σας.

Ενα καλό παράδειγμα είναι η σύγχυση που προκάλεσε στους μαθηματικούς, για αρκετούς αιώνες, η έννοια των μιγαδικών αριθμών. Ηταν γνωστό οτι το τετράγωνο ενός αριθμού διαφορετικού από το μηδέν, είτε θετικού είτε αρνητικού, είναι πάντοτε θετικό. Αρα η τετραγωνική ρίζα του -1 δεν μπορούσε να είναι ούτε θετικός ούτε αρνητικός αριθμός, και δεν υπήρχε θέση πάνω στην ευθεία των αριθμών για μια τέτοια ποσότητα. Για να ξεπεραστεί η σύγχυση ήταν απαραίτητο να τροποποιηθεί η έννοια των αριθμών, που συνδεόταν με σημεία μας ευθείας. Η τετραγωνική ρίζα του -1 έχει τη θέση της όχι στην ευθεία αλλά στο επίπεδο.

Σε αυτό το μάθημα θα προσπαθήσουμε, ξεκινώντας από τις γνωστές μαθηματικές έννοιες, να γνωρίσουμε σταδιακά νέες ιδέες, να αναμορφώσουμε τις σημαντικές γνώσεις που ήδη έχετε στα μαθηματικά, με τρόπο ώστε να προετοιμαστείτε για την προχωρημένη μελέτη των μαθηματικών. Πριν δώσουμε ορισμούς νέων εννοιών θα εξετάζουμε, στις διαλέξεις και στα εργαστήρια προβλημάτων, αρκετά παραδείγματα στα οποία να βασίσουμε τις νέες έννοιες.

Οι σημειώσεις αυτές είναι βασισμένες, στο μεγαλύτερο μέρος τους, στο βιβλίο Foundations of Mathematics των I.Stewart και D.Tall, Oxford University Press.

Περιεχόμενα

Κεφάλαιο 1

Σύνολα

Η έννοια του συνόλου θεωρείται θεμελιώδης στα σύγχρονα μαθηματικά — περισσότερο ακόμη και από την έννοια του αριθμού. Ένας από τους λόγους είναι οτι η γλώσσα των συνόλων μας επιτρέπει να διατυπώνουμε μαθηματικές ιδιότητες με μεγάλη γενικότητα: το Πυθαγόρειο Θεώρημα είναι σημαντικό γιατί ισχύει σε κάθε ορθογώνιο τρίγωνο, δηλαδή εκφράζει μια ιδιότητα του συνόλου των ορθογωνίων τριγώνων.

Η έννοια του συνόλου είναι αρχική της Θεωρίας Συνόλων, συνεπώς δεν ορίζεται στη βάση κάποιων απλούστερων εννοιών, ακριβώς όπως η έννοια του αριθμού στην Αριθμητική ή του σημείου στη Γεωμετρία. Αυτό δεν θα μας εμποδίσει να αποκτήσουμε μια αρκετά σαφή εικόνα για το τι είναι ένα σύνολο. Σύνολο είναι μια οποιαδήποτε συλλογή από αντικείμενα. Μπορεί να περιέχει πεπερασμένο ή άπειρο πλήθος αντικειμένων, ή ακόμα κανένα αντικείμενο. Τα αντικείμενα δεν είναι απαραίτητο να είναι ομοειδή. Μπορούμε να θεωρήσουμε ένα σύνολο από τρείς αριθμούς, δύο τρίγωνα και μια συνάρτηση.

Για να μελετήσουμε όλα τα σύνολα που εμφανίζονται στα Μαθηματικά, είναι χρήσιμο να ξεκινήσουμε με τις γενικές ιδιότητες που είναι κοινές σε όλα τα σύνολα. Στο πρώτο μέρος του μαθήματος θα εξετάσουμε διάφορους τρόπους να συνθέτουμε ή να τροποποιούμε κάποια σύνολα για να δημιουργήσουμε νέα σύνολα.

Στοιχεία. Ισότητα συνόλων

Τα αντικείμενα από τα οποία αποτελείται ένα σύνολο ονομάζονται **στοιχεία** του συνόλου. Λέμε οτι τα στοιχεία ενός συνόλου **ανήκουν** σ' αυτό. Για να συμβολίσουμε οτι το στοιχείο x ανήκει στο σύνολο S γράφουμε

$$x \in S.$$

Εάν το x δεν ανήκει στο S γράφουμε

$$x \notin S.$$

Για να γνωρίζουμε ποιό σύνολο εξετάζουμε, πρέπει να γνωρίζουμε ακριβώς ποιά είναι τα στοιχεία του. Και αντίστροφα, εάν γνωρίζουμε ακριβώς τα στοιχεία ενός συνόλου, γνωρίζουμε το σύνολο. Το ζήτημα είναι οτι μπορούμε να περιγράψουμε το ίδιο σύνολο με διαφορετικούς τρόπους. Για παράδειγμα, εάν A είναι το σύνολο των ριζών της εξίσωσης

$$x^2 - 6x + 8 = 0$$

και B το σύνολο των άρτιων αριθμών μεταξύ του 1 και του 5, τότε το A και το B έχουν ακριβώς δύο στοιχεία, τους αριθμούς 2 και 4. Συνεπώς το A και το B είναι το ίδιο σύνολο.

Δύο σύνολα είναι **ίσα** εάν έχουν τα ίδια στοιχεία. Συμβολίζουμε την ισότητα των συνόλων S και T με

$$S = T,$$

ενώ όταν δεν είναι ίσα γράφουμε

$$S \neq T.$$

Ο απλούστερος τρόπος να προσδιορίσουμε ένα σύνολο είναι να καταγράψουμε όλα τα στοιχεία του (εάν αυτό είναι δυνατό). Ο συνήθης συμβολισμός είναι να τα κλείνουμε σε αγκύλες $\{\ \}$. Οταν γράφουμε

$$S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$$

εννοούμε το σύνολο του οποίου τα στοιχεία είναι οι αριθμοί 1, 2, 3, 4, 5, 6, και μόνον αυτοί.

Πρέπει να τονίσουμε δύο σημεία σχετικά με αυτόν το συμβολισμό, συνέπειες και τα δύο της έννοιας της ισότητας για σύνολα. Πρώτον, η σειρά με την οποία γράφουμε τα στοιχεία είναι αδιάφορη:

$$\{5,\ 4,\ 3,\ 2,\ 6,\ 1\} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}.$$

Δεύτερον, επαναλήψεις των στοιχείων στην καταγραφή δεν αλλάζουν το σύνολο:

$$\{1,\ 2,\ 3,\ 4,\ 6,\ 1,\ 3,\ 5\} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}.$$

Για να προσδιορίσουμε κάποιο σύνολο, μπορεί να μην είναι πρακτικό, ή ούτε καν δυνατό, να καταγράψουμε όλα τα στοιχεία του. Το σύνολο των πρώτων αριθμών περιγράφεται πολύ καλύτερα από αυτήν τη φράση παρά με την απαρίθμηση μερικών πρώτων

$$\{2, 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ \ldots\}.$$

Θα μπορούσαμε να γράψουμε

$$P = \{\text{όλοι οι πρώτοι αριθμοί}\}.$$

Μία χρήσιμη παραλλαγή είναι

$$P = \{p \,|\, p \text{ είναι πρώτος αριθμός}\}.$$

Γενικότερα, ο συμβολισμός

$$Q = \{x \,|\, \text{‘κάτι σχετικό με το } x\text{’}\}$$

διαβάζεται “Q είναι το σύνολο όλων των x για τα οποία ισχύει το ‘κάτι σχετικό με το x’ ”. Για να προσδιορίσουμε, για παράδειγμα, το σύνολο των λύσεων της εξίσωσης $x^2-5x+6=0$ θα μπορούσαμε να λύσουμε την εξίσωση και να γράψουμε $S = \{2,\ 3\}$, ή θα μπορούσαμε να γράψουμε

$$S = \{x \,|\, x^2 - 5x + 6 = 0\}.$$

Ο δεύτερος τρόπος προσδιορίζει το σύνολο χωρίς να μας δίδει ρητά τα στοιχεία του, αλλά και χωρίς να χρειάζεται να λύσουμε την εξίσωση.

Με αυτό το συμβολισμό υπάρχει κάποια ασάφεια. Εάν αναφερόμαστε στους φυσικούς αριθμούς, το σύνολο

$$\{x \,|\, 1 \leq x \leq 5\}$$

αποτελείται από τους αριθμούς 1, 2, 3, 4, 5, αλλά εάν αναφερόμαστε στους πραγματικούς αριθμούς, τότε περιλαμβάνει και όλους τους υπόλοιπους αριθμούς μεταξύ του 1 και του 5. Ο καλύτερος τρόπος να κάνουμε αυτήν τη διάκριση είναι να προσδιορίσουμε το σύνολο Y από το οποίο επιλέγουμε τα x που ικανοποιούν το 'κάτι σχετικό με το x'. Ο συμβολισμός

$$X = \{x \in Y \,|\, \text{'κάτι σχετικό με το } x\text{'}\}$$

σημαίνει οτι X είναι το σύνολο των στοιχείων x του συνόλου Y για τα οποία ισχύει το 'κάτι σχετικό με το x'.

Ένας πιο σοβαρός λόγος για να διευκρινίζουμε το σύνολο Y από το οποίο επιλέγουμε τα στοιχεία του X είναι για να εξασφαλίσουμε οτι το 'κάτι σχετικό με το x' έχει νόημα για όλα τα $x \in Y$, είναι δηλαδή μια ιδιότητα που είναι σαφές εάν ισχύει ή δεν ισχύει για κάθε στοιχείο του Y, και τότε X είναι το σύνολο των στοιχείων του Y για τα οποία ισχύει αυτή η ιδιότητα.

Άσκηση 1.1 Ποιές από τις παρακάτω προτάσεις είναι αληθείς και ποιές ψευδείς; Εξηγήστε σύντομα την απάντησή σας.

α′. $1 \in \{1, 2\}$
β′. $3 \in \{1, 5, 2, 3\}$
γ′. $3 \in \{1, 5, 2\}$
δ′. $\{1, 3\} \in \{1, 3, 5, 2\}$
ε′. $\{5\} \in \{1, 3, 5, 2\}$
ϛ′. $2 \in \{x \in \mathbb{R} \,|\, x^2 - 3x + 2 = 0\}$
ζ′. $\{1, 4, 2, 3\} = \{2, 3, 1, 4, 3, 2\}$
η′. $\{a, d, b, d\} = \{a, b, d\}$
ϑ′. $\{a, b, d, d\} = \{a, b, a, d\}$
ι′. $\{x \in \mathbb{Q} \,|\, x^2 - 2x = 0\} = \{x \in \mathbb{R} \,|\, x^2 - 2x = 0\}$

Υποσύνολα

Ενα σύνολο B είναι **υποσύνολο** του A εάν κάθε στοιχείο του B είναι και στοιχείο του A. Λέμε επίσης οτι το B **περιέχεται** στο A και γράφουμε

$$B \subseteq A.$$

Πρόταση 1.1 *Εάν A και B είναι σύνολα, τότε $A = B$ εάν και μόνον εάν $A \subseteq B$ και $B \subseteq A$.*

Απόδειξη. Εάν $A = B$ τότε, εφόσον $A \subseteq A$, έπεται οτι $A \subseteq B$ και $B \subseteq A$. Αντιστρόφως, υποθέτουμε οτι $A \subseteq B$ και $B \subseteq A$. Τότε κάθε στοιχείο του A είναι στοιχείο το B και κάθε στοιχείο του B είναι στοιχείο του A. Άρα τα A και B έχουν τα ίδια στοιχεία, και συνεπώς $A = B$.

□

Πρόταση 1.2 *Εάν A, B, C είναι σύνολα, και $A \subseteq B$ και $B \subseteq C$, τότε $A \subseteq C$.*

Απόδειξη. Κάθε στοιχείο του A είναι στοιχείο του B και κάθε στοιχείο του B είναι στοιχείο του C. Άρα κάθε στοιχείο του A είναι στοιχείο του C, και συνεπώς $A \subseteq C$.

□

Είναι πολύ σημαντικό να διακρίνουμε υποσύνολα και στοιχεία. Τα στοιχεία του $\{1, 2\}$ είναι τα 1 και 2. Τα υποσύνολα του $\{1, 2\}$ είναι τα $\{1, 2\}$, $\{1\}$, $\{2\}$, και ακόμη ένα υποσύνολο, που προς το παρόν θα το συμβολίσουμε $\{\ \}$.

Η πρόταση 1.2 δεν ισχύει εάν αντικαταστήσουμε $\subseteq$ με $\in$. Τα στοιχεία ενός στοιχείου του συνόλου X δεν είναι απαραίτητα στοιχεία του X. Για παράδειγμα, εάν $A = 1$, $B = \{1, 2\}$ και $C = \{\{1, 2\}, \{3, 4\}\}$, τότε $A \in B$ και $B \in C$, αλλά τα στοιχεία του C είναι *τα σύνολα* $\{1, 2\}$ και $\{3, 4\}$, άρα $A = 1$ δεν είναι στοιχείο του C.

Το σύνολο που συμβολίσαμε $\{\ \}$ είναι ένα σύνολο στο οποίο δεν ανήκει κανένα στοιχείο. Ενα τέτοιο σύνολο το λέμε **κενό**. Για παράδειγμα, το σύνολο

$$\{x \in \mathbb{Z} \,|\, x = x + 1\}$$

είναι κενό, αφού η εξίσωση $x = x + 1$ δεν έχει λύσεις στο $\mathbb{Z}$. Ενα κενό σύνολο έχει κάποιες αξιοπρόσεκτες ιδιότητες. Εάν E είναι ένα κενό σύνολο και X είναι οποιοδήποτε σύνολο, τότε $E \subseteq X$. Γιατί; Πρέπει να δείξουμε οτι κάθε στοιχείο του E είναι στοιχείο του X. Για να μην ισχύει αυτό, θα πρέπει να υπάρχει κάποιο στοιχείο του E που να μην ανήκει στο X. Αφού το E είναι κενό, δεν υπάρχει κανένα τέτοιο στοιχείο.

Εάν E και F είναι δύο κενά σύνολα, από το προηγούμενο αποτέλεσμα έχουμε οτι $E \subseteq F$ και $F \subseteq E$. Αρα $E = F$. Ολα τα κενά σύνολα είναι ίσα. Αρα υπάρχει ένα μοναδικό κενό σύνολο. Δίνουμε σε αυτό το σύνολο ένα ειδικό σύμβολο:

$$\varnothing$$

συμβολίζει *το μοναδικό* κενό σύνολο.

Άσκηση 1.2 Ποιές από τις παρακάτω προτάσεις είναι αληθείς και ποιές ψευδείς; Εξηγήστε σύντομα την απάντησή σας.

α΄. $1 \subseteq \{1, 2\}$	β΄. $\{3, 1\} \subseteq \{1, 5, 2, 3\}$
γ΄. $\{3\} \subseteq \{1, 5, 2\}$	δ΄. $\{1, 3\} \in \{1, 3, 5, 2\}$
ε΄. $\{5\} \in \{1, 3, 5, 2\}$	ϛ΄. $2 \subseteq \{x \in \mathbb{R} \,|\, x^2 - 3x + 2 = 0\}$
ζ΄. $\{1, 4, 2, 3\} \subseteq \{2, 3, 1, 4, 3, 2\}$	η΄. $\{a, b, d, d\} \subseteq \{a, b, a, d\}$
ϑ΄. $\{b \in \mathbb{N} \,|\, b > 2\} = \{a \in \mathbb{N} \,|\, a > 2\}$	ι΄. $\{b \in \mathbb{N} \,|\, b > 2\} \subseteq \{a \in \mathbb{N} \,|\, a > 2\}$
ια΄. $\{2\} \subseteq \{1, \{2\}\}$	ιβ΄. $\{2\} \in \{1, \{2\}\}$
ιγ΄. $\{b \in \mathbb{N} \,|\, b \geq 2\} \subseteq \{a \in \mathbb{N} \,|\, a > 2\}$	ιδ΄. $\{x \in \mathbb{Q} \,|\, x^2 - 2 = 0\} = \varnothing$

Σύνολο των πάντων;

Οπως υπάρχει το κενό σύνολο, που δεν περιέχει κανένα στοιχείο, μπορούμε να αναρωτηθούμε εάν υπάρχει ένα σύνολο που περιέχει τα πάντα. Θα δούμε οτι αυτή η ιδέα είναι παρατραβηγμένη.

Ας θεωρήσουμε τη συλλογή Ω όλων των συνόλων. Εάν Ω είναι ένα σύνολο, τότε το ίδιο το Ω είναι στοιχείο του εαυτού του, $\Omega \in \Omega$. Τα συνηθισμένα σύνολα που έχουμε συναντήσει, όπως το σύνολο $\mathbb{N}$ των φυσικών αριθμών, δεν είναι στοιχεία του εαυτού τους. Μπορείτε να αφιερώσετε λίγη ώρα προσπαθώντας να φανταστείτε ένα σύνολο που είναι στοιχείο του εαυτού του.

Τώρα μπορούμε να θεωρήσουμε το υποσύνολο S του Ω που αποτελείται από τα σύνολα που δεν είναι στοιχεία του εαυτού τους,

$$S = \{A \in \Omega \,|\, A \notin A\}\,.$$

Αφού $S \subseteq \Omega$, το S είναι επίσης σύνολο, και μπορούμε να αναρωτηθούμε εάν το S είναι στοιχείο του εαυτού του. Τώρα όμως έχουμε το εξής παράδοξο.

- Εάν $S \in S$, τότε $S \in \Omega$ αλλά το S δεν ικανοποιεί την ιδιότητα που χαρακτηρίζει τα στοιχεία του S, και συνεπώς $S \notin S$.
- Εάν $S \notin S$, τότε $S \in \Omega$ και το S ικανοποιεί την ιδιότητα που χαρακτηρίζει τα στοιχεία του S, συνεπώς $S \in S$.

Οποιαδήποτε από τις δύο υποθέσεις για το S, οδηγεί σε αντίφαση.

Αυτό το παράδοξο, γνωστό με το όνομα παράδοξο του Russell, προέκυψε επειδή θεωρήσαμε οτι συλλογές όπως η S ή η Ω είναι σύνολα. Η αρχική μας περιγραφή ενός συνόλου ως μία *οποιαδήποτε* συλλογή δεν είναι επαρκής. Σε πιο προχωρημένα μαθήματα Θεωρίας Συνόλων, θα δούμε πώς ξεπερνιούνται τα παράδοξα, με κατάλληλο περιορισμό της έννοιας του συνόλου. Προς το παρόν, θα προσέχουμε τα σύνολα που εξετάζουμε να είναι σαφώς προσδιορισμένα, και να γνωρίζουμε ακριβώς ποιά στοιχεία ανήκουν στο σύνολο και ποιά όχι.

Η μη ύπαρξη ενός συνόλου των πάντων είναι ακόμη ένας λόγος για τον οποίο ο συμβολισμός

$$\{x \in Y \mid P(x)\},$$

όπου Y είναι ένα γνωστό σύνολο, και $P(x)$ είναι 'κάτι σχετικό με το x', είναι προτιμότερος από το συμβολισμό

$$\{x \mid P(x)\}.$$

Εχοντας προσδιορίσει το Y, μπορούμε να εξετάσουμε την ιδιότητα $P(x)$ και να βεβαιωθούμε οτι έχει νόημα για όλα τα στοιχεία του Y, πριν επιλέξουμε αυτά για τα οποία είναι αληθής.

Αλλοιώς είναι σαν να θεωρούμε το $\{x \in \Omega \mid P(x)\}$, το οποίο είδαμε οτι μπορεί να οδηγήσει σε παράδοξα. Παρατηρείστε οτι εάν θεωρήσουμε κάποιο συγκεκριμένο σύνολο που αποτελείται από σύνολα, η ιδιότητα $X \notin X$ δεν παρουσιάζει κανένα πρόβλημα. Για παράδειγμα, εάν $T = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, τότε

$$\{X \in T \mid X \notin X\} = \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\},$$

και προφανώς $T \notin T$.

Ενωση και τομή

Δύο σημαντικές μέθοδοι για να δημιουργήσουμε νέα σύνολα είναι η ένωση και η τομή. Η **ένωση** δύο συνόλων A και B είναι το σύνολο του οποίου τα στοιχεία είναι τα στοιχεία του A και τα στοιχεία του B και μόνον αυτά. Εάν

$$A = \{1, 2, 3\} \qquad B = \{3, 4, 5\}$$

τότε η ένωση είναι $\{1, 2, 3, 4, 5\}$. Συμβολίζουμε την ένωση των συνόλων A και B με $A \cup B$,

$$A \cup B = \{x \mid x \in A \text{ ή } x \in B \text{ (ή και τα δύο)}\}.$$

Η **τομή** δύο συνόλων A και B είναι το σύνολο του οποίου τα στοιχεία είναι όλα τα κοινά στοιχεία των A και B. Για τα σύνολα A και B του προηγούμενου παραδείγματος η τομή είναι το σύνολο $\{3\}$, γιατί μόνον το 3 ανήκει και στα δύο σύνολα. Συμβολίζουμε την τομή των συνόλων A και B με $A \cap B$,

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

Άσκηση 1.3 Προσδιορίστε τα παρακάτω σύνολα.

α′. $\{1,2,4\} \cup \{2,3,6\}$

β′. $\{1,2,4\} \cap \{2,3,6\}$

γ′. $A \cup B$, όπου $A = \{x \in \mathbb{Z} \,|\, x \geq 3\}$ και $B = \{y \in \mathbb{Z} \,|\, y \leq -3\}$.

δ′. $C \cap D$, όπου $C = \{x \in \mathbb{Z} \,|\, x \geq -3\}$ και $D = \{y \in \mathbb{Z} \,|\, y \leq 3\}$.

Πρόταση 1.3 *Εάν A, B, C είναι σύνολα, τότε*

1. $A \cup \varnothing = A$
2. $A \cup A = A$
3. $A \cup B = B \cup A$
4. $(A \cup B) \cup C = A \cup (B \cup C)$.

Απόδειξη. Μόνον το (4) παρουσιάζει κάποια δυσκολία. Υποθέτουμε οτι $x \in (A \cup B) \cup C$. Τότε $x \in A \cup B$ είτε $x \in C$. Εάν $x \in C$, τότε $x \in B \cup C$, άρα $x \in A \cup (B \cup C)$. Εάν $x \notin C$, τότε $x \in A$ είτε $x \in B$. Σε κάθε περίπτωση έχουμε $x \in A \cup (B \cup C)$. Εχουμε δείξει οτι εάν $x \in (A \cup B) \cup C$ τότε $x \in A \cup (B \cup C)$, δηλαδή

$$(A \cup B) \cup C \subseteq A \cup (B \cup C).$$

Με ένα παρόμοιο επιχείρημα δείχνουμε οτι

$$A \cup (B \cup C) \subseteq (A \cup B) \cup C.$$

Χρησιμοποιούμε την πρόταση 1.1 για να δείξουμε το ζητούμενο.

□

Παρόμοια αποτελέσματα ισχύουν για τις τομές.

Πρόταση 1.4 *Εάν A, B, C είναι σύνολα, τότε*

1. $A \cap \varnothing = \varnothing$
2. $A \cap A = A$
3. $A \cap B = B \cap A$
4. $(A \cap B) \cap C = A \cap (B \cap C)$.

□

Οι αποδείξεις είναι ανάλογες με αυτές της Πρότασης 1.3.

Άσκηση 1.4 Συμπληρώστε τις αποδείξεις των Προτάσεων 1.3 και 1.4.

Τέλος υπάρχουν δύο ταυτότητες που συνδέουν ενώσεις και τομές.

Πρόταση 1.5 *Εάν A, B, C είναι σύνολα, τότε*

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

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

Απόδειξη. Εάν $x \in A \cup (B \cap C)$, τότε $x \in A$ είτε $x \in B \cap C$. Εάν $x \in A$ τότε $x \in A \cup B$ και $x \in A \cup C$, άρα $x \in (A \cup B) \cap (A \cup C)$. Διαφορετικά, $x \in B \cap C$, κάτι που συνεπάγεται $x \in B$ και $x \in C$. Αρα $x \in A \cup B$ και $x \in A \cup C$, συνεπώς $x \in (A \cup B) \cap (A \cup C)$. Αυτό δείχνει οτι

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

Αντίστροφα, υποθέτουμε οτι $y \in (A \cup B) \cap (A \cup C)$. Τότε $y \in A \cup B$ και $y \in A \cup C$. Θα εξετάσουμε δύο περιπτώσεις: όταν $y \in A$ και όταν $y \notin A$. Στην πρώτη περίπτωση, $y \in A \cup (B \cap C)$. Στη δεύτερη περίπτωση, εφόσον $y \in A \cup B$, πρέπει να ισχύει $y \in B$, και παρόμοια $y \in C$. Έπεται οτι $y \in B \cap C$, και συνεπώς, και σε αυτήν την περίπτωση $y \in A \cup (B \cap C)$. Αρα

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

Τα δύο αποτελέσματα δίδουν τη ζητούμενη ταυτότητα. Η απόδειξη του 2 είναι ανάλογη.

□

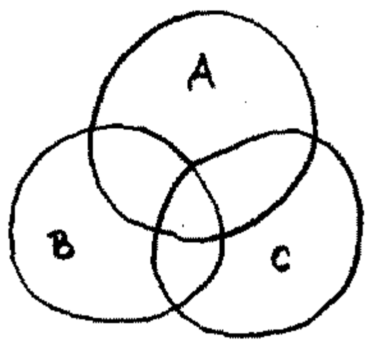
Άσκηση 1.5 Συμπληρώστε την απόδείξη της Πρότασης 1.5.

Η Πρόταση 1.5 δίδει δύο **επιμεριστικούς** κανόνες, ανάλογους με τον επιμεριστικό κανόνα για τον πολλαπλασιασμό ως προς την πρόσθεση:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)\,.$$

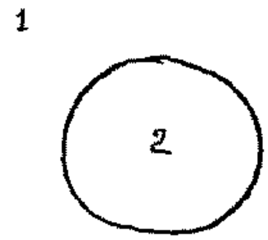
Προσέξτε οτι στην περίπτωση των αριθμητικών πράξεων δεν ισχύει η επιμεριστική ιδιότητα εάν αντιστρέψουμε τις πράξεις: η πρόσθεση δεν είναι επιμεριστική ως προς τον πολλαπλασιασμό.

Τα λεγόμενα **διαγράμματα Venn** προσφέρουν ένα τρόπο να παραστήσουμε αυτές τις συνολοθεωρητικές ταυτότητες.



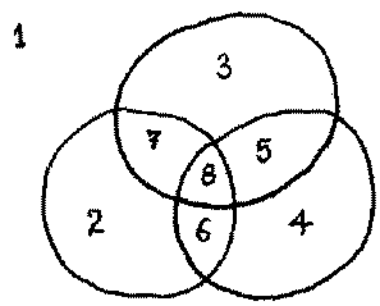
Σχήμα 1.1: Διάγραμμα Venn

Τέτοια σχέδια συχνά βοηθούν στην κατανόηση των σχέσεων μεταξύ των διαφόρων συνόλων, αλλά πρέπει να σχεδιαστούν προσεκτικά για να παριστάνουν τη γενικότερη κάθε φορά περίπτωση. Εάν έχουμε ένα σύνολο, στο διάγραμμα Venn εμφανίζονται δύο περιοχές: τα σημεία που ανήκουν στο σύνολο και αυτά που δεν ανήκουν σε αυτό (Σχήμα 1.2).



Σχήμα 1.2: Διάγραμμα Venn ενός συνόλου

Με δύο σύνολα έχουμε τέσσερεις περιοχές, ενώ με τρία σύνολα οκτώ περιοχές. Είναι εύκολο να σχεδιάσουμε τρεις κύκλους ώστε να διακρίνονται οι οκτώ περιοχές που παριστάνουν τη γενική περίπτωση για τρία σύνολα (Σχήμα 1.3).



Σχήμα 1.3: Διάγραμμα Venn τριών συνόλων

Για τέσσερα σύνολα, το ανάλογο σχήμα δεν μπορεί να γίνει με κύκλους. Μπορείτε να το καταφέρετε με τρεις κύκλους και ένα ελεύθερο σχήμα;

Τα διαγράμματα αποτελούν σημαντικό βοήθημα στην κατανόηση της κατάστασης. Όμως σε αυτό το στάδιο των σπουδών σας, όταν σας ζητείται να αποδείξετε μία σχέση μεταξύ συνόλων, μπορείτε να χρησιμοποιήσετε επικουρικά το διάγραμμα, αλλά είναι απαραίτητο να γράψετε την απόδειξη χρησιμοποιώντας με προσοχή το σωστό μαθηματικό συμβολισμό και ακριβείς μαθηματικές διατυπώσεις.

Άσκηση 1.6 Σχεδιάστε τα διαγράμματα Venn στις ακόλουθες περιπτώσεις:

α'. Έχουμε δύο σύνολα A και B τέτοια ώστε $(A \cup B) \subseteq B$ και $B \not\subseteq A$.

β'. Έχουμε τρία σύνολα A, B και C τέτοια ώστε $A \cap B \cap C = \varnothing$, $A \cap B \neq \varnothing$, $A \cap C \neq \varnothing$ και $B \cap C \neq \varnothing$.

Πρόταση 1.6 *Εάν A και B είναι σύνολα, οι επόμενες ιδιότητες είναι ισοδύναμες*

1. $A \subseteq B$
2. $A \cap B = A$
3. $A \cup B = B$.

Η πρόταση σημαίνει οτι κάθε μια από τις τρείς ιδιότητες ισχύει εάν και μόνον εάν ισχύουν και οι άλλες δύο. Συμβολικά

$$(A \subseteq B) \Leftrightarrow (A \cap B = A) \Leftrightarrow (A \cup B = B)$$

Απόδειξη. Υποθέτουμε οτι $A \subseteq B$ και θέλουμε να δείξουμε οτι $A \cap B = A$. Γνωρίζουμε οτι $A \cap B \subseteq A$. Εάν $x \in A$, τότε, αφού $A \subseteq B$, $x \in B$, άρα $x \in A \cap B$, και $A \subseteq A \cap B$. Άρα $A \cap B = A$.

Αντίστροφα, υποθέτουμε οτι $A \cap B = A$ και θέλουμε να δείξουμε οτι $A \subseteq B$. Εάν $x \in A$, τότε $x \in A \cap B$, άρα $x \in B$ και $A \subseteq B$.

Δείξαμε οτι τα 1 και 2 είναι ισοδύναμα.

Για την ισοδυναμία των 1 και 3, παρατηρούμε οτι το 3 λέει οτι εάν βάλουμε τα στοιχεία του A μαζί με τα στοιχεία του B, παίρνουμε το σύνολο B. Συμπληρώστε πιο αναλυτικά την απόδειξη, όπως στο προηγούμενο.

□

Συμπληρώματα

Εάν A και B είναι σύνολα, η συνολοθεωρητική **διαφορά** $A \setminus B$ ορίζεται ως το σύνολο όλων των στοιχείων του A που δεν ανήκουν στο B,

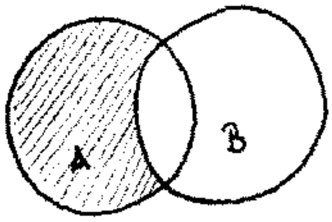
$$A \setminus B = \{x \in A \,|\, x \notin B\}.$$

Άσκηση 1.7 Εάν $A = \{1, 2, 3\}$ και $B = \{1, 5, 6, 7\}$, βρείτε τα σύνολα $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$ και $(A \cup B) \setminus (A \cap B)$.

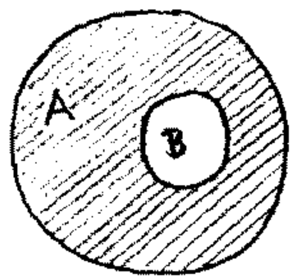
Εάν B είναι υποσύνολο του A ονομάζουμε το $A \setminus B$ **συμπλήρωμα του B ως προς το A**.

Δεν μπορούμε να ξεχάσουμε το A και να ορίσουμε το συμπλήρωμα του B ως το σύνολο όλων όσα δεν ανήκουν στο B, γιατί τότε η ένωση του B και του υποτιθέμενου συμπληρώματος θα ήταν το σύνολο Ω των πάντων, που όπως είδαμε δεν μπορεί να υπάρχει.

Σε συγκεκριμένες περιπτώσεις μπορεί να υπάρχει ένα σύνολο που περιέχει όλα τα αντικείμενα που εξετάζουμε. Τότε ονομάζουμε αυτό το σύνολο **χώρο**. Οταν αναφερόμαστε σε ακεραίους αριθμούς, ο χώρος μπορεί να είναι το σύνολο $\mathbb{Z}$ των ακεραίων. Οταν έχουμε στο



Σχήμα 1.4: Η συνολοθεωρητική διαφορά $A \setminus B$.



Σχήμα 1.5: Το συμπλήρωμα του B ως προς το A.

νου μας κάποιο συγκεκριμένο χώρο U, ορίζουμε το **συμπλήρωμα** B^c κάθε υποσυνόλου B του U να είναι

$$B^c = U \setminus B,$$

δηλαδή να είναι το συμπλήρωμα του B ως προς το χώρο U. Ορισμένες ιδιότητες του συμπληρώματος δίδουμε στην επόμενη Πρόταση.

Πρόταση 1.7 *Εάν A και B είναι υποσύνολα του χώρου U, ισχύουν τα ακόλουθα:*

1. $\varnothing^c = U$
2. $U^c = \varnothing$
3. $(A^c)^c = A$
4. *Εάν* $A \subseteq B$ *τότε* $B^c \subseteq A^c$.

Ιδιαίτερο ενδιαφέρον έχουν οι **κανόνες De Morgan** για τη σχέση του συμπληρώματος με ενώσεις και τομές:

Πρόταση 1.8 *Εάν A και B είναι υποσύνολα του χώρου U, ισχύουν τα ακόλουθα:*

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$.

Απόδειξη. Εάν $x \in (A \cup B)^c$, τότε $x \notin A \cup B$. Αυτό σημαίνει οτι $x \notin A$ και $x \notin B$, άρα $x \in A^c$ και $x \in B^c$, και συνεπώς $x \in A^c \cap B^c$. Επομένως

$$(A \cup B)^c \subseteq A^c \cap B^c .$$

Για να αποδείξουμε τον αντίθετο εγκλεισμό, αντιστρέφουμε τα βήματα της προηγούμενης απόδειξης. Ετσι αποδεικνύεται η 1.

Για να αποδείξουμε την 2 μπορούμε να ακολουθήσουμε ανάλογα βήματα. Ενας άλλος τρόπος είναι να αντικαταστήσουμε το A με τό A^c και το B με το B^c στην 1, που δίδει

$$(A^c \cup B^c)^c = A^{cc} \cap B^{cc} = A \cap B.$$

Κατόπιν παίρνουμε συμπληρώματα, και έχουμε

$$(A \cap B)^c = (A^c \cup B^c)^{cc} = A^c \cup B^c$$

που είναι η 2.

□

Άσκηση 1.8 Απλοποιήστε τις ακόλουθες εκφράσεις

α'. $(D^c \cup F)^c \cup (D \cap F)$

β'. $((X^c \cup Y) \cap (X^c \cup Y^c))^c$

Άσκηση 1.9 Δείξτε οτι για οποιαδήποτε υποσύνολα A και B του χώρου U, ισχύει η ισότητα $A \setminus B = A \cap B^c$, και χρησιμοποιήστε την για να δείξετε οτι

α'. $(A \setminus B) \setminus C = A \setminus (B \cup C)$

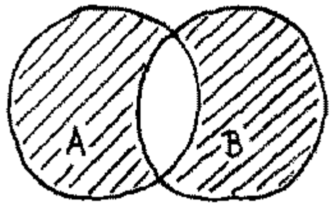
β'. $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.

Ορίζουμε τη **συμμετρική διαφορά** $A \triangle B$ δύο συνόλων A και B να είναι το σύνολο που περιέχει τα στοιχεία που ανήκουν ή στο A ή στο B, αλλά όχι και στα δύο:

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

Άσκηση 1.10 Δείξτε οτι

$$A \triangle B = (A \cup B) \setminus (A \cap B) .$$



Σχήμα 1.6: Η συμμετρική διαφορά.

Άσκηση 1.11 Υπολογίστε τα σύνολα $A \triangle A$ και $A \triangle \varnothing$. Δείξτε οτι $A \triangle B = B \triangle A$.

Μπορεί να προσέξατε οτι οι κανόνες της Θεωρίας Συνόλων παρουσιάζονται σε ζεύγη: για κάθε κανόνα, εάν αλλάξουμε όλες τις ενώσεις σε τομές και τις τομές σε ενώσεις, παίρνουμε έναν άλλο κανόνα. Θα ονομάσουμε αυτήν την παρατήρηση **Αρχή Δυϊκότητας του De Morgan**.

Εάν σε μια αληθή συνολοθεωρητική ταυτότητα στην οποία εμφανίζονται μόνον οι πράξεις $\cup$ και $\cap$, αντικαταστήσουμε κάθε $\cup$ με $\cap$ και κάθε $\cap$ με $\cup$, προκύπτει μια νέα αληθής ταυτότητα.

Η γενική απόδειξη αυτού του αποτελέσματος βασίζεται σε μια κάπως περίπλοκη επαγωγή, που κρύβει την απλότητα του βασικού επιχειρήματος. Ας θεωρήσουμε μια χαρακτηριστική περίπτωση.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{1.1}$$

Πάρετε τα συμπληρώματα και εφαρμόστε δύο φορές τους κανόνες De Morgan για να καταλήξετε στην

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

Αυτή η ταυτότητα ισχύει για οποιαδήποτε σύνολα A, B, C, άρα ισχύει και για τα A^c, B^c, C^c, και δίδει την ταυτότητα που προκύπτει από την 1.1 με εφαρμογή της δυϊκότητας De Morgan.

Σύνολα από σύνολα

Μερικές φορές εξετάζουμε σύνολα τα στοιχεία των οποίων είναι επίσης σύνολα. Για παράδειγμα, $S = \{A, B\}$, όπου $A = \{1, 2\}$, $B = \{2, 3, 4\}$. Ενα γενικότερο παράδειγμα είναι το σύνολο όλων των υποσυνόλων ενός συνόλου X, που ονομάζεται **δυναμοσύνολο** του X και συμβολίζεται $\mathfrak{P}(X)$:

$$Y \in \mathfrak{P}(X) \text{ εάν και μόνον εάν } Y \subseteq X$$

Εάν $X = \{0, 1\}$, τότε $\mathfrak{P}(X) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$.

Σε τέτοιες περιπτώσεις όπου κάθε στοιχείο του S είναι ένα σύνολο, μπορούμε να προχωρήσουμε ένα βήμα παραπέρα και να θεωρήσουμε τα στοιχεία των στοιχείων του S. Ετσι μπορούμε να γενικεύσουμε τις έννοιες της ένωσης και της τομής:

$$\bigcup S = \{x|\, x \in A \text{ για κάποιο } A \in S\},$$

και εάν $S \neq \varnothing$, [1]

$$\bigcap S = \{x|\, x \in A \text{ για κάθε } A \in S\}.$$

$\bigcup S$ είναι η **ένωση** του S, και $\bigcap S$ είναι η **τομή του** S. Η ένωση του S αποτελείται από όλα τα στοιχεία όλων των στοιχείων του S, ενώ η τομή του S αποτελείται από τα κοινά στοιχεία όλων των στοιχείων του S. Για παράδειγμα

$$\bigcup\{\{1,2\},\, \{2,3,4\}\} = \{1,2,3,4\}$$

$$\bigcap\{\{1,2\},\, \{2,3,4\}\} = \{2\}.$$

Για κάθε σύνολο X ισχύει

$$\bigcup \mathfrak{P}(X) = X$$

$$\bigcap \mathfrak{P}(X) = \varnothing.$$

Αυτός ο συμβολισμός αποτελεί πράγματι γενίκευση της ένωσης και της τομής δύο συνόλων. Εάν $S = \{A_1,\, A_2, \ldots,\, A_n\}$, ένας εναλλακτικός συμβολισμός είναι

$$\bigcup S = \bigcup_{r=1}^{n} A_r$$

$$\bigcap S = \bigcap_{r=1}^{n} A_r\ .$$

Άσκηση 1.12 Βρείτε το δυναμοσύνολο του συνόλου X, όπου $X = \{\alpha,\, \gamma,\, \omega\}$, και το δυναμοσύνολο του συνόλου A, όπου $A = \{a,\, \{a,\, b\}\}$.

Άσκηση 1.13 Εάν S είναι το σύνολο όλων των υποσυνόλων του $\mathbb{Z}$ στα οποία ανήκει το 0, βρείτε τα

$$\bigcup S \quad \text{και} \quad \bigcap S\,.$$

[1] Εάν $S = \varnothing$, η τομή $\bigcap S$ δεν ορίζεται. Εάν το S είναι κενό, τότε *οτιδήποτε* ανήκει σε *κάθε* στοιχείο του S, και θα είχαμε το σύνολο των πάντων.

Ασκήσεις

Υπενθυμίζουμε το συμβολισμό

$\mathbb{N}$: οι φυσικοί αριθμοί	$\mathbb{Z}$: οι ακέραιοι αριθμοί
$\mathbb{Q}$: οι ρητοί αριθμοί	$\mathbb{R}$: οι πραγματικοί αριθμοί

Σε αυτές τις ασκήσεις θέλουμε να προσέξουμε τη διάκριση μεταξύ

$\in$: ανήκει, είναι στοιχείο του ...

$\subseteq$: περιέχεται, είναι υποσύνολο του ...

Άσκηση 1.14 Ποιές από τις παρακάτω προτάσεις είναι αληθείς και ποιές ψευδείς; Εξηγείστε σύντομα την απάντησή σας.

α′. $1 \subseteq \{1,3,5,2\}$

β′. $\{1,2\} \subseteq \{1,3,5,2\}$

γ′. $\{x \in \mathbb{R} \,|\, x^2 - 3x + 2 = 0\} \subseteq \{1,3,5\}$

δ′. $\{x \in \mathbb{R} \,|\, x^2 - 3x + 2 = 0\} \in \mathbb{N}$

ε′. $\sqrt{2} \in \{x \in \mathbb{Q} \,|\, x^2 - 2 = 0\}$

ϛ′. $-3 \in \{a \in \mathbb{N} \,|\, a > 2\}$

ζ′. $\{1\} \in \{1,2,3\}$

η′. $\{1\} \subseteq \{1,2,3\}$

ϑ′. $1 \subseteq \{1,2,3\}$

ι′. $\{1,2\} \subseteq \{1,\{2\}\}$

ια′. $\{\{2\}\} \in \{1,\{2\}\}$

ιβ′. $\{\{2\}\} \subseteq \{1,\{2\}\}$

ιγ′. $\varnothing \subseteq \varnothing$

ιδ′. $\varnothing \in \varnothing$

ιε′. $\varnothing \in \{\varnothing\}$

ιϛ′. $\varnothing \subseteq \{\varnothing\}$

Άσκηση 1.15 Προσδιορίστε τα παρακάτω σύνολα.

α′. $\{1,2,\{4\}\} \cup \{2,3,6\}$

β′. $\{1,\{2\},4\} \cap \{2,3,6\}$

γ′. $A \cup B$, όπου $A = \{x \in \mathbb{Z} \,|\, |x| \geq 3\}$ και $B = \{y \in \mathbb{Z} \,|\, y \leq -3\}$.

δ′. $C \cap D$, όπου $C = \{x \in \mathbb{Z} \,|\, |x| \geq 3\}$ και $D\{y \in \mathbb{Z} \,|\, y \leq 3\}$.

ε′. $A \cup \{A\}$, όπου $A = \{1,2,3\}$.

ϛ′. $\varnothing \cup \{\varnothing\}$

ζ′. $\varnothing \cap \{\varnothing\}$

Άσκηση 1.16 4. Ποιά από τα παρακάτω σύνολα είναι ίσα;

α′. $\{-1,1,2\}$

β′. $\{-1,2,1,2\}$

γ′. $\{n \in \mathbb{Z} \,|\, |n| \leq 2$ και $n \neq 0\}$

δ′. $\{-2,2\} \cup \{1,-1\}$

Άσκηση 1.17 Εάν $V = \{\alpha,\, f,\, X\}$ και $W = \{1,\, f,\, \varnothing,\, \{\alpha\}\}$, βρείτε τα $V \setminus W$ και $W \setminus V$.

Άσκηση 1.18 Εάν $A = \{a,\, b,\, \{a,\, c\},\, \varnothing\}$, βρείτε τα σύνολα

α′. $A \setminus \{a\}$

β′. $A \setminus \varnothing$

γ′. $A \setminus \{a,\, c\}$

δ′. $A \setminus \{\{a,\, c\}\}$

ε′. $A \vartriangle \{a,\, c\}$

ϛ′. $\{a\} \setminus A$

Άσκηση 1.19 Δείξτε οτι η συμμετρική διαφορά έχει την προσεταιριστική ιδιότητα:

$$(A \vartriangle B) \vartriangle C = A \vartriangle (B \vartriangle C)\,.$$

Άσκηση 1.20 Αποδείξτε οτι:

α′. $(A \vartriangle B) \vartriangle A = B$

β′. $(A \vartriangle B) \cap C = (A \cap C) \vartriangle (B \cap C)$

Άσκηση 1.21 Χρησιμοποιήστε το προηγούμενο αποτέλεσμα για να δείξετε οτι εάν A, B και C είναι (οποιαδήποτε) σύνολα και $A \vartriangle B = A \vartriangle C$ τότε $B = C$. Αποδείξτε οτι η εξίσωση $A \vartriangle X = B$ έχει μοναδική λύση.

Άσκηση 1.22 Εάν $X = X_1 \cup X_2$, δείξτε οτι

$$\bigcup X = \left(\bigcup X_1\right) \cup \left(\bigcup X_2\right)\,.$$

Άσκηση 1.23 Εάν $A = \{\varnothing,\, \{\varnothing\}\}$ και $B = \{a,\, \{a\},\, b\}$, προσδιορίστε για κάθε μια από τις παρακάτω προτάσεις εάν είναι αληθής ή ψευδής:

α′. $\varnothing \in \mathfrak{P}(A)$

β′. $\varnothing \subseteq \mathfrak{P}(A)$

γ′. $\{\varnothing\} \in \mathfrak{P}(A)$

δ′. $\{\{a\}\} \in \mathfrak{P}(B)$

ε′. $\{\{a\}\} \subseteq \mathfrak{P}(B)$

ϛ΄. $\{\{a\}, b\} \subseteq \mathfrak{P}(B)$

ζ΄. $\{\{a\}, \{\{a\}\}\} \subseteq \mathfrak{P}(B)$

Άσκηση 1.24 Δίδεται ένα σύνολο X, ένα υποσύνολο $A \subseteq X$ και $Z = X \cup \mathfrak{P}(X)$. Δείξτε οτι $A \subseteq Z$ και $A \in Z$.

Άσκηση 1.25 Εάν το σύνολο A έχει n στοιχεία, πόσα στοιχεία έχει το δυναμοσύνολο $\mathfrak{P}(A)$; (Μπορείτε να εξετάσετε μικρά n για να μαντέψετε την απάντηση, και στη συνέχεια να χρησιμοποιήσετε τη μέθοδο της επαγωγής για την απόδειξη.)

Άσκηση 1.26 Πρόβλημα για γερούς λύτες.
Δείξτε οτι δεν υπάρχει σύνολο X τέτοιο ώστε $\mathfrak{P}(X) \subseteq X$. (Εξετάστε τα υποσύνολα Y του X που έχουν την ιδιότητα $Y \notin Y$, για να οδηγηθείτε σε αντίφαση ανάλογη με το παράδοξο του Russell.)

Κεφάλαιο 2

Σχέσεις

Η έννοια της **σχέσης** είναι μια από τις βασικότερες στη θεωρία συνόλων, και χρησιμοποιείται σε όλους τους κλάδους των μαθηματικών, και σε πολλές άλλες περιπτώσεις. Παραδείγματα σχέσεων μεταξύ αριθμών είναι 'μεγαλύτερος από', 'μικρότερος από', 'είναι διαιρέτης του', 'είναι ίσος προς', 'δεν είναι ίσος προς', ... Παραδείγματα από τη θεωρία συνόλων είναι 'είναι υποσύνολο', 'ανήκει', ... Παραδείγματα από άλλες περιοχές είναι 'είναι αδελφός της', 'είναι μητέρα του', ... Ολες αυτές οι εκφράσεις αναφέρονται σε δύο πράγματα, και το πρώτο είτε έχει τη σχέση που αναφέρεται προς το δεύτερο, είτε δεν την έχει. Για παράδειγμα, η έκφραση $a > b$, όπου a και b είναι ακέραιοι αριθμοί, είτε είναι αληθής είτε δεν είναι ($2 > 1$ είναι αληθής, $1 > 2$ δεν είναι αληθής).

Πρέπει να διακρίνουμε το πρώτο από το δεύτερο από τα δύο πράγματα που σχετίζονται: $a > b$ είναι διαφορετικό από $b > a$. Ετσι το πρώτο πράγμα που θα κάνουμε είναι να περιγράψουμε **διατεταγμένα ζεύγη**. Σε πολλές περιπτώσεις τα αντικείμενα στα οποία αναφέρεται η σχέση ανήκουν σε διαφορετικά σύνολα.

Θα περιγράψουμε την έννοια της σχέσης χρησιμοποιώντας τις έννοιες της θεωρίας συνόλων, και κατόπιν θα εξετάσουμε πιο αναλυτικά δύο πολύ σημαντικά είδη σχέσεων: τις σχέσεις ισοδυναμίας και τις σχέσεις διάταξης.

Διατεταγμένα ζεύγη

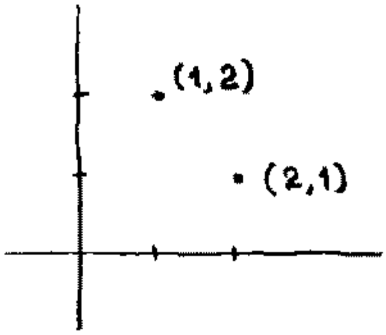
Σε ένα σύνολο, η διάταξη (η σειρά) με την οποία γράφουμε τα στοιχεία δεν κάνει διαφορά, έτσι ώστε $\{a, b\} = \{b, a\}$. Σε ορισμένες περιπτώσεις όμως αυτή η διάταξη έχει σημασία. Για παράδειγμα, στην αναλυτική γεωμετρία, οι συντεταγμένες ενός σημείου του επιπέδου παριστάνονται από ζεύγη πραγματικών αριθμών (x, y). Η διάταξη έχει σημασία, αφού το σημείο με συντεταγμένες $(1, 2)$ είναι διαφορετικό από το σημείο με συντεταγμένες $(2, 1)$, Σχήμα 2.1.

Συμβολίζουμε το διατεταγμένο ζεύγος (x, y), με παρενθέσεις αντί για αγκύλες, για να το διακρίνουμε από το σύνολο $\{x, y\}$. Η βασική ιδιότητα που απαιτούμε από το νέο αντικείμενο είναι

$$(x, y) = (u, v) \text{ εάν και μόνον εάν } x = u \text{ και } y = v\ .$$

Εάν A και B είναι σύνολα, το **καρτεσιανό γινόμενο** $A \times B$ είναι το σύνολο όλων των διατεταγμένων ζευγών με πρώτο στοιχείο από το A και δεύτερο στοιχείο από το B:

$$A \times B = \{(x, y) |\, x \in A, \text{ και } y \in B\}\ .$$



Σχήμα 2.1: Συντεταγμένες σημείων στο επίπεδο.

Στην προηγούμενη παράγραφο προσδιορίσαμε πότε θα λέμε οτι δύο διατεταγμένα ζεύγη είναι ίσα, αλλά δεν έχουμε δόσει ακόμα έναν ορισμό για ένα διατεταγμένο ζεύγος, χρησιμοποιώντας τις έννοιες της θεωρίας συνόλων. Για να οδηγηθούμε σε έναν ορισμό, ας σκεφθούμε πώς παίρνουμε ένα διατεταγμένο ζεύγος: διαλέγουμε πρώτα ένα στοιχείο x από το σύνολο A, και μετά ένα στοιχείο y από το σύνολο B. Εχοντας διαλέξει το στοιχείο x έχουμε το μονοσύνολο $\{x\}$. Κατόπιν διαλέγουμε το στοιχείο y και έχουμε το σύνολο με δύο στοιχεία $\{x, y\}$. Συνολοθεωρητικά, αυτή η διαδικασία περιγράφεται από τα σύνολα $\{x\}$ και $\{x, y\}$, δηλαδή από το σύνολο $\{\{x\}, \{x, y\}\}$. Ο Πολωνός μαθηματικός Kuratowski έδωσε τον ακόλουθο ορισμό.

Ορισμός. Το **διατεταγμένο ζεύγος** (x, y) δύο στοιχείων x και y ορίζεται να είναι το σύνολο

$$(x, y) = \{\{x\}, \{x, y\}\} .$$

Πρέπει να ελέγξουμε οτι αυτός ο ορισμός συμφωνεί με τον τρόπο που θέλουμε να προσδιορίσουμε την ισότητα δύο διατεταγμένων ζευγών.

Πρόταση 2.1 *Με τον ορισμό του Kuratowski ισχύει οτι*

$$(x, y) = (u, v) \text{ εάν και μόνον εάν } x = u \text{ και } y = v .$$

Απόδειξη. Είναι προφανές οτι εάν $x = u$ και $y = v$, τότε $(x, y) = (u, v)$.

Στην αντίθετη κατεύθυνση, υποθέτουμε οτι $(x, y) = (u, v)$. Εάν $x \neq y$, τότε $\{\{x\}, \{x, y\}\}$ έχει δύο διαφορετικά στοιχεία, το $\{x\}$ και το $\{x, y\}$, άρα και το $(u, v) = \{\{u\}, \{u, v\}\}$ πρέπει να έχει δύο διαφορετικά στοιχεία. Αυτό σημαίνει οτι $u \neq v$, γιατί εάν $u = v$ τότε $\{u, v\} = \{u\}$. Συμπεραίνουμε οτι $\{x\} = \{u\}$ ή $\{x\} = \{u, v\}$. Εάν $\{x\} = \{u, v\}$ θα είχαμε $u \in \{x\}$ και $v \in \{x\}$, άρα $u = x = v$, που αντιφάσκει προς το προηγούμενο συμπέρασμα. Συνεπώς έχουμε $\{x\} = \{u\}$ και $x = u$.

Με ανάλογο επιχείρημα έχουμε οτι $\{x, y\} = \{u, v\}$, και αφού $x = u$, $x \neq y$ και $y \in \{u, v\}$, συμπεραίνουμε οτι $y = v$.

Εάν $x = y$, τότε ο συνολοθεωρητικός ορισμός του ζεύγους γίνεται

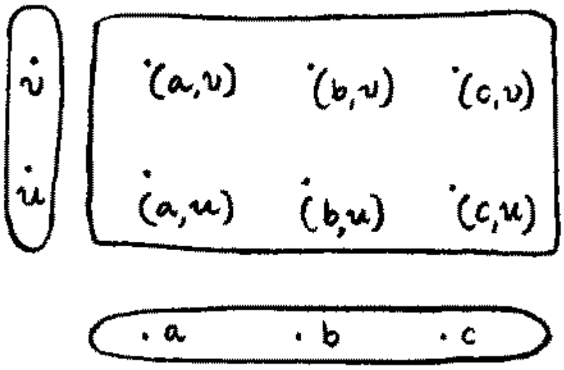
$$(x, y) = (x, x) = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\} ,$$

άρα το (x, y) έχει μόνον ένα στοιχείο, το $\{x\}$. Εάν $(x, y) = (u, v)$, τότε το (u, v) έχει επίσης μόνον ένα στοιχείο, άρα $\{u\} = \{u, v\}$, και συνεπώς $u = v$, $(u, v) = \{\{u\}\}$. Αρα η ισότητα $(x, y) = (u, v)$ γίνεται $\{\{x\}\} = \{\{u\}\}$ και εν συνεχεία $\{x\} = \{u\}$ και $x = u$. Σε αυτήν την περίπτωση έχουμε $x = y = u = v$, και η απόδειξη ολοκληρώθηκε.

□

Είδαμε οτι έχουμε ένα συνολοθεωρητικό ορισμό του διατεταγμένου ζεύγους, που κάνει ακριβές το τι εννοούμε με πρώτο και δεύτερο στοιχείο του ζεύγους. Στην πράξη, όταν σκεφτόμαστε ένα διατεταγμένο ζεύγος έχουμε τη διαισθητική εικόνα του 'πρώτου' και 'δεύτερου' στοιχείου, ή μια παραλλαγή της εικόνας των συντεταγμένων ενός σημείου στο επίπεδο. Είναι χρήσιμο όμως να γνωρίζουμε οτι εάν κάποτε τη χρειαστούμε, υπάρχει η αυστηρή έννοια, βασισμένη μόνο στις έννοιες της θεωρίας συνόλων.

Η εικόνα των συντεταγμένων στο επίπεδο μπορεί να χρησιμοποιηθεί για να παραστήσουμε άλλα σύνολα. Για παράδειγμα, εάν $A = \{a, b, c\}$ και $B = \{u, v\}$, παριστάνουμε το καρτεσιανό γινόμενο $A \times B$ με το Σχήμα 2.2



Σχήμα 2.2: Το καρτεσιανό γινόμενο $A \times B$.

Προσέξτε οτι $A \times B \neq B \times A$. Για παράδειγμα, εάν $A = \{a, b, c\}$ και $B = \{u, v\}$, τότε

$$A \times B = \{(a, u),\ (a, v),\ (b, u),\ (b, v),\ (c, u),\ (c, v)\}$$

ενώ

$$B \times A = \{(u, a),\ (u, b),\ (u, c),\ (v, a),\ (v, b),\ (v, c)\}\ .$$

Άσκηση 2.1 Δίδονται τα σύνολα $X = \{1,\ 2,\ 3\}$ και $Y = \{1,\ 4,\ \beta\}$. Βρείτε τα καρτεσιανά γινόμενα $X \times Y$ και $Y \times X$.

Πρόταση 2.2 *Για οποιαδήποτε σύνολα A, B, C ισχύουν οι ταυτότητες:*

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

4. $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Απόδειξη. Θα αποδείξουμε μόνο το (1), και θα αφήσουμε τα υπόλοιπα ως ασκήσεις.

Θεωρούμε $(u,v) \in (A \cup B) \times C$. Τότε $u \in A \cup B$ και $v \in C$. Αρα $u \in A$ ή $u \in B$. Εάν $u \in A$ τότε $(u,v) \in A \times C$. Εάν $u \in B$ τότε $(u,v) \in B \times C$. Σε κάθε περίπτωση $(u,v) \in (A \times C) \cup (B \times C)$. Αρα

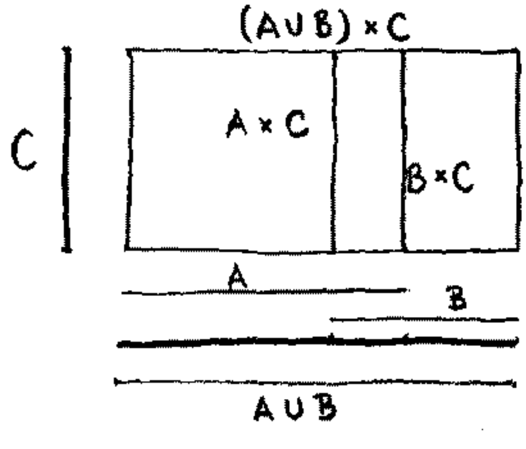
$$(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)\,.$$

Τώρα θεωρούμε $x = (y,z) \in (A \times C) \cup (B \times C)$. Είτε $x \in A \times C$ ή $x \in B \times C$. Στην πρώτη περίπτωση, $y \in A$ και $z \in C$. Στη δεύτερη περίπτωση $y \in B$ και $z \in C$. Αρα σε κάθε περίπτωση $y \in A \cup B$ και $z \in C$, συνεπώς $x = (y,z) \in (A \cup B) \times C$. Αρα

$$(A \times C) \cup (B \times C) \subseteq (A \cup B) \times C\,.$$

□

Το αποτέλεσμα μπορεί να παρασταθεί στο ακόλουθο διάγραμμα του Σχήματος 2.3.



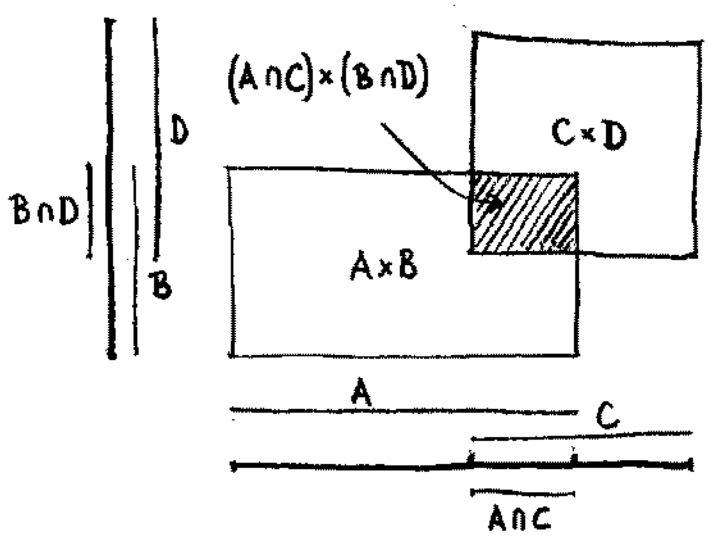
Σχήμα 2.3: Καρτεσιανό γινόμενο ένωσης δύο συνόλων.

Όπως και με τα διαγράμματα Venn, τέτοια διαγράμματα καρτεσιανών γινομένων αποτελούν βοηθήματα για την απόδειξη, αλλά σε αυτό το στάδιο των σπουδών σας απαιτείται να γράφετε την απόδειξη αναλυτικά, χρησιμοποιώντας το σωστό μαθηματικό συμβολισμό και ακριβείς μαθηματικές διατυπώσεις.

Άσκηση 2.2 Αποδείξτε τα 2, 3, και 4 της Πρότασης 2.2

Πρόταση 2.3 *Για οποιαδήποτε σύνολα A, B, C, D ισχύει*

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)\,.$$



Σχήμα 2.4: Καρτεσιανό γινόμενο τομών.

□

Άσκηση 2.3 Ακολουθώντας τη μέθοδο της προηγούμενης απόδειξης, και με τη βοήθεια του Σχήματος 2.4, συμπληρώστε την απόδειξη της Πρότασης 2.3.

Το αντίστοιχο αποτέλεσμα δεν ισχύει για ενώσεις στη θέση των τομών!

Άσκηση 2.4 Σχεδιάστε το αντίστοιχο σχήμα για το καρτεσιανό γινόμενο των ενώσεων συνόλων, και αποδείξτε οτι

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)\,.$$

Βρείτε ένα παράδειγμα για να δείξετε οτι δεν ισχύει πάντα ο αντίθετος εγκλεισμός.

Είναι εύκολο τώρα να ορίσουμε διατεταγμένες τριάδες, τετράδες κ.ο.κ.

$$(a, b, c) = ((a, b),\ c)$$

$$(a, b, c, d) = (((a, b),\ c),\ d)$$

Αυτά τα σύνολα είναι στοιχεία επαναλαμβανομένων καρτεσιανών γινομένων

$$A \times B \times C = (A \times B) \times C$$

$$A \times B \times C \times D = ((A \times B) \times C) \times D\ .$$

Στο Κεφάλαιο 3 θα δούμε έναν άλλο τρόπο να ορίσουμε τη γενική έννοια της διατεταγμένης n-άδας

$$(a_1,\ a_2,\ a_3,\ \ldots,\ a_n)$$

για κάθε φυσικό αριθμό n.

Σχέσεις

Διαισθητικά, μια σχέση μεταξύ δύο μαθηματικών αντικειμένων a και b είναι κάποια συνθήκη που αναφέρεται στα a και b και η οποία είτε είναι αληθής για συγκεκριμένες τιμές των a και b είτε είναι ψευδής. Για παράδειγμα, $a > b$ είναι μια σχέση μεταξύ φυσικών αριθμών:

$$2 > 1 \text{ είναι αληθής}$$

$$1 > 2 \text{ είναι ψευδής}$$

$$15 > 23 \text{ είναι ψευδής}$$

κ.ο.κ. Η σχέση είναι κάποια ιδιότητα των ζευγών των στοιχείων a και b. Προσέξτε οτι πρέπει να χρησιμοποιήσουμε διατεταγμένα ζεύγη (a, b), αφού, για παράδειγμα $2 > 1$ είναι αληθής ενώ $1 > 2$ είναι ψευδής.

Εάν γνωρίζουμε για ποιά διατεταγμένα ζεύγη (a, b) αληθεύει οτι $a > b$, τότε ουσιαστικά γνωρίζουμε τη σχέση 'μεγαλύτερο από'. Αυτή η παρατήρηση οδηγεί στον ορισμό της σχέσης μέσω ενός συνόλου διατεταγμένων ζευγών.

Ορισμός. Εάν A και B είναι σύνολα, μία **διμελής σχέση μεταξύ των στοιχείων των συνόλων $\boldsymbol{A}$ και $\boldsymbol{B}$** είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times B$.

Εάν $A = B$, λέμε οτι έχουμε μια **σχέση στο $\boldsymbol{A}$**, δηλαδή ένα υποσύνολο του $A \times A$.

Για παράδειγμα, η σχέση 'μεγαλύτερο από' στο σύνολο $\mathbb{N}$ των φυσικών αριθμών είναι το σύνολο όλων των διατεταγμένων ζευγών (a, b), όπου a, $b \in \mathbb{N}$ και $a > b$, με τη συνήθη σημασία.

Εάν $\boldsymbol{\rho}$ είναι μια σχέση μεταξύ των συνόλων A και B, λέμε οτι το $a \in A$ και το $b \in B$ σχετίζονται μέσω της $\boldsymbol{\rho}$ εάν $(a, b) \in \boldsymbol{\rho} \subseteq A \times B$. Χρησιμοποιούμε επίσης το συμβολισμό $a\,\boldsymbol{\rho}\,b$ εννοώντας οτι $(a, b) \in \boldsymbol{\rho}$. Αυτός ο συμβολισμός είναι πιο κοντά στο συνήθη συμβολισμό για πολλές από τις πιο κοινές σχέσεις: $a = b$, $a > b$, $a \geq b$, $a|b$ (a είναι διαιρέτης του b).

Μπορούμε να παραστήσουμε μια σχέση γραφικά, σαν υποσύνολο του καρτεσιανού γινομένου:

Η σχέση $\geq$ στο $\mathbb{N}$ παριστάνεται στο Σχήμα 2.5.

Η σχέση $=$ στο $\mathbb{N}$ είναι το υποσύνολο $\{(x, x) |\, x \in \mathbb{N}\}$, και παριστάνεται από 'τα σημεία στη διαγώνιο', όπως στο Σχήμα 2.6.

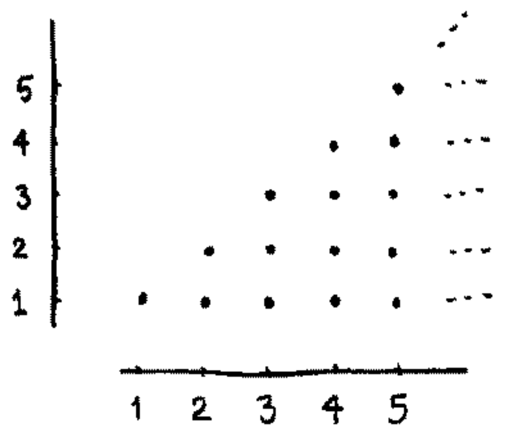
Εάν $X = \{1, 2, 3, 4, 5, 6\}$ και $|$ συμβολίζει τη σχέση 'είναι διαιρέτης του' στο X, ως σύνολο διατεταγμένων ζευγών έχουμε

$$\begin{aligned} | \; = \; & \{(1,1),\, (1,2),\, (1,3),\, (1,4),\, (1,5),\, (1,6),\, (2,2),\, (2,4),\, (2,6), \\ & (3,3),\, (3,6),\, (4,4),\, (5,5),\, (6,6)\}. \end{aligned}$$

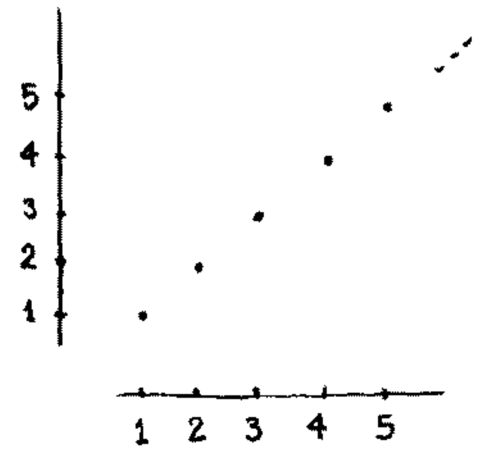
Δύο σχέσεις $\boldsymbol{\sigma}$ και $\boldsymbol{\rho}$ μεταξύ των στοιχείων δύο συνόλων A και B, είναι δύο υποσύνολα του καρτεσιανού γινομένου $A \times B$. Συνεπώς μπορούμε να εφαρμόσουμε συνολοθεωρητικές πράξεις σε αυτές, και να πάρουμε σύνολα όπως $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$, $\boldsymbol{\rho} \cap \boldsymbol{\sigma}$, $\boldsymbol{\rho} \setminus \boldsymbol{\sigma}$, $\boldsymbol{\sigma} \setminus \boldsymbol{\rho}$. Κάθε ένα από αυτά τα σύνολα ορίζει επίσης μία σχέση μεταξύ των στοιχείων των A και B.

Άσκηση 2.5 Δίδονται οι σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο σύνολο των φυσικών αριθμών, $\mathbb{N} = \{1,\, 2,\, 3,\, \ldots\}$, που ορίζονται από:

$$(a,\, b) \in \boldsymbol{\rho} \text{ εάν } a \mid b$$



Σχήμα 2.5: Η σχέση $\geq$ στο σύνολο των φυσικών αριθμών.



Σχήμα 2.6: Η σχέση ισότητας στο σύνολο των φυσικών αριθμών.

και

$$(a,\, b) \in \boldsymbol{\sigma} \text{ εάν } a^2 \mid b\,.$$

Περιγράψτε με ιδιότητες διαιρετότητας τις σχέσεις

$$\boldsymbol{\rho} \cup \boldsymbol{\sigma}, \qquad \boldsymbol{\rho} \cap \boldsymbol{\sigma}, \qquad \boldsymbol{\rho} \setminus \boldsymbol{\sigma}, \qquad \boldsymbol{\sigma} \setminus \boldsymbol{\rho}\,.$$

Εάν αντιστρέψουμε τη διάταξη των στοιχείων σε κάθε διατεταγμένο ζεύγος σε μια σχέση, παίρνουμε την **αντίστροφη σχέση**. Εάν $\boldsymbol{\rho}$ είναι μια σχέση μεταξύ των στοιχείων του A

και του B, η αντίστροφη σχέση $\boldsymbol{\rho}^{-1}$ είναι η σχέση μεταξύ των στοιχείων του B και του A, η οποία ορίζεται ως

$$\boldsymbol{\rho}^{-1} = \{(b,\, a) \in B \times A \,|\, (a,\, b) \in \boldsymbol{\rho}\}\,.$$

Εάν έχουμε μια σχέση $\boldsymbol{\rho}$ μεταξύ των στοιχείων των συνόλων A και B, και υποσύνολα $U \subseteq A$ και $V \subseteq B$, ορίζουμε τον **περιορισμό** $\boldsymbol{\sigma}$ της σχέσης $\boldsymbol{\rho}$ στο U και στο V

$$\boldsymbol{\sigma} = \{(a,b) \in \boldsymbol{\rho} | \, a \in U,\, b \in V\} = \boldsymbol{\rho} \cap (U \times V)\,.$$

Οσον αφορά στοιχεία του U και του V, η $\boldsymbol{\sigma}$ και η $\boldsymbol{\rho}$ λένε τα ίδια πράγματα. Η μόνη διαφορά είναι οτι η $\boldsymbol{\sigma}$ δεν λέει τίποτα για τα στοιχεία που δεν ανήκουν στο U και στο V.

Σχέσεις ισοδυναμίας

Στα μαθηματικά, τόσο στα στοιχειώδη όσο και στα προχωρημένα, η διάκριση μεταξύ άρτιων και περιττών ακεραίων είναι συχνά σημαντική. (Οι περιττοί ακέραιοι είναι αυτοί που γράφονται στη μορφή $2n + 1$ για n ακέραιο, δηλαδή οι $\ldots, -5, -3, -1, 1, 3, 5, \ldots$, ενώ οι άρτιοι είναι αυτοί που γράφονται στη μορφή $2n$ για n ακέραιο, δηλαδή οι $\ldots, -4, -2, 0, 2, 4, \ldots$. Το σύνολο $\mathbb{Z}$ όλων των ακεραίων χωρίζεται σε δύο, ξένα μεταξύ τους υποσύνολα

$$\mathbb{Z}_1 = \text{ το σύνολο των περιττών ακεραίων}$$

$$\mathbb{Z}_0 = \text{ το σύνολο των αρτίων ακεραίων}\,,$$

έτσι ώστε

$$\mathbb{Z}_1 \cap \mathbb{Z}_0 = \varnothing\ ,\ \mathbb{Z}_1 \cup \mathbb{Z}_0 = \mathbb{Z}\ .$$

Μπορούμε να χωρίσουμε το $\mathbb{Z}$ σε αυτά τα υποσύνολα χρησιμοποιώντας μια σχέση, που θα συμβολίσουμε προς το παρόν με $\sim$. Για $m,\, n \in \mathbb{Z}$ ορίζουμε

$$m \sim n \text{ εάν και μόνον εάν } m - n \text{ είναι πολλαπλάσιο του } 2.$$

Τότε

- *όλοι* οι περιττοί ακέραιοι σχετίζονται μέσω της $\sim$,
- *όλοι* οι άρτιοι ακέραιοι σχετίζονται μέσω της $\sim$,
- *κανένας* άρτιος ακέραιος δεν σχετίζεται με κάποιο περιττό ακέραιο,
- *κανένας* περιττός ακέραιος δεν σχετίζεται με κάποιο άρτιο ακέραιο.

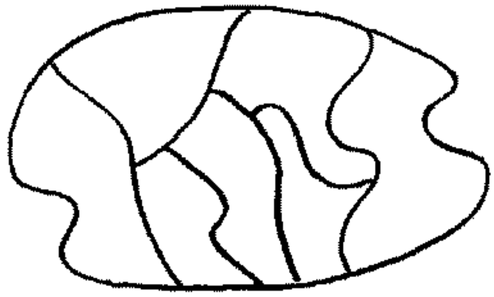
Αυτή η δυνατότητα οφείλεται σε κάποιες γενικές ιδιότητες της σχέσης $\sim$ τις οποίες θα εξετάσουμε.

Γενικότερα, υποθέστε οτι ένα σύνολο είναι χωρισμένο σε κάποια κομμάτια που είναι ξένα ανά δύο.

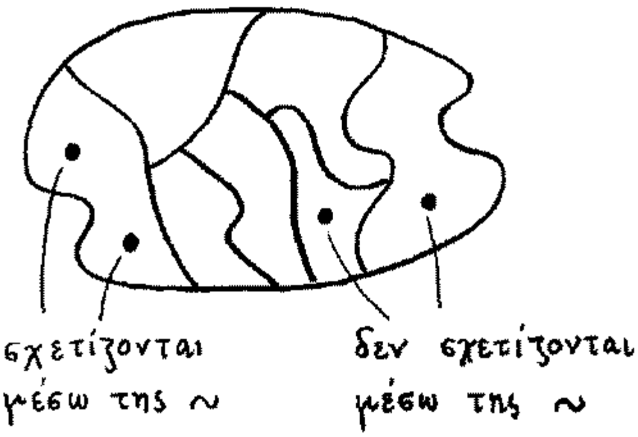
Μπορούμε να ορίσουμε μια σχέση $\sim$

$$x \sim y \quad \text{εάν και μόνον εάν} \quad x \text{ και } y \text{ βρίσκονται στο ίδιο κομμάτι}$$

όπως φαίνεται στο Σχήμα 2.8.



Σχήμα 2.7: Σύνολο χωρισμένο σε κομμάτια, ξένα ανά δύο.



Σχήμα 2.8: Η σχέση 'ανήκουν στο ίδιο κομμάτι'.

Αντίστροφα, μπορούμε να πάρουμε τα κομμάτια από τη σχέση $\sim$: το κομμάτι στο οποίο ανήκει το στοιχείο x είναι το

$$E_x = \{y \in X | \, x \sim y\} \; .$$

Εάν κατασκευάσουμε υποσύνολα με ανάλογο τρόπο από μια άλλη σχέση, τα πράγματα μπορεί να είναι διαφορετικά. Για παράδειγμα, μπορεί τα κομμάτια να μην είναι ξένα μεταξύ τους. Εάν χρησιμοποιήσουμε τη σχέση 'είναι διαιρέτης του', $|$, στο σύνολο $\{1, 2, 3, 4, 5, 6\}$, έχουμε

$$\begin{aligned} E_1 &= \{1, 2, 3, 4, 5, 6\} \\ E_2 &= \{2, 4, 6\} \\ E_3 &= \{3, 6\} \\ E_4 &= \{4\} \\ E_5 &= \{5\} \\ E_6 &= \{6\} \; . \end{aligned}$$

Εάν χρησιμοποιήσουμε τη σχέση $>$ στους φυσικούς αριθμούς, το x δεν ανήκει καν στο E_x, το οποίο προφανώς δεν είναι 'το κομμάτι στο οποίο ανήκει το x'.

Σε τί διαφέρει η σχέση $\sim$ από τις άλλες, ώστε σε εκείνη την περίπτωση να παίρνουμε το χώρισμα στα E_x; Παρατηρούμε τρεις εντελώς στοιχειώδεις ιδιότητες:

> το x ανήκει στο ίδιο κομμάτι με τον εαυτό του, δηλαδή το ζεύγος (x, x) ανήκει στη σχέση,
>
> εάν το x ανήκει στο ίδιο κομμάτι με το y, τότε το y ανήκει στο ίδιο κομμάτι με το x,
>
> εάν το x ανήκει στο ίδιο κομμάτι με το y, και το y ανήκει στο ίδιο κομμάτι με το z, τότε το x ανήκει στο ίδιο κομμάτι με το z.

Προφανώς, μια σχέση $\sim$ με την ιδιότητα οτι $x \sim y$ εάν και μόνον εάν το x και το y ανήκουν στο ίδιο κομμάτι, πρέπει να έχει τις τρεις ανάλογες ιδιότητες, τις οποίες διατυπώνουμε τυπικά στον ακόλουθο ορισμό.

Ορισμός. Μια σχέση $\sim$ στο σύνολο X ονομάζεται **σχέση ισοδυναμίας στο X** εάν έχει τις ακόλουθες ιδιότητες για όλα τα $x, y, z \in X$.

(ΣΙ1) $x \sim x$ (η σχέση $\sim$ είναι **ανακλαστική**).

(ΣΙ2) Εάν $x \sim y$, τότε $y \sim x$ (η σχέση $\sim$ είναι **συμμετρική**).

(ΣΙ3) Εάν $x \sim y$ και $y \sim z$, τότε $x \sim z$ (η σχέση $\sim$ είναι **μεταβατική**).

Θα δούμε οτι κάθε σχέση ισοδυναμίας σε ένα σύνολο X προκύπτει από το χώρισμα του συνόλου X σε κομμάτια. Πρώτα όμως θα ορίσουμε ακριβώς τι εννοούμε με χώρισμα σε ξένα μεταξύ τους κομμάτια.

Ορισμός. Μια **διαμέριση** του συνόλου X είναι ένα σύνολο $\mathcal{D}$ του οποίου τα στοιχεία είναι *μη κενά* υποσύνολα του X, έτσι ώστε

(Δ1) Κάθε $x \in X$ ανήκει σε κάποιο $A \in \mathcal{D}$,

(Δ2) Εάν $A, B \in \mathcal{D}$ και $A \neq B$, τότε $A \cap B = \varnothing$.

Τα 'κομμάτια' είναι τα στοιχεία του $\mathcal{D}$. Η ιδιότητα (Δ1) λέει οτι το X είναι η ένωση όλων των κομματιών. Η (Δ2) λέει οτι τα κομμάτια δεν τέμνονται μεταξύ τους.

Εάν $\sim$ είναι μια σχέση ισοδυναμίας, ορίζουμε την **κλάση ισοδυναμίας** (ως προς τη σχέση $\sim$) του στοιχείου $x \in X$ να είναι το σύνολο

$$E_x = \{y \in X | \, x \sim y\} \, .$$

Θεώρημα 2.4 *Εστω $\sim$ μια σχέση ισοδυναμίας σε ένα σύνολο X. Τότε $\mathcal{D} = \{E_x | \, x \in X\}$ είναι διαμέριση του X. Η σχέση 'ανήκει στο ίδιο στοιχείο της $\mathcal{D}$' είναι η ίδια με τη $\sim$.*

Αντίστροφα, εάν $\mathcal{D}$ είναι διαμέριση του X, θεωρούμε τη σχέση $\sim$ που ορίζεται ως $x \sim y$ εάν και μόνον εάν x και y βρίσκονται στο ίδιο στοιχείο της $\mathcal{D}$. Τότε $\sim$ είναι σχέση ισοδυναμίας, και η αντίστοιχη διαμέριση σε κλάσεις ισοδυναμίας είναι η $\mathcal{D}$.

Απόδειξη. Εφόσον $x \in E_x$ η ιδιότητα (Δ1) για τη διαμέριση ικανοποιείται. Θα ελέγξουμε τη (Δ2). Υποθέτουμε οτι $E_x \cap E_y \neq \varnothing$. Τότε υπάρχει $z \in E_x \cap E_y$, για το οποίο ισχύει $x \sim z$ και $y \sim z$. Από τη συμμετρική ιδιότητα, $z \sim y$ και από μεταβατικότητα $x \sim y$.

Θα δείξουμε οτι αυτό συνεπάγεται $E_x = E_y$. Εάν $u \in E_x$, τότε $x \sim u$ και $y \sim x$, άρα $y \sim u$. Συνεπώς $u \in E_y$ και $E_x \subseteq E_y$. Παρόμοια $E_y \subseteq E_x$. Αυτό δείχνει οτι $E_x = E_y$.

Εχουμε δείξει οτι ή $E_x \cap E_y = \varnothing$ ή $E_x = E_y$. Αυτό είναι λογικά ισοδύναμο με το (Δ2).

Τώρα ορίζουμε $x \approx y$ να σημαίνει 'x και y ανήκουν στην ίδια κλάση ισοδυναμίας'. Τότε

$$\begin{aligned} x \approx y \qquad & \text{εάν και μόνον εάν } x,\, y \in E_z \text{ για κάποιο } z \\ & \text{εάν και μόνον εάν } z \sim x \text{ και } z \sim y \text{ για κάποιο } z \\ & \text{εάν και μόνον εάν } x \sim y\ . \end{aligned}$$

Αρα $\approx$ και $\sim$ είναι η ίδια σχέση.

Το αντίστροφο αποτέλεσμα αποδεικνύεται με παρόμοιο τρόπο, αλλά είναι ευκολότερο. Το αφήνουμε για άσκηση.

□

Οι ιδιότητες οι οποίες χαρακτηρίζουν μία σχέση ισοδυναμίας είναι αρκετά σημαντικές ώστε να τις εξετάσουμε και μεμονομένα.

Ορισμός. Μια σχέση $\boldsymbol{\rho}$ στο σύνολο A λέγεται

1. **Ανακλαστική**, εάν για κάθε $x \in A$, $(x, x) \in \boldsymbol{\rho}$.

2. **Συμμετρική**, εάν για κάθε $x, y \in A$, εάν $(x, y) \in \boldsymbol{\rho}$ τότε $(y, x) \in \boldsymbol{\rho}$.

3. **Μεταβατική**, εάν για κάθε $x, y, z \in A$, εάν $(x, y) \in \boldsymbol{\rho}$ και $(y, z) \in \boldsymbol{\rho}$, τότε $(x, z) \in \boldsymbol{\rho}$.

Άσκηση 2.6 Θεωρούμε τις σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο X, δηλαδή $\boldsymbol{\rho}, \boldsymbol{\sigma} \subseteq X \times X$. Εάν οι $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ είναι ανακλαστικές, δείξτε οτι η $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$ και η $\boldsymbol{\rho} \cap \boldsymbol{\sigma}$ είναι επίσης ανακλαστικές. Είναι η σχέση $\boldsymbol{\rho} \setminus \boldsymbol{\sigma}$ ανακλαστική;

Άσκηση 2.7 Δίδουμε διάφορες σχέσεις στο $\mathbb{R}$. Ποιές από αυτές είναι ανακλαστικές, συμμετρικές, μεταβατικές;

α′. $x < y$

β′. $x \geq y$

γ′. $|x - y| < 1$

δ′. $|x - y| \leq 0$

ε′. $x - y$ είναι ρητός

ϛ′. $x - y$ είναι άρρητος

Παράδειγμα σχέσης ισοδυναμίας: Αριθμητική modulo 3.

Θα χρησιμοποιήσουμε την έννοια της σχέσης ισοδυναμίας για να γενικεύσουμε τη διάκριση μεταξύ άρτιων και περιττών ακεραίων, και να εισαγάγουμε τους **ακεραίους modulo $\boldsymbol{n}$**, για $n \geq 3$.

Πρώτα εξετάζουμε την περίπτωση $n = 3$. Ορίζουμε τη σχέση **ισοτιμίας modulo 3**, $\equiv_3$, στο $\mathbb{Z}$

$$m \equiv_3 n \quad \text{εάν και μόνον εάν} \quad m - n \text{ είναι πολλαπλάσιο του } 3\,.$$

Πρόταση 2.5 $\equiv_3$ *είναι σχέση ισοδυναμίας.*

Απόδειξη.

(ΣΙ1) $m - m = 0 = 3 \cdot 0$.

(ΣΙ2) Εάν $m - n = 3k$ τότε $n - m = 3(-k)$.

(ΣΙ3) Εάν $m - n = 3k$ και $n - p = 3l$, τότε $m - p = 3(k + l)$.

□

Γνωρίζουμε οτι οι κλάσεις ισοδυναμίας, που σε αυτήν την περίπτωση ονομάζονται **κλάσεις υπολοίπων mod3**, αποτελούν διαμέριση του συνόλου των ακεραίων. Ας δούμε μερικά παραδείγματα.

$$\begin{aligned}
E_0 &= \{y |\, 0 \equiv_3 y\} \\
&= \{y |\, y - 0 \text{ είναι πολλαπλάσιο του } 3\} \\
&= \{y |\, y = 3k \text{ για κάποιο } k \in \mathbb{Z}\}\,.
\end{aligned}$$

$$\begin{aligned}
E_1 &= \{y |\, 1 \equiv_3 y\} \\
&= \{y |\, y - 1 \text{ είναι πολλαπλάσιο του } 3\} \\
&= \{y |\, y = 3k + 1 \text{ για κάποιο } k \in \mathbb{Z}\}\,.
\end{aligned}$$

$$\begin{aligned}
E_2 &= \{y |\, 2 \equiv_3 y\} \\
&= \{y |\, y = 3k + 2 \text{ για κάποιο } k \in \mathbb{Z}\}\,.
\end{aligned}$$

$$E_3 = \{y |\, y = 3k + 3 \text{ για κάποιο } k \in \mathbb{Z}\}\,.$$

Ομως, $3k + 3 = 3(k + 1)$, άρα $E_3 = E_0$. Παρόμοια, $E_4 = E_1$, $E_5 = E_2$, $E_{-1} = E_2$, $E_{-2} = E_1$, κ.ο.κ. Κάθε ακέραιος είναι της μορφής $3k$, $3k + 1$ ή $3k + 2$, άρα έχουμε ακριβώς τρείς κλάσεις υπολοίπων:

$$\begin{aligned}
E_0 &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\
E_1 &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\
E_2 &= \{\ldots, -7, -4, -1, 2, 5, 8, 12, \ldots\}
\end{aligned}$$

Ας εξετάσουμε τώρα εάν μπορούμε να κάνουμε αριθμητικές πράξεις με αυτές τις κλάσεις ισοδυναμίας.

Για να αποσαφηνίσουμε το συμβολισμό, θα συμβολίσουμε την κλάση υπολοίπων του n με n_3 αντί για E_n. Έτσι οι τρεις κλάσεις συμβολίζονται 0_3, 1_3, 2_3, και θέτουμε $\mathbb{Z}_3 = \{0_3, 1_3, 2_3\}$. Ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού στο σύνολο $\mathbb{Z}_3$ ως εξής:

$$m_3 + n_3 = (m+n)_3 \tag{2.1}$$
$$m_3 n_3 = (mn)_3 \tag{2.2}$$

Για παράδειγμα, $1_3 + 2_3 = 3_3 = 0_3$, $2_3 2_3 = 4_3 = 1_3$.

Αφήνοντας προς το παρόν το ερώτημα της χρησιμότητας ενός τέτοιου ορισμού, ας εξετάσουμε εάν τα πράγματα είναι τόσο απλά όσο φαίνονται. Θα δούμε οτι μια πιο προσεκτική μελέτη μπορεί να μας κάνει να ανησυχήσουμε, αλλά λίγο περισσότερη προσοχή θα μας πείσει οτι δεν υπάρχει πρόβλημα, τουλάχιστον σε αυτήν την περίπτωση.

Ιδού κάτι που πρέπει να μας προβληματίσει: η ίδια κλάση έχει πολλά διαφορετικά ονόματα. $1_3 = 4_3 = 7_3 = \dots$, $2_3 = 5_3 = 8_3 = \dots$. Ο ορισμός μπορεί να δίδει διαφορετικά αποτελέσματα, ανάλογα με το πιο όνομα χρησιμοποιούμε! Είδαμε οτι $1_3 + 2_3 = 0_3$. Αλλά $1_3 = 7_3$ και $2_3 = 8_3$, άρα θέλουμε $1_3 + 2_3 = 7_3 + 8_3 = 15_3$. Πράγματι, $15_3 = 0_3$, άρα μέχρι τώρα πάμε καλά. Τι συμβαίνει στη γενική περίπτωση;

Εάν $i_3 = j_3$ τότε $i - j = 3k$ για κάποιο k, και εάν $m_3 = n_3$ τότε $m - n = 3l$ για κάποιο l. Από τον κανόνα (2.1) έχουμε δύο δυνατές απαντήσεις:

$$i_3 + m_3 = (i+m)_3, \qquad j_3 + n_3 = (j+n)_3.$$

Όμως

$$i + m = j + 3k + n + 3l = (j+n) + 3(k+l),$$

και συνεπώς

$$(i+m)_3 = (j+n)_3.$$

Άρα έχουμε το ίδιο αποτέλεσμα στις δύο περιπτώσεις, και ο κανόνας (2.1) ορίζει πραγματικά την πρόσθεση κλάσεων υπολοίπων.

Παρόμοια πρέπει να εξετάσουμε εάν έχουμε πραγματικά ορίσει τον πολλαπλασιασμό κλάσεων με τον κανόνα (2.2). Για τα i, j, m, n όπως παραπάνω, έχουμε

$$i_3 m_3 = (im)_3, \qquad j_3 n_3 = (jn)_3.$$

Αλλά

$$im = (j+3k)(n+3l) = jn + 3(jl + nk + 3kl),$$

άρα

$$(im)_3 = (jn)_3,$$

που σημαίνει οτι ο (2.2) ορίζει τον πολλαπλασιασμό.

Αυτό το πρόβλημα δημιουργεί αρκετή σύγχυση. Εμφανίζεται κάθε φορά που προσπαθούμε να ορίσουμε πράξεις ανάμεσα σε σύνολα με ένα κανόνα της μορφής 'διάλεξε στοιχεία από τα σύνολα, κάνε κάποια πράξη μεταξύ τους, και πάρε το σύνολο στο οποίο ανήκει το αποτέλεσμα'. Σε περιπτώσεις όπως η παραπάνω, που ο συμβολισμός κρύβει μια τέτοια διαδικασία, πρέπει να είμαστε πολύ προσεκτικοί, να εξετάσουμε τι σημαίνει ο συμβολισμός και να μην παρασυρθούμε σε τυφλό χειρισμό των συμβόλων. Πρέπει να ελέγξουμε οτι οι διαφορετικές επιλογές δίδουν το ίδιο αποτέλεσμα.

Ούτε είναι ασφαλές να πιστεύουμε οτι κάποιος εύλογος ορισμός θα δουλεύει σωστά. Για παράδειγμα, ας προσπαθήσουμε να ορίσουμε δυνάμεις στο $\mathbb{Z}_3$. Ενας φυσιολογικός τρόπος να το κάνουμε είναι να μιμηθούμε τις (2.1) και (2.2), και να ορίσουμε

$$m_3{}^{n_3} = (m^n)_3.$$

Για παράδειγμα, $2_3{}^{2_3} = (2^2)_3 = 4_3 = 1_3$. Θα μπορούσαμε ακόμα να αποδείξουμε οτι ικανοποιούνται οι κανόνες των δυνάμεων

$$m_3{}^{n_3+p_3} = (m^{n+p})_3 = (m^n m^p)_3 = (m^n)_3(m^p)_3 = m_3{}^{n_3} m_3{}^{p_3}. \qquad (*)$$

Αν όμως εφαρμόσουμε αυτόν τον 'ορισμό', εφόσον $2_3 = 5_3$, έχουμε

$$1_3 = 2_3{}^{2_3} = 2_3{}^{5_3} = (2^5)_3 = (32)_3 = 2_3.$$

Αλλά $1_3 \neq 2_3$, και πρέπει να παραδεχθούμε οτι ο ορισμός και ο κανόνας (*) που συμπεράναμε είναι μια ευλογοφανής, και γι'αυτό επικίνδυνη, ανοησία. Οι μαθηματικοί λένε οτι πρέπει να εξετάσουμε πως η πράξη είναι 'καλά ορισμένη'.

Ας επιστρέψουμε στην αριθμητική του $\mathbb{Z}_3$. Μπορούμε να κατασκευάσουμε πίνακες πρόσθεσης και πολλαπλασιασμού

$+$	0_3	1_3	2_3
0_3	0_3	1_3	2_3
1_3	1_3	2_3	0_3
2_3	2_3	0_3	1_3

$\times$	0_3	1_3	2_3
0_3	0_3	0_3	0_3
1_3	0_3	1_3	2_3
2_3	0_3	2_3	1_3

Μπορούμε να επαληθεύσουμε πολλούς κανόνες της αριθμητικής ανάλογους με αυτούς των ακεραίων, όπως:

$$x + y = y + x \qquad x(y + z) = xy + xz.$$

Εάν αντί για 3 χρησιμοποιήσουμε κάποιον άλλο ακέραιο $n \geq 4$, μπορούμε με ανάλογο τρόπο να κατασκευάσουμε τους ακεραίους modulo n. Ορίζουμε τη σχέση ισοτιμίας modulo n, $\equiv_n$:

$$x \equiv_n y \text{ εάν και μόνον εάν } x - y \text{ είναι πολλαπλάσιο του } n.$$

Έχουμε n διαφορετικές κλάσεις υπολοίπων mod$n$, 0_n, 1_n, 2_n, $\ldots$, $(n-1)_n$, ενώ $n_n = 0_n$, $(n+1)_n = 1_n$ κ.ο.κ. Η κλάση x_n αποτελείται από τους ακεραίους που αφήνουν υπόλοιπο x όταν διαιρεθούν με το n. Στο σύνολο $\mathbb{Z}_n$ των κλάσεων υπολοίπων mod n μπορούμε να ορίσουμε αριθμητικές πράξεις όπως στο $\mathbb{Z}_3$.

Άσκηση 2.8 Βρείτε όλα τα διατεταγμένα ζεύγη στοιχείων του $\mathbb{Z}_{12}$, (a, b) για τα οποία ισχύει: $a \cdot b = 0_{12}$.

Σχέσεις διάταξης

Οι σχέσεις διάταξης που συναντούμε όταν ασχολούμαστε με αριθμούς, όπως $4 < 5$, $7 > 2\pi$, $x^2 \geq 0$, $1 - x^2 \leq 1$ για κάθε πραγματικό αριθμό x, συνδέονται όλες μεταξύ τους:

$$x < y \text{ σημαίνει το ίδιο με } y > x,$$

$$x \le y \text{ σημαίνει το ίδιο με } y \ge x,$$

$$x \le y \text{ σημαίνει το ίδιο με } x < y \text{ ή } x = y,$$

$$x < y \text{ σημαίνει το ίδιο με } x \le y \text{ και } x \ne y\,.$$

Οταν χρησιμοποιούμε συγκεκριμένους αριθμούς, μπορεί να είναι προτιμότερο να χρησιμοποιήσουμε τις γνήσιες ανισότητες $<$ ή $>$. Δεν θα γράφαμε $2+2 \ge 4$, (παρ'ολο που είναι σωστό) αφού γνωρίζουμε κάτι πιο συγκεκριμένο, οτι $2+2=4$. Παρόμοια, θα γράφαμε $2+2>3$, γιατί αυτό δίδει πιο συγκεκριμένη πληροφορία από το $2+2 \ge 3$. Σε γενικότερες καταστάσεις είναι συχνά προτιμότερο το αντίθετο. Για παράδειγμα, όταν (a_n) και (b_n) είναι ακολουθίες που συγκλίνουν στα όρια a και b αντίστοιχα, εάν $a_n \ge b_n$ για κάθε n, τότε μπορούμε να συμπεράνουμε οτι $a \ge b$. Ομως η υπόθεση οτι ισχύει η γνήσια ανισότητα $a_n > b_n$ δεν συνεπάγεται οτι $a > b$. Θα ξεκινήσουμε με τη μελέτη των ασθενών σχέσεων διάταξης.

Ορισμός. Μια σχέση $\boldsymbol{\rho}$ στο σύνολο A ονομάζεται **ασθενής σχέση διάταξης** εάν έχει τις ακόλουθες ιδιότητες για όλα τα x, y, $z \in A$.

(ΑΔ1) Εάν $x\,\boldsymbol{\rho}\,y$ και $y\,\boldsymbol{\rho}\,z$ τότε $x\,\boldsymbol{\rho}\,z$,

(ΑΔ2) Για κάθε δύο στοιχεία x και y του A, ισχύει ένα από τα $x\,\boldsymbol{\rho}\,y$ ή $y\,\boldsymbol{\rho}\,x$, ή και τα δύο,

(ΑΔ3) Εάν $x \ne y$ και ισχύει $x\,\boldsymbol{\rho}\,y$, τότε δεν ισχύει $y\,\boldsymbol{\rho}\,x$ (η $\boldsymbol{\rho}$ είναι **αντισυμμετρική**).

Οι ιδιότητες (ΑΔ2) και (ΑΔ3) σημαίνουν οτι εάν $x \ne y$, ισχύει *ακριβώς ένα* από τα $x\,\boldsymbol{\rho}\,y$ ή $y\,\boldsymbol{\rho}\,x$. Συνεπώς εάν ισχύουν και τα δύο $x\,\boldsymbol{\rho}\,y$ και $y\,\boldsymbol{\rho}\,x$, τότε $x = y$.

Αυτές οι ιδιότητες προφανώς ισχύουν για τις σχέσεις $\ge$ και $\le$. Αυτό δεν πρέπει να μας εκπλήττει. Γνωρίζουμε οτι για κάθε σχέση $\boldsymbol{\rho}$ μπορούμε να ορίσουμε την αντίστροφη σχέση $\boldsymbol{\sigma} = \boldsymbol{\rho}^{-1}$ μέσω της

$$x\,\boldsymbol{\sigma}\,y \quad \text{εάν και μόνον εάν} \quad y\,\boldsymbol{\rho}\,x\,.$$

Άσκηση 2.9 Εάν $\boldsymbol{\rho}$ είναι σχέση ασθενούς διάταξης, τότε η αντίστροφη σχέση είναι επίσης ασθενής διάταξη.

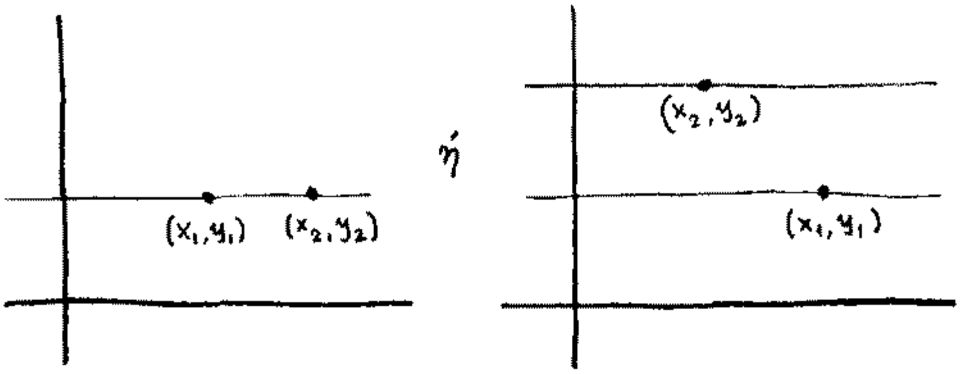
Παράδειγμα 2.1 Εάν $A = \{a, b, c\}$, όπου τα a, b, c είναι όλα διαφορετικά, μια ασθενής διάταξη ορίζεται από $a\,\boldsymbol{\rho}\,b$, $a\,\boldsymbol{\rho}\,c$, $b\,\boldsymbol{\rho}\,c$, $a\,\boldsymbol{\rho}\,a$, $b\,\boldsymbol{\rho}\,b$, $c\,\boldsymbol{\rho}\,c$. Μπορούμε να αναπαραστήσουμε αυτή τη διάταξη εάν θεωρήσουμε τα a, b, c ως τρία σημεία σε μια γραμμή, με $x\,\boldsymbol{\rho}\,y$ εάν το x βρίσκεται στα αριστερά του y ή εάν $x = y$. Η αντίστροφη σχέση βάζει τα στοιχεία στη σειρά c, b, a.

Παράδειγμα 2.2 Ορίζουμε στο επίπεδο τη σχέση $\boldsymbol{\rho}$ με:

$$(x_1, y_1)\,\boldsymbol{\rho}\,(x_2, y_2) \quad \text{εάν} \quad \begin{array}{l} \text{είτε } y_1 < y_2 \\ \text{είτε } y_1 = y_2 \text{ και } x_1 \le x_2 \end{array}$$

Στο Σχήμα 2.9 βλέπουμε οτι $(x_1, y_1)\,\boldsymbol{\rho}\,(x_2, y_2)$ σημαίνει οτι είτε το (x_1, y_1) βρίσκεται σε μια οριζόντια γραμμή γνήσια κάτω από το (x_2, y_2), ή τα δύο σημεία βρίσκονται στην ίδια οριζόντια γραμμή και το (x_1, y_1) είναι ίσο ή βρίσκεται στα αριστερά του (x_2, y_2).

Παράδειγμα 2.3 Στο σύνολο $A = \{\{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}\}$, ορίζουμε $x\,\boldsymbol{\rho}\,y$ να σημαίνει $x \subseteq y$ για x, $y \in A$.



Σχήμα 2.9: Σχέση διάταξης στο επίπεδο.

Άσκηση 2.10 Ελέγξτε οτι ικανοποιούνται οι ιδιότητες (ΑΔ1), (ΑΔ2) και (ΑΔ3) για τα παραπάνω παραδείγματα.

Άσκηση 2.11 Δείξτε οτι κάθε σχέση ασθενούς διάταξης είναι ανακλαστική.

Η σχέση 'είναι υποσύνολο του' (στο σύνολο των υποσυνόλων ενός χώρου U) ικανοποιεί

$$(X \subseteq Y \text{ και } Y \subseteq Z) \text{ συνεπάγεται } X \subseteq Z$$

$$(X \subseteq Y \text{ και } Y \subseteq X) \text{ συνεπάγεται } X = Y$$

αλλά εν γένει μπορεί να έχουμε σύνολα X, Y με $X \not\subseteq Y$ και $Y \not\subseteq X$. Αυτό σημαίνει οτι ο εγκλεισμός συνόλων ικανοποιεί γενικά τις (ΑΔ1) και (ΑΔ3), αλλά όχι την (ΑΔ2). Μια σχέση σε ένα σύνολο A που ικανοποιεί τις ιδιότητες (ΑΔ1) και ΑΔ(3) ονομάζεται **μερική διάταξη**. Εάν A είναι οποιοδήποτε σύνολο του οποίου τα στοιχεία είναι σύνολα, ο εγκλεισμός ορίζει μια μερική διάταξη στο A.

Εάν $\boldsymbol{\rho}$ είναι μια ασθενής διάταξη στο σύνολο A, τότε η αντίστοιχη **γνήσια διάταξη** $\boldsymbol{\tau}$ ορίζεται με

$$x \,\boldsymbol{\tau}\, y \text{ εάν και μόνον εάν } x \,\boldsymbol{\rho}\, y \text{ και } x \neq y\,.$$

Για παράδειγμα, εάν $\boldsymbol{\rho}$ είναι η $\leq$, τότε $\boldsymbol{\tau}$ είναι η $<$.

Πρόταση 2.6 *Μια γνήσια διάταξη* $\boldsymbol{\tau}$ *στο σύνολο* A *ικανοποιεί:*

(ΓΔ1) $a \,\boldsymbol{\tau}\, b$ *και* $b \,\boldsymbol{\tau}\, c$ *συνεπάγονται* $a \,\boldsymbol{\tau}\, c$

(ΓΔ2) εάν $a, b \in A$, *τότε ακριβώς μια από τις ακόλουθες σχέσεις ισχύει (και οι άλλες δύο όχι)*

$$a \,\boldsymbol{\tau}\, b, \quad b \,\boldsymbol{\tau}\, a, \quad a = b\,.$$

Απόδειξη. Θεωρούμε τη γνήσια διάταξη $\boldsymbol{\tau}$ που αντιστοιχεί στην ασθενή διάταξη $\boldsymbol{\rho}$. Υποθέτουμε οτι ισχύουν οι $a \,\boldsymbol{\tau}\, b$ και $b \,\boldsymbol{\tau}\, c$. Τότε ισχύουν $a \,\boldsymbol{\rho}\, b$ και $b \,\boldsymbol{\rho}\, c$, και από την (ΑΔ1) συμπεραίνουμε οτι $a \,\boldsymbol{\rho}\, c$. Δεν μπορεί να ισχύει $a = c$, γιατί εάν ίσχυε, με αντικατάσταση στην $b\,\boldsymbol{\rho}\,c$ παίρνουμε $b\,\boldsymbol{\rho}\,a$ και μαζί με τη $a\,\boldsymbol{\rho}\,b$ και την (ΑΔ3), έχουμε $a = b$, που είναι αδύνατον αφού $a\,\boldsymbol{\tau}\,b$. Εχουμε επαληθεύσει τη (ΓΔ1).

Από την (ΑΔ2) έχουμε, για κάθε $a, b \in A$, μία από τις $a\,\boldsymbol{\rho}\,b$ ή $b\,\boldsymbol{\rho}\,a$. Αρα ισχύει μια από τις $a\,\boldsymbol{\tau}\,b$ ή $a = b$ ή $b\,\boldsymbol{\tau}\,a$. Η $a = b$ αντιφάσκει με τις άλλες δύο, άρα δεν μπορούν να ισχύουν ταυτόχρονα. Η $a\,\boldsymbol{\tau}\,b$ και η $b\,\boldsymbol{\tau}\,a$ δεν μπορούν να ισχύουν ταυτόχρονα, γιατί τότε θα είχαμε $a\,\boldsymbol{\rho}\,b$ και $b\,\boldsymbol{\rho}\,a$, και από την (ΑΔ3), $a = b$, που πάλι δίδει αντίφαση. Εχουμε επαληθεύσει τη (ΓΔ2).

□

Η ιδιότητα (ΓΔ2) ονομάζεται **κανόνας τριχοτομίας**.

Ασκήσεις

Άσκηση 2.12 Ελέγξατε εάν ισχύουν οι ισότητες

α΄. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

β΄. $(A \vartriangle B) \times C = (A \times C) \vartriangle (B \times C)$.

Άσκηση 2.13 Στο $A = \mathbb{N} \times \mathbb{N}$ ορίζουμε τη σχέση $\boldsymbol{\sigma}$, δηλαδή $\boldsymbol{\sigma} \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$, ως εξής:

$$(m,\, n)\ \boldsymbol{\sigma}\ (r,\, s) \quad \text{εάν} \quad m + s = r + n\,.$$

Δείξτε οτι η $\boldsymbol{\sigma}$ είναι σχέση ισοδυναμίας. Οι κλάσεις ισοδυναμίας αυτής της σχέσης αντιστοιχούν με φυσιολογικό τρόπο στα στοιχεία ενός γνωστού συνόλου. Ποιό είναι αυτό;

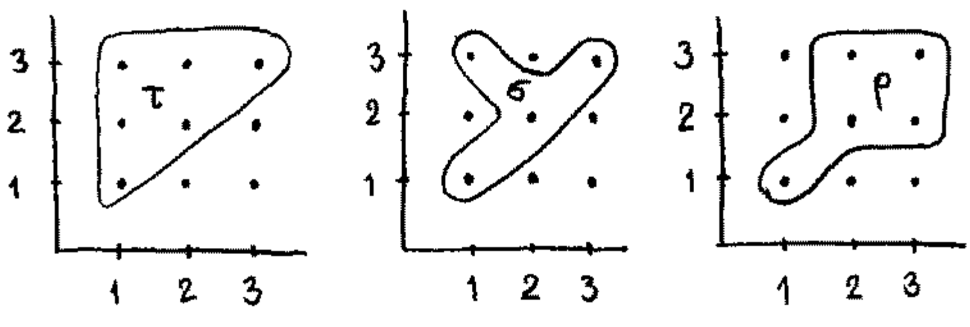
Άσκηση 2.14 Θεωρούμε τις σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο X, δηλαδή $\boldsymbol{\rho}, \boldsymbol{\sigma} \subseteq X \times X$. Εάν οι $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ είναι συμμετρικές, εξετάστε εάν η $\boldsymbol{\rho} \cup \boldsymbol{\sigma}$ η $\boldsymbol{\rho} \cap \boldsymbol{\sigma}$ και η $\boldsymbol{\rho} \setminus \boldsymbol{\sigma}$ είναι επίσης συμμετρικές.

Άσκηση 2.15 Υπάρχει κάποιο λάθος στην παρακάτω απόδειξη οτι εάν μία σχέση $\sim$ είναι συμμετρική και μεταβατική, τότε είναι ανακλαστική; Εξηγήστε την απάντησή σας.
'Απόδειξη': Εστω $a \sim b$. Αφού η $\sim$ είναι συμμετρική, $b \sim a$. Αφού η $\sim$ είναι μεταβατική, από τα $a \sim b$ και $b \sim a$ συμπεραίνουμε $a \sim a$. Αρα η $\sim$ είναι ανακλαστική.

Άσκηση 2.16 Θεωρούμε το σύνολο $A = \{1,\, 2,\, 3\}$ και τις σχέσεις που ορίζονται στο Σχήμα 2.10.

α΄. Ποιο υποσύνολο του $A \times A$ αποτελεί τη σχέση $x > y$ στο A;

β΄. Πώς συμβολίζουμε συνήθως τη σχέση που ορίζεται από το υποσύνολο $\boldsymbol{\tau}$ του $A \times A$;

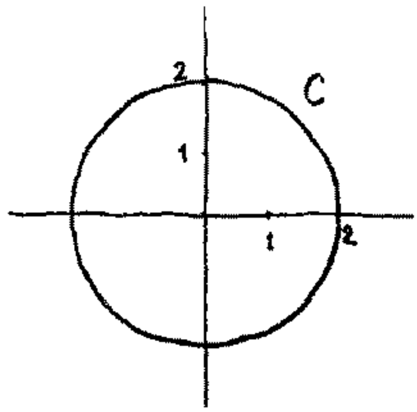


Σχήμα 2.10: Σχέσεις στο σύνολο $A = \{1,\, 2,\, 3\}$.

γ΄. Για κάθε μια από τις σχέσεις $\boldsymbol{\rho}$ και $\boldsymbol{\sigma}$ στο A, εξετάστε εάν είναι ανακλαστική, συμμετρική, μεταβατική.

δ΄. Εάν κάποια από τις σχέσεις $\boldsymbol{\rho}$, $\boldsymbol{\sigma}$ είναι σχέση ισοδυναμίας, ποιά είναι η αντίστοιχη διαμέριση του A;

Άσκηση 2.17 Ποια σχέση στο $\mathbb{R}$ ορίζει ο κύκλος $C \subseteq \mathbb{R} \times \mathbb{R}$; (Σχήμα 2.11)



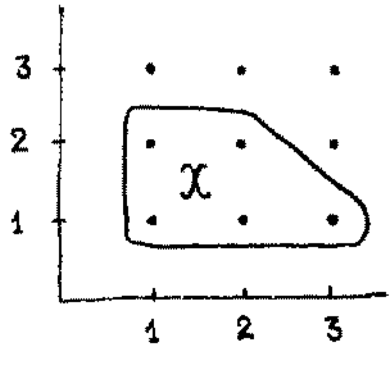
Σχήμα 2.11: Ο κύκλος ως σχέση.

Άσκηση 2.18 Σε κάθε μία από τις ακόλουθες περιπτώσεις βρείτε τα ελάχιστα στον αριθμό στοιχεία με τα οποία πρέπει να συμπληρωθεί το σύνολο $\boldsymbol{\chi}$ ώστε να ορίζει μία σχέση (Σχήμα 2.12)

α΄. ανακλαστική,

β΄. συμμετρική,

γ΄. μεταβατική.



Σχήμα 2.12: Σχέση στο σύνολο $A = \{1,\ 2,\ 3\}$.

Άσκηση 2.19 Στο $\mathbb{Z}$ θεωρούμε τις σχέσεις $\equiv_6$ και $\equiv_4$. Ποιά είναι η σχέση $\equiv_6 \cap \equiv_4$;

Άσκηση 2.20 Θεωρούμε τα σύνολα $A = \{1, 2, 3\}$, $B = \{a, b\}$ και $C = A \times B$.

α΄. Γράψτε όλα τα στοιχεία του C.

β΄. Σχεδιάστε το καρτεσιανό γινόμενο $A \times C$.

γ΄. Ορίζουμε τη σχέση $\boldsymbol{\rho}$ μεταξύ των συνόλων A και C, με

$$x\,\boldsymbol{\rho}\,(u, v) \qquad \text{εάνν} \qquad x > u\,.$$

Σημειώστε στο σχέδιο του $A \times C$ το υποσύνολο που ορίζει τη σχέση $\boldsymbol{\rho}$.

Άσκηση 2.21 Στο σύνολο $\{1, 2, 3, 4, 5, 6\}$ ορίζουμε τη σχέση

$$x\,\boldsymbol{\rho}\,y \quad \text{εάνν} \quad y \text{ είναι πολλαπλάσιο του } x\,.$$

Εξετάστε εάν η σχέση $\boldsymbol{\rho}$ ικανοποιεί τη μεταβατική και την αντισυμμετρική ιδιότητα, και εάν τις ικανοποιεί, εξετάστε τι είδους διάταξη είναι.

Κεφάλαιο 3

Συναρτήσεις

Η έννοια της συνάρτησης έχει τεράστια σημασία στα σύγχρονα Μαθηματικά. Αρχικά η έννοια της συνάρτησης κατέλαβε κεντρική θέση στον Απειροστικό Λογισμό. Η σημερινή έννοια εξελίχθηκε σταδιακά από τις πρώτες προσπάθειες να ορισθεί η έννοια της συνάρτησης, που ήταν κάπως συγκεχυμένες. Σήμερα η Θεωρία Συνόλων, δίδει έναν πολύ γενικό και απλό ορισμό. Η μεγάλη γενικότητα του ορισμού κάνει απαραίτητη την επιβολή επιπλέον περιορισμών σε διάφορους κλάδους: στον Απειροστικό Λογισμό, για παράδειγμα, ενδιαφερόμαστε σε συναρτήσεις που είναι διαφορίσιμες ή ολοκληρώσιμες.

Σε αυτό το Κεφάλαιο θα αναπτύξουμε, μέσα από παραδείγματα, την έννοια της συνάρτησης και θα δούμε κάποιες από τις γενικές ιδιότητες συναρτήσεων. Το γράφημα μιας συνάρτησης συνδέεται τόσο με τον τυπικό ορισμό όσο και την παραδοσιακή εικόνα.

Η παραδοσιακή εικόνα

Παραδοσιακά, εισάγουμε μια 'μεταβλητή' x, που συνήθως είναι πραγματικός αριθμός, και μιλάμε για τη 'συνάρτηση $f(x)$ του x'. Το βασικό είναι οτι μπορούμε να υπολογίσουμε την τιμή $f(x)$ για κάθε δεδομένη τιμή της x (πιθανόν με κάποιους περιορισμούς, όπως $x \neq 0$ ή $x > 0$, που εξαρτώνται από τη συνάρτηση). Ετσι η τετραγωνική συνάρτηση παίρνει τιμή x^2 για κάθε x, η εκθετική συνάρτηση παίρνει την τιμή e^x για κάθε πραγματικό αριθμό x, η συνάρτηση $\tan$ παίρνει την τιμή $\tan(x)$ για κάθε x εκτός από τα περιττά πολλαπλάσια του $\pi/2$, η λογαριθμική συνάρτηση παίρνει την τιμή $\log(x)$ για κάθε πραγματικό $x > 0$, το παραγοντικό $x!$ ορίζεται μόνο για θετικούς ακεραίους.

Σε κάθε περίπτωση μπορούμε, θεωρητικά, να υπολογίσουμε την τιμή της συνάρτησης που αντιστοιχεί στις σχετικές τιμές του x. Η συνάρτηση συσχετίζει σε κάθε κατάλληλο πραγματικό αριθμό x μια τιμή $f(x)$ που είναι επίσης κάποιος πραγματικός αριθμός.

Δεν πρέπει να συγχέομε τις τιμές της συνάρτησης με την ίδια τη συνάρτηση. Η λογαριθμική συνάρτηση δεν είναι η τιμή $\log(x)$, αλλά ο κανόνας 'πάρε το λογάριθμο' που μας λέει πώς να βρούμε την τιμή. Μπορούμε να πούμε οτι είναι το σύμβολο log. Σκεφτόμαστε μια συνάρτηση σαν ένα 'κανόνα', που για κάθε πραγματικό αριθμό x, πιθανόν με κάποιους περιορισμούς, ορίζει έναν άλλο πραγματικό αριθμό $f(x)$. Θα επιμείνουμε να είναι η $f(x)$ μοναδικά προσδιορισμένη: ένας κανόνας που δίδει δύο διαφορετικές απαντήσεις σε ένα ερώτημα δεν είναι ιδιαίτερα χρήσιμος. Αυτό σημαίνει οτι πρέπει να είμαστε προσεκτικοί με συναρτήσεις όπως 'τετραγωνική ρίζα', και να προσδιορίζουμε εάν εννοούμε τη θετική ή την αρνητική ρίζα.

Άσκηση 3.1 Η περίμετρος, σε μέτρα, ενός τετραγώνου με πλευρά s μέτρα είναι $P = 4s$.

α′. Γράψτε αυτήν τη σχέση σε μορφή συνάρτησης, όπου g είναι το όνομα της συνάρτησης.

β′. Υπολογίστε $g(s+4)$ και γράψτε τι σημαίνει.

γ′. Υπολογίστε $g(s)+4$ και γράψτε τι σημαίνει.

δ′. Υπολογίστε $g(4s)$ και γράψτε τι σημαίνει.

Η γενική έννοια της συνάρτησης

Η πιο γενική έννοια της συνάρτησης έρχεται από την παραδοσιακή, εάν αφαιρέσουμε τον περιορισμό να είναι τα x και $f(x)$ πραγματικοί αριθμοί. Το απλούστερο είναι να μη θέσουμε κανέναν περιορισμό στο τι είναι τα x και $f(x)$. Τότε πρέπει να κάνουμε πιο σαφές τι εννοούμε με ‘κανόνα’.

Θεωρούμε δύο σύνολα, A και B. Αρχικά, ονομάζουμε *συνάρτηση από το* A στο B έναν κανόνα που αντιστοιχεί σε κάθε στοιχείο του A ένα *μοναδικό* στοιχείο του B.

Αυτός ο ορισμός δίδει μία πολύ ευρεία έννοια. Περιλαμβάνει όλα τα προηγούμενα παραδείγματα: θεωρούμε ως A ένα κατάλληλο υποσύνολο του $\mathbb{R}$, και ως B το $\mathbb{R}$. Για την εκθετική συνάρτηση $A=\mathbb{R}$, $B=\mathbb{R}$ και ο κανόνας είναι $f(x)=e^x$. Για το λογάριθμο $A=\{x\in\mathbb{R}|\, x>0\}$, $B=\mathbb{R}$ και ο κανόνας $f(x)=\log(x)$. Για το παραγοντικό $A=\mathbb{N}$, $B=\mathbb{N}$ και $f(x)=x!$

Παραδείγματα άλλου είδους συναρτήσεων:

$A=\{$όλοι οι κύκλοι στο επίπεδο$\}$, $B=\mathbb{R}$, $f(x)=$ η ακτίνα του x.

$A=\{$όλα τα μη κενά υποσύνολα του $\{0,\,2,\,4\}\}$, $B=\mathbb{N}$, $f(x)=$ ο μικρότερος αριθμός στο x.

$A=\mathbb{Z}$, $B=\{0,1,2\}$, $f(x)=$ το υπόλοιπο του x όταν το διαιρέσουμε με το 3.

Η συνήθης ορολογία είναι να ονομάζουμε το A **πεδίο ορισμού** της f και το B **πεδίο τιμών** της f, και να γράφουμε

$$f:\,A\to B$$

για να συμβολίσουμε τη συνάρτηση f με πεδίο ορισμού A και πεδίο τιμών B.

Αυτό που απομένει να αποσαφηνίσουμε για να έχουμε τον τυπικό ορισμό της συνάρτησης είναι ο ‘κανόνας’. Θα καταφύγουμε στην ίδια ιδέα που χρησιμοποιήσαμε για τις σχέσεις: θα εκφράσουμε τη συσχέτιση μεταξύ του στοιχείου $x\in A$ και του στοιχείου $f(x)\in B$ βάζοντάς τα σε ένα διατεταγμένο ζεύγος $(x,\,f(x))$. Ο ‘κανόνας’ τώρα γίνεται ένας ‘κατάλογος’, το σύνολο όλων των διατεταγμένων ζευγών $(x,\,f(x))$ για όλα τα x στο A, και αυτό δεν είναι τίποτε άλλο από ένα υποσύνολο του καρτεσιανού γινομένου $A\times B$. Η απαίτηση να ορίζεται το $f(x)$ για κάθε $x\in A$ σημαίνει οτι για κάθε $x\in A$ πρέπει να υπάρχει *κάποιο* στοιχείο (x,y) στο σύνολο. Η μοναδικότητα του $f(x)$ σημαίνει οτι το y πρέπει να είναι *μοναδικό*. Τώρα βλέπουμε πώς το σύνολο των διατεταγμένων ζευγών εκφράζει τον κανόνα. Για να βρούμε το $f(x)$ αναζητούμε στο σύνολο ένα ζεύγος με πρώτο στοιχείο x. Ενα τέτοιο ζεύγος (x,y) υπάρχει και είναι μοναδικό. Θέτουμε $f(x)=y$.

Ορισμός. Εάν A και B είναι σύνολα, μια **συνάρτηση** $f:\,A\to B$ είναι ένα υποσύνολο f του $A\times B$, τέτοιο ώστε:

Σ1 Εάν $x \in A$, τότε υπάρχει $y \in B$ τέτοιο ώστε $(x, y) \in f$.

Σ2 Αυτό το y είναι μοναδικό. Δηλαδή εάν $x \in A$ και υπάρχουν y, $z \in B$ τέτοια ώστε $(x, y) \in f$ και $(x, z) \in f$, τότε $y = z$.

Μια συνάρτηση ονομάζεται επίσης **απεικόνιση**, ή **μετασχηματισμός**.

Βλέπουμε οτι μία συνάρτηση είναι μια σχέση, που ικανοποιεί τις ιδιότητες Σ1 και Σ2. Σύμφωνα με αυτόν τον ορισμό, η τετραγωνική συνάρτηση $y = x^2$ στο $\mathbb{R}$ είναι το υποσύνολο του $\mathbb{R} \times \mathbb{R}$

$$\{(x, x^2) | \, x \in \mathbb{R}\} \, .$$

Για να επανέλθουμε στο συνήθη ορισμό θέτουμε $f(x)$ το μοναδικό στοιχείο $y \in B$ για το οποίο $(x, y) \in f$. Έχουμε $y = f(x)$ εάν και μόνον εάν $(x, \, y) \in f$.

Η παραδοσιακή έννοια της συνάρτησης δίδει περισσότερη έμφαση στον τρόπο με τον οποίο παίρνουμε το $f(x)$ από το x. Στα σύγχρονα Μαθηματικά προτιμούμε, για τον τυπικό ορισμό της γενικής έννοιας της συνάρτησης, να μην αναφερθούμε σε αυτό, αλλά να θεωρήσουμε οτι η ίδια η συνάρτηση δίδει την αντιστοίχηση, μέσω των ζευγών $(x, \, f(x))$. Στην καθημερινή χρήση χρησιμοποιούμε εκφράσεις πιο κοντά στην παραδοσιακή έννοια, όπως:

‘Ορίζουμε μια συνάρτηση $f : A \to B$ μέσω της $f(x) = \dots$ για κάθε $x \in A$’.

Σε κάθε περίπτωση οι τελείες ‘...’ αντικαθίστανται από τη διαδικασία μέσω της οποίας βρίσκουμε το $f(x)$ από το x.

Αυτό που πρέπει να προσέχουμε σε κάθε περίπτωση είναι να ελέγξουμε οτι η διαδικασία ‘...’ ορίζει το $f(x)$ με μοναδικό τρόπο, και οτι η τιμή $f(x)$ ανήκει στο B για κάθε $x \in A$.

Ας δούμε μερικά παραδείγματα όπου αυτές οι συνθήκες *δεν ικανοποιούνται.*

‘Ορίζουμε $f : \mathbb{R} \to \mathbb{R}$ με $f(x) = \dfrac{x^2 + 17x + 93}{x + 1}$.’

Αυτό δεν ορίζει συνάρτηση γιατί όταν $x = -1$, το κλάσμα δεν ορίζεται, άρα η τιμή $f(-1)$ δεν έχει προσδιοριστεί ως πραγματικός αριθμός. Εάν αλλάξουμε τον ορισμό σε $f : \mathbb{R} \backslash \{-1\} \to \mathbb{R}$ τότε είναι εντάξει.

‘Ορίζουμε $f : \{x \in \mathbb{Q} | \, x > 0\} \to \mathbb{Q}$ με $f(x) = \sqrt{x}$’,

όπου $\sqrt{x}$ είναι η θετική τετραγωνική ρίζα. Σε αυτήν την περίπτωση για κάποιες τιμές του x στο $\{x \in \mathbb{Q} | \, x > 0\}$ η τιμή της $\sqrt{x}$ δεν είναι ρητός αριθμός.

‘ Ορίζουμε $f : \mathbb{R} \to \mathbb{Z}$ με $f(x) =$ ο πλησιέστερος ακέραιος προς το x ’.

Σε αυτήν την περίπτωση η τιμή $f(\frac{1}{2})$ δεν ορίζεται με μοναδικό τρόπο.

***Άσκηση* 3.2** Οι παρακάτω συναρτήσεις έχουν πεδίο τιμών το $\mathbb{R}$, και πεδίο ορισμού κάποιο υποσύνολο του $\mathbb{R}$. Βρείτε σε κάθε περίπτωση πιο είναι το μεγαλύτερο δυνατό πεδίο ορισμού.

α′. $h(x) = \log x$

β′. $\alpha(v) = -v$

γ′. $j(\beta) = \frac{1}{\beta^2 - 1}$

δ′. $g(u) = \log \log \cos u$

Γενικές ιδιότητες συναρτήσεων

Εάν $f : A \to B$ είναι συνάρτηση, η **εικόνα** της f είναι το υποσύνολο του B:

$$f(A) = \{f(x) |\, x \in A\}\ .$$

Η εικόνα της f συμβολίζεται επίσης $\operatorname{im}(f)$

Η εικόνα της f είναι το σύνολο των τιμών $f(x)$ που παίρνουμε για όλα τα x από το πεδίο ορισμού. *Δεν* είναι απαραίτητο να είναι όλο το πεδίο τιμών. Για παράδειγμα, εάν $f : \mathbb{R} \to \mathbb{R}$ είναι η συνάρτηση με τιμές $f(x) = x^2$ τότε η εικόνα είναι το σύνολο των θετικών πραγματικών αριθμών μαζί με το μηδέν (το σύνολο των *μη αρνητικών* πραγματικών αριθμών), και όχι όλο το πεδίο τιμών $\mathbb{R}$.

Η έλλειψη συμμετρίας στον ορισμό της συνάρτησης μπορεί να φανεί παράξενη. Απαιτούμε να ορίζεται το $f(x)$ για κάθε $x \in A$, αλλά δεν απαιτούμε κάθε $b \in B$ να είναι της μορφής $f(x)$ για κάποιο x. Ο λόγος γι' αυτό είναι πρακτικός: όταν χρησιμοποιούμε μια συνάρτηση πρέπει να ξέρουμε εάν ορίζεται. Η ακριβής γνώση του πεδίου ορισμού είναι λοιπόν αναγκαία. Είναι λιγότερο σημαντικό να γνωρίζουμε ακριβώς που βρίσκονται οι τιμές $f(x)$, και μπορούμε να διαλέξουμε το πεδίο τιμών ανάλογα με την περίπτωση (υπό τον όρο οτι η εικόνα περιέχεται στο πεδίο τιμών). Για παράδειγμα, εάν $f : \mathbb{N} \to \mathbb{R}$ είναι η συνάρτηση με τιμές $f(n) = \sqrt[3]{n!}$, η εικόνα της f είναι το σύνολο των κυβικών ριζών των παραγοντικών

$$\{1,\ \sqrt[3]{2},\ \sqrt[3]{6},\ \sqrt[3]{24},\ \sqrt[3]{120}, \ldots\}\ .$$

Είναι απλούστερο να ορίσουμε μία συνάρτηση χρησιμοποιώντας κάποιο ευρύ πεδίο τιμών, και να αφήσουμε το ερώτημα ποιό ακριβώς κομμάτι του πεδίου τιμών αποτελεί η εικόνα για την περίπτωση που το χρειαστούμε.

Πρέπει να παρατηρήσουμε οτι, μιλώντας αυστηρά, δεν μπορούμε να αναφερόμαστε 'στο' πεδίο τιμών μιας συνάρτησης. Θεωρήστε για παράδειγμα τις συναρτήσεις

$$\begin{array}{ll} f : \mathbb{R} \to \mathbb{R} & f(x) = x^2, \\ g : \mathbb{R} \to \mathbb{R}^+ & g(x) = x^2, \end{array} \tag{3.1}$$

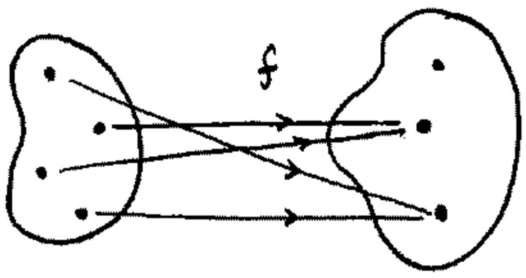
όπου $\mathbb{R}^+ = \{x \in \mathbb{R} |\, x \geq 0\}$. Η πρώτη έχει πεδίο τιμών $\mathbb{R}$, η δεύτερη $\mathbb{R}^+$. Ομως ο τυπικός ορισμός μιας συνάρτησης ως σύνολο διατεταγμένων ζευγών δίδει και για τις δύο περιπτώσεις το ίδιο σύνολο ζευγών $\{(x, x^2) |\, x \in \mathbb{R}\}$. Οι συναρτήσεις f και g είναι ίσες.

Το πεδίο τιμών μιας συνάρτησης δεν είναι σαφώς προσδιορισμένο. Οποιοδήποτε σύνολο περιέχει την εικόνα της συνάρτησης μπορεί να θεωρηθεί ως πεδίο τιμών. Το πεδίο ορισμού, αντιθέτως, είναι μοναδικά προσδιορισμένο.

Μπορούμε να ξεπεράσουμε αυτήν την ασάφεια ορίζοντας μια συνάρτηση να είναι μια διατεταγμένη τριάδα (f, A, B) και όχι απλώς το σύνολο των ζευγών f. Σε ορισμένους κλάδους των μαθηματικών αυτό είναι απαραίτητο, αλλά εδώ θα προτιμήσουμε να δεχθούμε την ασάφεια του απλούστερου ορισμού. Ο συμβολισμός $f : A \to B$ προσδιορίζει σε ποιό πεδίο τιμών αναφερόμαστε σε κάθε περίπτωση.

Για να παραστήσουμε συναρτήσεις $f : \mathbb{R} \to \mathbb{R}$ συχνά χρησιμοποιούμε το γράφημα. Για συναρτήσεις μεταξύ άλλων συνόλων είναι συνήθως προτιμότερη μια παράσταση της μορφής του Σχήματος 3.1.

Για κάθε $x \in A$ η τιμή $f(x)$ βρίσκεται στο άκρο του αντίστοιχου βέλους. Οι συνθήκες του ορισμού της συνάρτησης σε αυτήν τη γραφική παράσταση είναι:



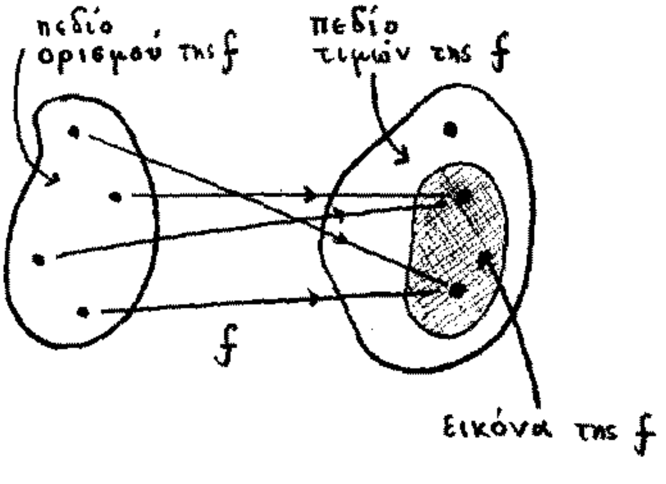
Σχήμα 3.1: Παράσταση συνάρτησης με βέλη.

Σ1′ Ακριβώς ένα βέλος ξεκινάει από κάθε στοιχείο του A,

Σ2′ Ολα τα βέλη καταλήγουν σε στοιχεία του B.

Αυτή η γραφική παράσταση, όπως και τα διαγράμματα Venn, είναι χρήσιμη σε απλά παραδείγματα.

Σε αυτήν την παράσταση η εικόνα της f αποτελείται από τα στοιχεία του B στα οποία καταλήγουν βέλη, Σχήμα 3.2.



Σχήμα 3.2: Η εικόνα της συνάρτησης f.

Η εικόνα θα είναι όλο το σύνολο B εάν κάθε στοιχείο του B βρίσκεται στο τέλος κάποιου βέλους.

Άσκηση 3.3 Προσδιορίστε την εικόνα για τις ακόλουθες συναρτήσεις $f : \mathbb{R} \to \mathbb{R}$.

α′. $f(x) = x^3$

β′. $f(x) = x - 4$

γ′. $f(x) = e^x + 3$

δ′. $f(x) = \begin{cases} 1/x & \text{εάν } x \neq 0 \\ 0 & \text{εάν } x = 0 \end{cases}$

Ορισμός. Λέμε οτι μια συνάρτηση $f : A \to B$ είναι **επεικονική** (ή **επί του B**, ή οτι είναι μία **επεικόνιση**) εάν κάθε στοιχείο του B είναι της μορφής $f(x)$ για κάποιο $x \in A$.

Αυτό συμβαίνει ακριβώς όταν ισχύει $f(A) = B$. Εάν μια συνάρτηση είναι ή όχι επεικονική εξαρτάται από την επιλογή του πεδίου τιμών, η οποία πρέπει να είναι σαφής από τα συμφραζόμενα, όπως στη φράση '$f : A \to B$ είναι επεικονική' (ή 'f είναι επί του B'), όπου το πεδίο τιμών είναι το σύνολο B. Ετσι, από τις συναρτήσεις f και g στην (3.1) η f δεν είναι επεικονική, ενώ η g είναι.

Εάν κανένα στοιχείο του B δεν βρίσκεται στο τέλος δύο διαφορετικών βελών, έχουμε ένα άλλο σημαντικό είδος συνάρτησης:

Ορισμός. Λέμε οτι μια συνάρτηση $f : A \to B$ είναι **ενεικονική** (ή **ένα προς ένα** ή οτι είναι μια **ενεικόνιση**) εάν, για κάθε $x, y \in A$, όταν $f(x) = f(y)$, τότε $x = y$.

Σε αυτήν την περίπτωση η επιλογή του πεδίου τιμών δεν δημιουργεί κανένα πρόβλημα: εάν μια συνάρτηση είναι ενεικονική με μια επιλογή πεδίου τιμών έχει την ίδια ιδιότητα και με κάθε άλλη επιλογή. Ας δούμε κάποια παραδείγματα:

1. $f : \mathbb{R} \to \mathbb{R}$, όπου $f(x) = x^2$. Αυτή δεν είναι ενεικονική, αφού $f(1) = 1 = f(-1)$ αλλά $1 \neq -1$.

2. $h : \mathbb{R}^+ \to \mathbb{R}$, όπου $h(x) = x^2$. Αυτή είναι ενεικονική: εάν x και y είναι μη αρνητικοί πραγματικοί αριθμοί και $x^2 = y^2$ τότε $0 = x^2 - y^2 = (x-y)(x+y)$, άρα είτε $x - y = 0$ οπότε $x = y$, είτε $x + y = 0$ που για x και y μη αρνητικούς συνεπάγεται $x = 0 = y$. Σε κάθε περίπτωση $x = y$.

3. $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}$, όπου $f(x) = 1/x$. Αυτή είναι ενεικονική: εάν $1/x = 1/y$ τότε $x = y$.

Οι 'καλύτερες' συναρτήσεις είναι αυτές που έχουν και τις δύο ιδιότητες:

Ορισμός. Λέμε οτι μια συνάρτηση $f : A \to B$ είναι **αμφιμονοσήμαντη** (ή **αμφεικονική**) εάν είναι ενεικονική και επεικονική.

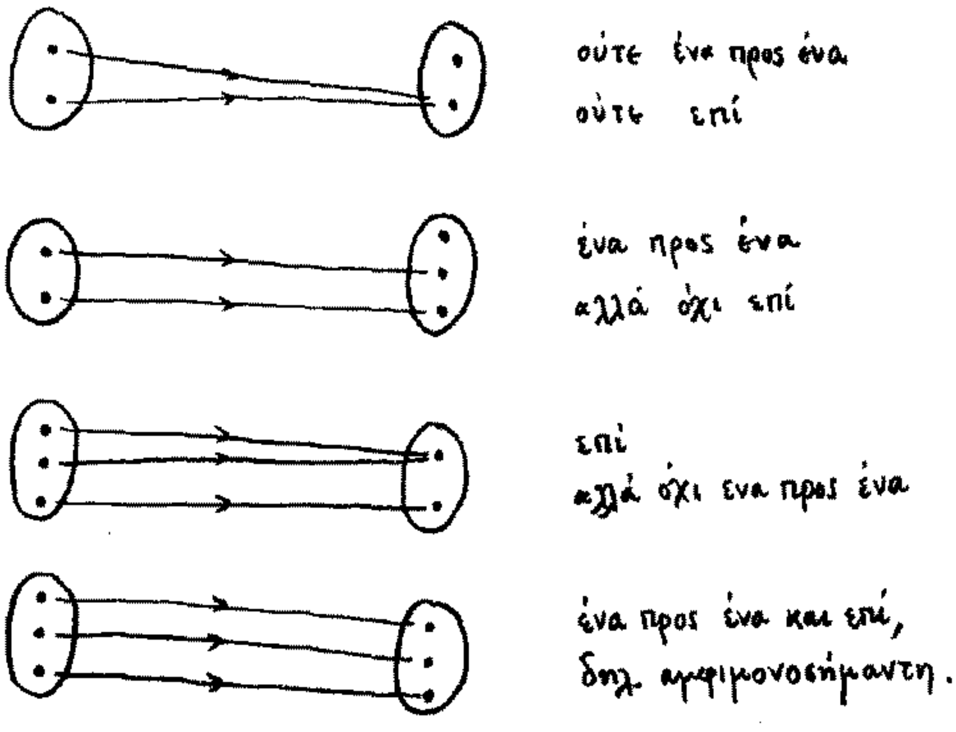
Αυτή η ιδιότητα εξαρτάται από την επιλογή του πεδίου τιμών. Προφανώς η $f : A \to B$ είναι αμφιμονοσήμαντη εάν και μόνον εάν κάθε $b \in B$ είναι της μορφής $b = f(x)$ για ένα μοναδικό $x \in A$.

Όλοι οι δυνατοί συνδυασμοί των ιδιοτήτων ενεικόνισης και επεικόνισης μπορούν να εμφανιστούν, όπως δείχνει το Σχήμα 3.3.

Μια πολύ απλή και πολύ σημαντική συνάρτηση, που ορίζεται σε κάθε σύνολο, είναι η **ταυτοτική** συνάρτηση $i_A : A \to A$ η οποία ορίζεται ως $i_A(a) = a$ για κάθε $a \in A$. Η i_A είναι προφανώς αμφιμονοσήμαντη.

Άσκηση 3.4 Για κάθε μία από τις συναρτήσεις της Άσκησης 3.3, βρείτε εάν είναι

α′. ενεικονική



Σχήμα 3.3: Παραδείγματα συναρτήσεων.

β΄. επεικονική επί του $\mathbb{R}$

γ΄. αμφιμονοσήμαντη.

Άσκηση 3.5 Δώστε παραδείγματα συναρτήσεων $f : \mathbb{Z} \to \mathbb{Z}$ που να είναι:

α΄. ούτε ενεικονική, ούτε επεικονική,

β΄. ενεικονική, αλλά όχι επεικονική,

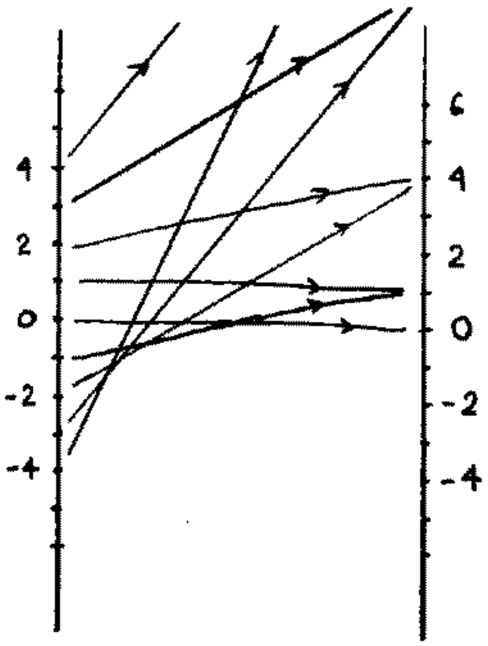
γ΄. επεικονική, αλλά όχι ενεικονική,

δ΄. ενεικονική και επεικονική.

Προσέξτε οτι η εικόνα της f πρέπει να περιέχεται στο $\mathbb{Z}$.

Το γράφημα μιας συνάρτησης

Εχουμε δύο διαφορετικούς τρόπους να παραστήσουμε γραφικά συναρτήσεις από το $\mathbb{R}$ στο $\mathbb{R}$. Το γράφημα της συνάρτησης και την παράσταση με βέλη. Είναι ενδιαφέρον να συγκρίνουμε



Σχήμα 3.4: Παράσταση της συνάρτησης $f(x) = x^2$ με βέλη, I.

τις δύο παραστάσεις. Για τη συνάρτηση $f(x) = x^2$, $(x \in \mathbb{R})$, η παράσταση με βέλη έχει τη μορφή του Σχήματος 3.4.

Μπορούμε να σχεδιάσουμε την παράσταση καλύτερα εάν τοποθετήσουμε το A οριζόντια ώστε να συμπίπτει με το B στο 0, όπως στο Σχήμα 3.5.

Αν περιορίσουμε τα βέλη να είναι μόνον οριζόντια ή κατακόρυφα έχουμε την παράσταση του Σχήματος 3.6.

Σε αυτό το σχήμα είναι φανερό οτι το σημαντικό είναι το σημείο στο οποίο υπάρχει η γωνία σε κάθε βέλος. Καθώς μεταβάλουμε το x όλες οι γωνίες βρίσκονται σε μία καμπύλη, όπως στο Σχήμα 3.7, και εάν αφαιρέσουμε τα βέλη, η καμπύλη που εμφανίζεται στο Σχήμα 3.8 είναι ακριβώς το γράφημα της συνάρτησης f.

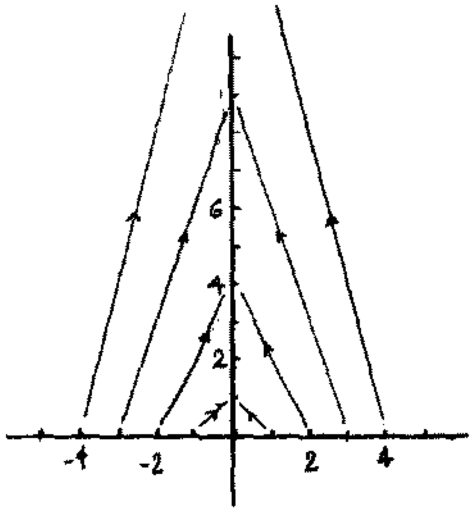
Αντίστροφα, στο γράφημα μπορούμε να προσθέσουμε τα βέλη: αρχίζουμε στο $x \in A$ και κινούμαστε κατακόρυφα μέχρι να συναντήσουμε το γράφημα, κατόπιν οριζόντια μέχρι να συναντήσουμε το B. Αυτό το σημείο θα είναι το $f(x)$.

Τι παριστάνει το γράφημα της συνάρτησης σύμφωνα με τη θεωρία συνόλων; Το επίπεδο είναι το $\mathbb{R} \times \mathbb{R}$, και η γωνία στο βέλος από το x στο $f(x)$ βρίσκεται στο σημείο $(x, f(x))$. Αρα το γράφημα της f παριστάνει το σύνολο

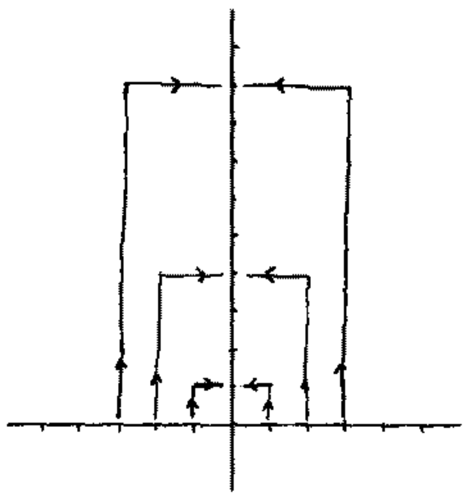
$$\{(x, f(x)) | \, x \in \mathbb{R}\} .$$

Αλλά αυτό είναι ακριβώς ο τυπικός ορισμός της ίδιας της συνάρτησης f. Σχεδιάζοντας το $\mathbb{R} \times \mathbb{R}$ σαν το επίπεδο, το γράφημα προκύπτει ως η φυσική παράσταση της συνάρτησης f.

Για μια γενική συνάρτηση $f : A \to B$ έχουμε μια ανάλογη εικόνα. Πρέπει να σχεδιάσουμε το $A \times B$, και να χρησιμοποιήσουμε αυτό αντί του επιπέδου. Εάν $A = \{a, b, c\}$ και $B =$



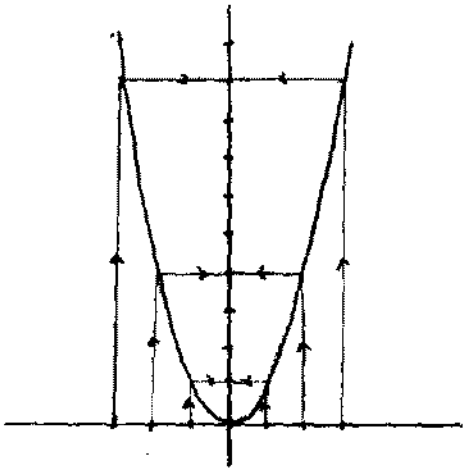
Σχήμα 3.5: Παράσταση της συνάρτησης $f(x) = x^2$ με βέλη, II.



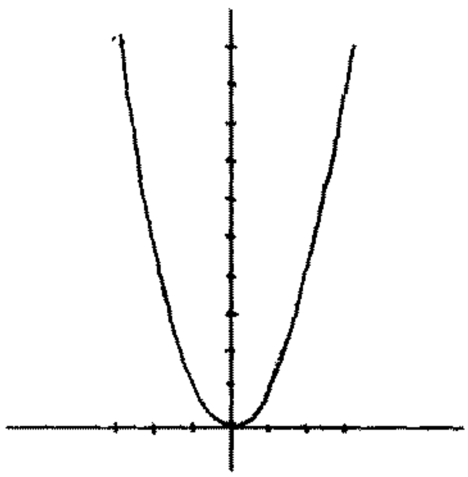
Σχήμα 3.6: Παράσταση της συνάρτησης $f(x) = x^2$ με βέλη, III.

$\{p, q\}$, και $f(a) = q$, $f(b) = p$, $f(c) = q$, η f έχει το 'γράφημα' που εμφανίζεται στο Σχήμα 3.9.

Κατ' αναλογία, το γράφημα μιας συνάρτησης από το $\mathbb{R}$ στο $\mathbb{R}$ θα έπρεπε να έχει τη μορφή του Σχήματος 3.10, αλλά η παραδοσιακή παράσταση, με τους άξονες σχεδιασμένους μέσα στο επίπεδο, είναι πιο συνηθισμένη και πρακτική. Πρέπει όμως να θυμόμαστε οτι οι άξονες δεν αποτελούν μέρος του γραφήματος, αλλά χρησιμεύουν ως δείκτες για τα σημεία (x, y) του επιπέδου.



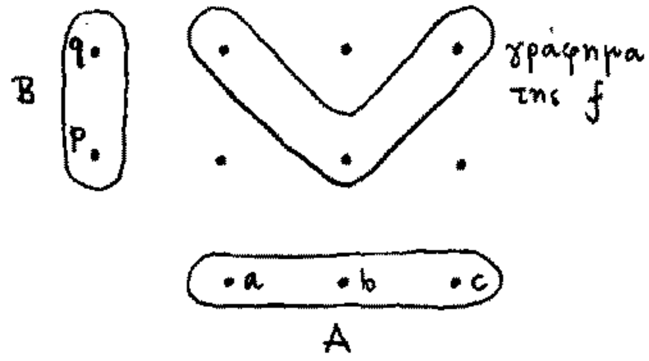
Σχήμα 3.7: Παράσταση της συνάρτησης $f(x) = x^2$ με βέλη, IV.



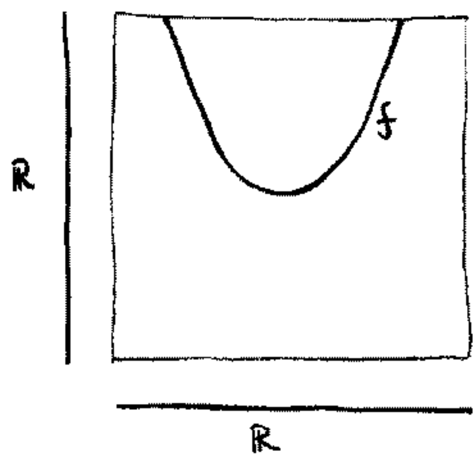
Σχήμα 3.8: Το γράφημα της συνάρτησης $f(x) = x^2$.

Σύνθεση συναρτήσεων

Εάν $f : A \to B$ και $g : C \to D$ είναι δύο συναρτήσεις, και η εικόνα της f είναι υποσύνολο του C, τότε μπορούμε να **συνθέσουμε** την f και τη g, εφαρμόζοντας πρώτα την f και μετά τη g.



Σχήμα 3.9: Γράφημα συνάρτησης.



Σχήμα 3.10: Γράφημα συνάρτησης.

Τυπικά, εάν ικανοποιούνται οι παραπάνω υποθέσεις, ορίζουμε τη συνάρτηση

$$g \circ f : A \to D$$

με

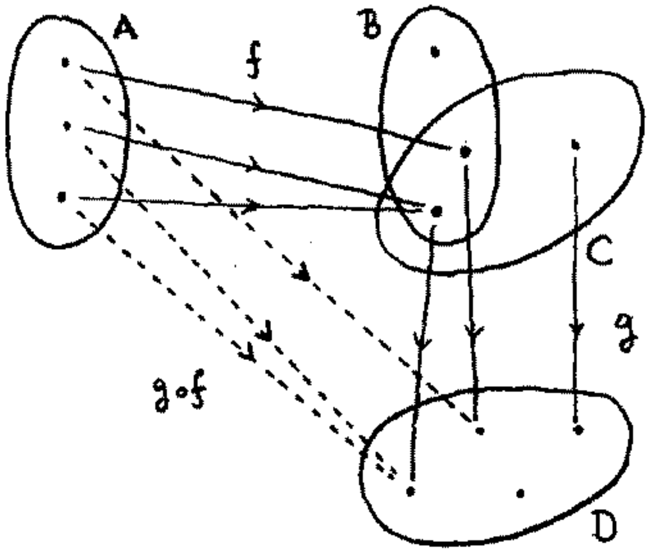
$$(g \circ f)(x) = g(f(x)) .$$

Η υπόθεση οτι $f(A) \subseteq C$ είναι απαραίτητη για να ελέγξουμε οτι έχουμε ορίσει μια συνάρτηση από το A στο D, πράγμα που δεν παρουσιάζει δυσκολία.

Μια σημαντική ιδιότητα της σύνθεσης συναρτήσεων είναι η προσεταιριστικότητα:

Πρόταση 3.1 *Εάν $f : A \to B$, $g : C \to D$ και $h : E \to F$ είναι συναρτήσεις, τέτοιες ώστε η εικόνα της f είναι υποσύνολο του C και η εικόνα της g είναι υποσύνολο του E, τότε ορίζονται οι δύο συναρτήσεις*

$$h \circ (g \circ f) : A \to F$$



Σχήμα 3.11: Σύνθεση συναρτήσεων.

$$(h \circ g) \circ f : A \to F$$

και είναι ίσες.

Απόδειξη. Εύκολα ελέγχουμε οτι ικανοποιούνται οι συνθήκες ώστε να ορίζονται οι δύο συναρτήσεις. Λέγοντας οτι οι συναρτήσεις είναι ίσες εννοούμε οτι τα δύο υποσύνολα του $A \times F$ που ορίζουν τις συναρτήσεις είναι ίσα. Αυτό σημαίνει οτι για κάθε $x \in A$ οι δύο συναρτήσεις παίρνουν την ίδια τιμή. Πράγματι

$$(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))),$$
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

□

Άσκηση 3.6 Δίδονται οι συναρτήσεις f, g και h από τους φυσικούς αριθμούς στους φυσικούς αριθμούς, που ορίζονται από:

α′. $f(n) = n + 1$

β′. $g(n) = 2n$

γ′. $h(n) = \begin{cases} 0 & \text{εάν } n \text{ είναι άρτιος} \\ 1 & \text{εάν } n \text{ είναι περιττός} \end{cases}$

Καθορίστε τις συναρτήσεις $f \circ f$, $f \circ g$, $g \circ f$, $g \circ h$, $h \circ g$ και $(f \circ g) \circ h$.

Άσκηση 3.7 Δίδονται συναρτήσεις f και g τέτοιες ώστε να ορίζεται η σύνθεση $g \circ f$. Δείξτε οτι α′. Εάν η $g \circ f$ είναι επεικονική, τότε η g είναι επεικονική.

β′. Εάν η $g \circ f$ είναι ενεικονική, τότε η f είναι ενεικονική.

γ′. Βρείτε παραδείγματα συναρτήσεων f και g για να δείξετε οτι δεν ισχύουν οι αντίστροφες συνεπαγωγές, δηλαδή οτι εάν η g είναι επεικονική ή εάν η f είναι ενεικονική, δεν ισχύει υποχρεωτικά το ίδιο για τη σύνθεση $g \circ f$.

Άσκηση 3.8 Εάν $f : A \to B$ και $g : B \to C$ είναι αμφιμονοσήμαντες, δείξτε οτι $g \circ f : A \to C$ είναι αμφιμονοσήμαντη.

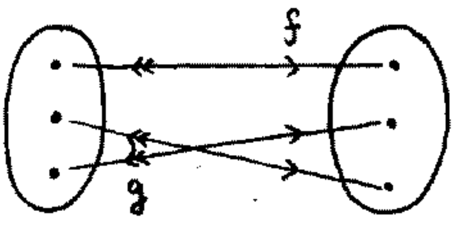
Αντίστροφες Συναρτήσεις

Συχνά σκεφτόμαστε οτι η συνάρτηση $f : A \to B$ παίρνει ένα στοιχείο $x \in A$ και του κάνει κάτι για να καταλήξει με το $f(x) \in B$. Μερικές φορές μπορούμε να βρούμε μια συνάρτηση που κάνει το αντίστροφο και αναιρεί αυτό που έκανε η f.

Ορισμός. Θεωρούμε μια συνάρτηση $f : A \to B$. Τότε η συνάρτηση $g : B \to A$ ονομάζεται **αντίστροφη συνάρτηση** της f εάν

1. $g(f(x)) = x$ για κάθε $x \in A$ και
2. $f(g(y)) = y$ για κάθε $y \in B$.

Προσέξτε οτι οι δύο συνθήκες γράφονται, ισοδύναμα, ως $g \circ f = i_A$ και $f \circ g = i_B$. Στο ακόλουθο σχήμα η f παριστάνεται με απλά βέλη και η g με διπλά.



Σχήμα 3.12: Αντίστροφη συνάρτηση.

Θεώρημα 3.2 *Μια συνάρτηση $f : A \to B$ έχει αντίστροφη συνάρτηση εάν και μόνο εάν η f είναι αμφιμονοσήμαντη.*

Απόδειξη. Υποθέτουμε οτι η f έχει αντίστροφη συνάρτηση g. Για να αποδείξουμε οτι η f είναι ενεικονική, υποθέτουμε οτι $f(x) = f(y)$. Τότε $x = g(f(x)) = g(f(y)) = y$, άρα η f είναι πράγματι ενεικόνιση. Για να αποδείξουμε οτι η f είναι επεικονική, θεωρούμε $y \in B$. Τότε $y = f(g(y))$, άρα το y είναι της μορφής $f(x)$, για $x = g(y)$. Συνεπώς η f είναι επεικόνιση.

Αντίστροφα, υποθέτουμε οτι η f είναι αμφιμονοσήμαντη. Τότε, αφού η f είναι επεικονική, για κάθε $y \in B$ υπάρχει $x \in A$ τέτοιο ώστε $y = f(x)$. Εφόσον η f είναι ενεικονική, αυτό το x είναι μοναδικό. Ορίζουμε τη συνάρτηση $g : B \to A$ με $g(y) = x$. Η g είναι η αντίστροφη συνάρτηση της f.

□

Η αντίστροφη συνάρτηση, εάν υπάρχει, είναι μοναδική: υποθέτουμε οτι g και h είναι αντίστροφες συναρτήσεις της $f : A \to B$. Τότε, για κάθε $y \in B$, υπάρχει μοναδικό $x \in A$ τέτοιο ώστε $y = f(x)$, και

$$g(y) = g(f(x)) = x = h(f(x)) = h(y)\,.$$

Συνεπώς $g = h$.

Την αντίστροφη συνάρτηση της $f : A \to B$ τη συμβολίζουμε $f^{-1} : B \to A$. Παρατηρείστε οτι εάν θεωρήσουμε την f ως μία σχέση μεταξύ των στοιχείων του A και του B, τότε η αντίστροφη συνάρτηση f^{-1} είναι ακριβώς η αντίστροφη σχέση μεταξύ των στοιχείων του B και του A.

Παράδειγμα 3.1 $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^3$. Αυτή είναι αμφιμονοσήμαντη, και έχει αντίστροφη συνάρτηση $g : \mathbb{R} \to \mathbb{R},\ g(x) = \sqrt[3]{x}$.

Παράδειγμα 3.2 $f : \mathbb{R} \to \mathbb{R},\ f(x) = x^2$. Δεν είναι ούτε ενεικονική ούτε επεικονική, άρα δεν έχει αντίστροφη συνάρτηση. Τί συμβαίνει με τις τετραγωνικές ρίζες; Μπορούμε να θεωρήσουμε την αμφιμονοσήμαντη συνάρτηση f με πεδίο ορισμού και πεδίο τιμών το $\mathbb{R}^+ = \{x \in \mathbb{R}\,|\, x \geq 0\}$. Τότε η f έχει αντίστροφο $g(x) = \sqrt{x}$ (τη θετική τετραγωνική ρίζα).

Παράδειγμα 3.3 Υποθέτουμε γνωστές κάποιες ιδιότητες της εκθετικής και της λογαριθμικής συνάρτησης. Θεωρούμε τη συνάρτηση $f : \mathbb{R} \to \mathbb{R},\ f(x) = e^x$. Αυτή είναι ενεικονική, γιατί εάν $e^x = e^y$ τότε $e^{x-y} = 1$ άρα $x - y = 0$ και συνεπώς $x = y$. Όμως δεν είναι επεικονική, και συνεπώς δεν έχει αντίστροφη συνάρτηση. Μπορούμε όμως να θεωρήσουμε τη συνάρτηση $f : \mathbb{R} \to \mathbb{R}^\#$ όπου $\mathbb{R}^\# = \{x \in \mathbb{R}|\, x > 0\}$ και $f(x) = e^x$. Τώρα η f είναι αμφιμονοσήμαντη, και η $g : \mathbb{R}^\# \to \mathbb{R},\ g(y) = \log y$ είναι η αντίστροφη συνάρτηση.

Παράδειγμα 3.4 Υποθέτουμε γνωστές κάποιες ιδιότητες των τριγωνομετρικών συναρτήσεων. Θεωρούμε την $f : \mathbb{R} \to \mathbb{R},\ f(x) = \sin x$. Αυτή δεν είναι ούτε επεικονική ούτε ενεικονική, άρα δεν έχει αντίστροφη συνάρτηση. Πώς θα ορίσουμε το τόξο ημιτόνου, arcsin; Εάν ορίσουμε $\arcsin y$ ως το μοναδικό αριθμό x με $-\pi/2 \leq x \leq \pi/2$ τέτοιον ώστε $\sin x = y$, τότε έχουμε $\sin(\arcsin y) = y$, αλλά δεν ισχύει $\arcsin(\sin x) = x$. Για παράδειγμα, $\arcsin(\sin 6\pi) = \arcsin 0 = 0 \neq 6\pi$.

Μερικές φορές λέγεται οτι η arcsin είναι *πλειότιμη*, δηλαδή οτι οι τιμές της δεν είναι μοναδικά ορισμένες. Σύμφωνα με τον ορισμό της συνάρτησης που δώσαμε, τότε δεν μπορεί να είναι συνάρτηση.

Η καλύτερη λύση είναι να θεωρήσουμε την

$$f : \{x \in \mathbb{R}|\, -\pi/2 \leq x \leq \pi/2\} \to \{x \in \mathbb{R}|\, -1 \leq x \leq 1\},\ f(x) = \sin x\,.$$

Τότε η f είναι αμφιμονοσήμαντη, και arcsin είναι αντίστροφη συνάρτηση αυτής της συνάρτησης.

Άσκηση 3.9 Για τη συνάρτηση της Άσκησης 3.1, σε τί μονάδες εκφράζεται η ποσότητα $g^{-1}(8)$;

Πρόταση 3.3 *Εάν $f : A \to B$ και $g : B \to C$ είναι αμφιμονοσήμαντες, τότε $g \circ f : A \to C$ είναι αμφιμονοσήμαντη και*

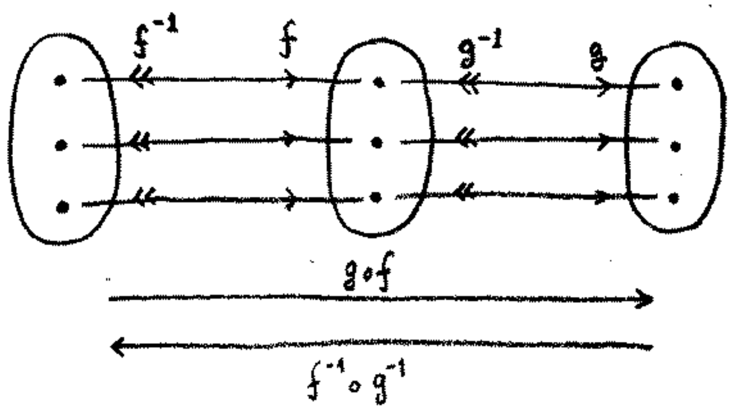
$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}\,.$$

Απόδειξη. Γνωρίζουμε οτι $g \circ f$ είναι αμφιμονοσήμαντη, (Άσκηση 3.8). Επαληθεύουμε οτι $f^{-1} \circ g^{-1}$ είναι η αντίστροφη συνάρτηση, (δες Σχήμα 3.13). Έχουμε

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ (g \circ f)) \\ &= f^{-1} \circ ((g^{-1} \circ g) \circ f) \\ &= f^{-1} \circ (i_B \circ f) \\ &= f^{-1} \circ f \\ &= i_A\,.\end{aligned}$$

Παρόμοια δείχνουμε οτι $(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C$.

□



Σχήμα 3.13: Αντίστροφη συνάρτηση σύνθεσης συναρτήσεων.

Δεξιά και αριστερά αντίστροφα

Είδαμε οτι μια συνάρτηση $f : A \to B$ έχει αντίστροφη συνάρτηση μόνον όταν είναι αμφιμονοσήμαντη. Μερικές φορές μπορούμε να βρούμε μία συνάρτηση που να αντιστρέφει την f μόνον από τη μια πλευρά.

Ορισμός. Θεωρούμε μια συνάρτηση $f : A \to B$. Τότε η συνάρτηση $g : B \to A$ ονομάζεται

1. **αριστερό αντίστροφο** της f εάν $g(f(x)) = x$ για κάθε $x \in A$,
2. **δεξιό αντίστροφο** της f εάν $f(g(y)) = y$ για κάθε $y \in B$.

Προσέξτε οτι αυτές οι συνθήκες γράφονται, ισοδύναμα, ως

1. Η g είναι αριστερό αντίστροφο της f εάν $g \circ f = i_A$,

2. Η g είναι δεξιό αντίστροφο της f εάν $f \circ g = i_B$,

Θεώρημα 3.4 *Μια συνάρτηση $f : A \to B$ έχει*

1. *αριστερό αντίστροφο εάν και μόνον εάν είναι ενεικονική,*

2. *δεξιό αντίστροφο εάν και μόνον εάν είναι επεικονική,*

Απόδειξη. 1. Υποθέτουμε οτι η f έχει αριστερό αντίστροφο g. Για να αποδείξουμε οτι η f είναι ενεικονική, υποθέτουμε οτι $f(x) = f(y)$. Τότε $x = g(f(x)) = g(f(y)) = y$, άρα η f είναι πράγματι ενεικόνιση.

Αντίστροφα, υποθέτουμε οτι η f είναι ενεικονική. Εάν $y \in B$ και $y = f(x)$, ορίζουμε $g(y) = x$. Εφόσον η f είναι ενεικονική, αυτό το x είναι μοναδικό. Εάν το y δεν ανήκει στην εικόνα της f, τότε δεν υπάρχει τέτοιο x· διαλέγουμε οποιοδήποτε $a \in A$ και ορίζουμε $g(y) = a$. Με αυτόν τον τρόπο το $g(y)$ ορίζεται για κάθε $y \in B$ και $g : B \to A$ είναι συνάρτηση. Αλλά, από τον ορισμό, $g(f(x)) = x$, άρα η g είναι αριστερό αντίστροφο.

2. Υποθέτουμε οτι η f έχει δεξιό αντίστροφο g. Εάν $y \in B$ τότε $y = f(g(y))$, άρα το y είναι της μορφής $f(x)$, για $x = g(y)$. Συνεπώς η f είναι επεικόνιση.

Αντίστροφα, υποθέτουμε οτι η f είναι επεικονική, και θεωρούμε $y \in B$. Τότε $y = f(x)$ για κάποιο $x \in A$, ίσως όχι μοναδικό. Για κάθε $y \in B$ ορίζουμε $g(y)$ να είναι κάποιο στοιχείο του A τέτοιο ώστε $f(g(y)) = y$. Τότε g είναι συνάρτηση και είναι δεξιό αντίστροφο της f. $\square$

Παράδειγμα 3.5 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Δεν είναι ούτε ενεικονική ούτε επεικονική, άρα δεν έχει αντίστροφο κανενός είδους. Μπορούμε να κάνουμε την f επεικονική εάν θεωρήσουμε ως πεδίο τιμών το $\mathbb{R}^+ = \{x \in \mathbb{R} \,|\, x \geq 0\}$. Τώρα η f έχει δεξιό αντίστροφο $g(x) = \sqrt{x}$ (τη θετική τετραγωνική ρίζα). Η g δεν είναι όμως αριστερό αντίστροφο αφού

$$\sqrt{x^2} = x \text{ εάν } x \geq 0 \text{ και } \sqrt{x^2} = -x > 0 \text{ εάν } x < 0\,.$$

Παράδειγμα 3.6 Θεωρούμε την απεικόνιση $f : \mathbb{C} \to \mathbb{R}$ που ορίζεται με $f(z) = \frac{1}{2}(z + \bar{z})$. Αυτή δεν είναι αμφιμονοσήμαντη, αλλά είναι επεικονική. Η συνάρτηση $g : \mathbb{R} \to \mathbb{C}$ που ορίζεται με $g(x) = x + \mathrm{i}0 \in \mathbb{C}$ είναι δεξιό αντίστροφο: $f \circ g(x) = \frac{1}{2}(x + x) = x$.

Πρόταση 3.5 *Εάν μια συνάρτηση έχει αριστερό και δεξιό αντίστροφο, τότε έχει αντίστροφη συνάρτηση, και κάθε δεξιό ή αριστερό αντίστροφο είναι ίσο με αυτήν.*

Απόδειξη. Εάν η $f : A \to B$ έχει αριστερό και δεξιό αντίστροφο, τότε η f είναι αμφιμονοσήμαντη, και έχει αντίστροφη συνάρτηση f^{-1}. Εάν g είναι ένα αριστερό αντίστροφο, τότε

$$g = g \circ i_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = i_A \circ f^{-1} = f^{-1}\,.$$

Παρόμοια, εάν h είναι ένα δεξιό αντίστροφο τότε $h = f^{-1}$.

$\square$

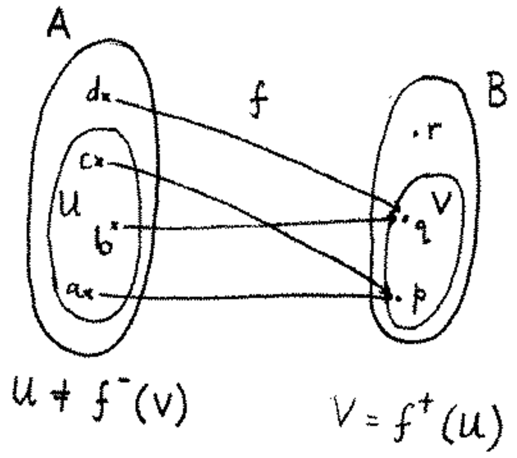
Εικόνα και αντίστροφη εικόνα υποσυνόλων

Εάν $f : A \to B$ είναι συνάρτηση,

1. Για κάθε υποσύνολο $U \subseteq A$, ορίζουμε την **εικόνα** του U μέσω της f ως το υποσύνολο του B που αποτελείται ακριβώς από τα στοιχεία στα οποία απεικονίζονται τα στοιχεία του U. Την εικόνα του U μέσω της f θα συμβολίζομε, προσωρινά, με $f^+(U)$:
$$U \subseteq A, \quad f^+(U) = \{f(x) \,|\, x \in U\} \subseteq B.$$
2. Για κάθε υποσύνολο $Y \subseteq B$, ορίζουμε την **αντίστροφη εικόνα** του Y μέσω της f ως το υποσύνολο του A που αποτελείται από όλα τα στοιχεία του A τα οποία απεικονίζονται σε στοιχεία του Y. Την αντίστροφη εικόνα του Y μέσω της f θα συμβολίζομε, προσωρινά, με $f^-(Y)$:
$$Y \subseteq B, \quad f^-(Y) = \{x \in A \,|\, f(x) \in Y\}.$$

Η εικόνα και η αντίστροφη εικόνα ορίζονται για κάθε συνάρτηση και για κάθε υποσύνολο του πεδίου ορισμού ή του πεδίου τιμών, αντίστοιχα. Ειδικότερα, προσέξτε οτι η αντίστροφη εικόνα ορίζεται ανεξάρτητα από το εάν η f έχει αντίστροφη συνάρτηση.

Παράδειγμα 3.7 Θεωρούμε τα σύνολα $A = \{a, b, c, d\}$ και $B = \{p, q, r\}$ και τη συνάρτηση $f : A \to B$ που δίδεται στο Σχήμα 3.14, καθώς και τα υποσύνολα $U = \{a, b, c\} \subseteq A$ και $V = \{p, q\} \subseteq B$.



Σχήμα 3.14: Εικόνες και αντίστροφες εικόνες.

Παρατηρήστε οτι ισχύουν οι ακόλουθες ισότητες.

$$\begin{aligned} f^+(\{a\}) &= \{p\} = f^+(\{c\}) \\ f^+(\{b\}) &= \{q\} \\ f^+(\{a, b\}) &= \{p, q\} = f^+(\{b, c\}) \end{aligned}$$

$$\begin{aligned} f^-(\{p\}) &= \{a, c\} \\ f^-(\{q\}) &= \{b, d\} \\ f^-(\{r\}) &= \varnothing \\ f^+(U) &= \{p, q\} = V \\ f^-(V) &= A \neq U. \end{aligned}$$

Ειδικότερα προσέξτε οτι $f^+(U \cap \{d\}) \neq f^+(U) \cap f^+(\{d\})$.

Μπορούμε να θεωρήσουμε την f^+ και την f^- ως συναρτήσεις στα σύνολα των υποσυνόλων του A και του B αντίστοιχα:

$$f^+ : \mathfrak{P}(A) \to \mathfrak{P}(B)$$

$$f^- : \mathfrak{P}(B) \to \mathfrak{P}(A)$$

Προσέξτε οτι, παρά την ονομασία της, η f^- δεν είναι εν γένει η αντίστροφη συνάρτηση της $f^+ : \mathfrak{P}(A) \to \mathfrak{P}(B)$, όπως φαίνεται από το παράδειγμα 3.7:

$$f^+(\{a\}) = \{p\} \text{ αλλά } f^-(\{p\}) = \{a, c\}.$$

Πρόταση 3.6 *Εάν $f : A \to B$ είναι συνάρτηση, οι συναρτήσεις $f^+ : \mathfrak{P}(A) \to \mathfrak{P}(B)$ και $f^- : \mathfrak{P}(B) \to \mathfrak{P}(A)$ έχουν τις ακόλουθες ιδιότητες: Εάν $U, V \subseteq A$ και $X, Y \subseteq B$,*

1. $f^+(\varnothing) = \varnothing, \quad f^-(\varnothing) = \varnothing, \quad f^-(B) = A$
2. $f^+(U \cup V) = f^+(U) \cup f^+(V)$
3. $f^+(U \cap V) \subseteq f^+(U) \cap f^+(V)$
4. $f^-(X \cup Y) = f^-(X) \cup f^-(Y)$
5. $f^-(X \cap Y) = f^-(X) \cap f^-(Y)$
6. $f^-(B \setminus Y) = A \setminus f^-(Y)$.

Απόδειξη. Θα αποδείξουμε την 2. Εάν $y \in f^+(U \cup V)$, τότε υπάρχει $x \in U \cup V$ τέτοιο ώστε $y = f(x)$. Εάν $x \in U$, τότε $y \in f^+(U)$, ενώ εάν $x \in V$, τότε $y \in f^+(V)$. Σε κάθε περίπτωση $y \in f^+(U) \cup f^+(V)$. Αντίστροφα, εάν $y \in f^+(U) \cup f^+(V)$, τότε υπάρχει $x \in U$ τέτοιο ώστε $y = f(x)$, είτε υπάρχει $x \in V$ τέτοιο ώστε $y = f(x)$. Σε κάθε περίπτωση, $y \in f^+(U \cup V)$.

Από το παράδειγμα 3.7 βλέπουμε οτι στο 3 δεν ισχύει εν γένει η ισότητα. Αφήνουμε την απόδειξη των άλλων ιδιοτήτων ως άσκηση.

□

Εδώ χρησιμοποιήσαμε το συμβολισμό $f^+(U)$ και $f^-(Y)$ για ευκρίνεια, αλλά ο συμβολισμός που χρησιμοποιούν οι μαθηματικοί είναι

$$f(U) \text{ για την εικόνα του } U \subseteq A \text{ μέσω της } f,$$

και

$$f^{-1}(V) \text{ για την αντίστροφη εικόνα του } V \subseteq B \text{ μέσω της } f$$

Συνήθως το νόημα του συμβολισμού f ή f^{-1} είναι σαφές από τα συμφραζόμενα, και δεν υπάρχει κίνδυνος σύγχυσης μεταξύ της συνάρτησης f και των συναρτήσεων 'εικόνα μέσω της f', 'αντίστροφη εικόνα μέσω της f'. Ιδιαίτερη προσοχή χρειάζεται όταν το V είναι μονοσύνολο. Πολύ συχνά οι μαθηματικοί αντί για $f^{-1}(\{p\})$ γράφουν $f^{-1}(p)$ εννοώντας την αντίστροφη εικόνα του μονοσυνόλου $\{p\}$. Όταν συναντάτε αυτό το συμβολισμό δεν πρέπει να θεωρήσετε οτι η f είναι αντιστρέψιμη συνάρτηση εκτός εάν αυτό γίνεται σαφές από τα συμφραζόμενα.

Άσκηση 3.10 Εάν $f: A \to B$ είναι συνάρτηση, και $U, V \subseteq A$, $X, Y \subseteq B$, δείξτε οτι

α′. $f(\varnothing) = \varnothing, \quad f^{-1}(\varnothing) = \varnothing, \quad f^{-1}(B) = A$

β′. $f(U \cap V) \subseteq f(U) \cap f(V)$

γ′. Εάν f είναι ενεικόνιση, τότε $f(U \cap V) = f(U) \cap f(V)$

δ′. $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$

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

ϛ′. $f^{-1}(B \setminus X) = A \setminus f^{-1}(X)$

Περιορισμός

Εάν $f: A \to B$ είναι συνάρτηση και X είναι υποσύνολο του A, ορίζουμε τη συνάρτηση

$$f|_X : X \to B$$

που ονομάζεται **περιορισμός** της f στο X, με

$$f|_X(x) = f(x) \qquad (x \in X).$$

Αυτή διαφέρει από την f μόνον εις το οτι αγνοούμε τα x που δεν ανήκουν στο X. Παρατηρούμε οτι η εικόνα $f(X)$ του συνόλου X είναι η εικόνα της περιορισμένης συνάρτησης, $\operatorname{im}(f|_X)$.

Ο περιορισμός είναι μια μάλλον τετριμμένη πράξη στις συναρτήσεις. Είναι χρήσιμη κυρίως για να εστιάσουμε την προσοχή μας στη συμπεριφορά της f στο υποσύνολο X. Μερικές φορές αυτό είναι χρήσιμο: στο παράδειγμα 3.4 παρατηρήσαμε οτι η $\sin: \mathbb{R} \to I$, όπου $I = \{x \in \mathbb{R} | -1 \leq x \leq 1\}$, δεν είναι αμφιμονοσήμαντη. Εάν $X = \{x \in \mathbb{R} | -\pi/2 \leq x \leq \pi/2\}$, ο περιορισμός $\sin|_X : X \to I$ είναι αμφιμονοσήμαντη συνάρτηση.

Ο περιορισμός της ταυτοτικής απεικόνισης $i_A : A \to A$ σε ένα υποσύνολο $X \subseteq A$ δίδει την **εμφύτευση**

$$i_A|_X : X \to A$$

για την οποία $i_A|_X(x) = x$ για κάθε $x \in X$. Αυτή είναι η ίδια συνάρτηση με την i_X αλλά με ευρύτερο πεδίο τιμών.

Ακολουθίες και n-άδες

Μπορούμε να χρησιμοποιήσουμε τις συναρτήσεις για να διευκρινίσουμε ορισμένες έννοιες. Εχουμε ορίσει διατεταγμένα ζεύγη, διατεταγμένες τριάδες, κλπ. αλλά δεν έχουμε ένα γενικό ορισμό.

Θεωρούμε το σύνολο $X_n = \{1, 2, 3, \ldots, n\} = \{x \in \mathbb{N} | 1 \leq x \leq n\}$. Εάν S είναι ένα σύνολο, μια **διατεταγμένη n-άδα** στοιχείων του S, ή **πεπερασμένη ακολουθία** στο S, μπορεί να οριστεί ως μία συνάρτηση

$$f : X_n \to S\,.$$

Με αυτόν τον τρόπο προσδιορίζουμε τα στοιχεία $f(1), f(2), f(3), \ldots, f(n)$ του S. Αν αλλάξουμε το συμβολισμό σε $(f_1, f_2, \ldots, f_n)$ βλέπουμε οτι δύο διατεταγμένες n-άδες $(f_1, f_2, \ldots, f_n)$ και $(g_1, g_2, \ldots, g_n)$ είναι ίσες εάν και μόνον εάν $f_1 = g_1$, $f_2 = g_2$, $\ldots$, $f_n = g_n$. Αυτό είναι που θέλουμε να ισχύει για διατεταγμένες n-άδες.

Παρόμοια, μια **ακολουθία** $a_1, a_2, \ldots$ στο S μπορεί να οριστεί ως μια συνάρτηση

$$f : \mathbb{N} \to S$$

όπου θέτουμε $f(n) = a_n$.

Στην περίπτωση των διατεταγμένων ζευγών, αυτός ο ορισμός τυπικά δίδει διαφορετικά αντικείμενα από τον ορισμό του Kuratowski, αλλά έχει πάλι την ιδιότητα οτι $(f_1, f_2) = (g_1, g_2)$ εάν και μόνον εάν $f_1 = g_1$ και $f_2 = g_2$, που είναι αυτό που ζητάμε.

Συναρτήσεις πολλών μεταβλητών

Στον Απειροστικό Λογισμό συναντάμε ‘συναρτήσεις δύο μεταβλητών’ όπως

$$f(x, y) = x^2 - 3y^3 + \cos xy \qquad (x, y \in \mathbb{R})\,.$$

Είναι πολύ εύκολο τώρα να ορίσουμε αυστηρά αυτές τις έννοιες. Η παραπάνω f είναι μια συνάρτηση που ορίζεται στο σύνολο των διατεταγμένων ζευγών (x, y), δηλαδή

$$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}\,.$$

Γενικότερα, εάν A και B είναι σύνολα, μια συνάρτηση δύο μεταβλητών $a \in A$ και $b \in B$ είναι μια συνάρτηση που ορίζεται στο $A \times B$ ή σε ένα υποσύνολό του. Παρόμοια, συναρτήσεις n μεταβλητών είναι απλώς συναρτήσεις που ορίζονται σε ένα σύνολο διατεταγμένων n-άδων.

Διμελείς πράξεις

Μια **διμελής πράξη** σε ένα σύνολο A είναι απλά μια συνάρτηση $f : A \times A \to A$. Εχουμε πολλά παραδείγματα τέτοιων αντικειμένων.

Παράδειγμα 3.8

1. Πρόσθεση στο $\mathbb{N}$, $\alpha : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\alpha(x, y) = x + y$.

2. Πολλαπλασιασμός στο $\mathbb{N}$, $\mu : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\mu(x, y) = xy$.

3. Αφαίρεση στο $\mathbb{Z}$, $\sigma : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\sigma(x, y) = x - y$.

4. Στο δυναμοσύνολο $\mathfrak{P}(X)$ ενός συνόλου X ορίζουμε τη διμελή πράξη 'ένωση', $u : \mathfrak{P}(X) \times \mathfrak{P}(X) \to \mathfrak{P}(X)$, $u(Y_1, Y_2) = Y_1 \cup Y_2$.

5. Εάν X είναι ένα σύνολο, θεωρούμε το σύνολο M όλων των συναρτήσεων από το X στο X, έτσι ώστε $f \in M$ σημαίνει $f : X \to X$. Ορίζουμε τη διμελή πράξη της σύνθεσης συναρτήσεων, $c : M \times M \to M$, $c(g, f) = g \circ f$.

Για τις περισσότερες διμελείς πράξεις που χρησιμοποιούνται στα μαθηματικά έχει καθιερωθεί ένας συμβολισμός της μορφής $x \circ y$ για το $f(x, y)$. Γι' αυτό συνήθως συμβολίζουμε μια διμελή πράξη $\circ : A \times A \to A$ και την εικόνα $\circ(x, y)$ με $x \circ y$. Συχνά ονομάζουμε το $x \circ y$ *γινόμενο* ή *σύνθεση* των x και y. Σε μερικές περιπτώσεις το ενδιάμεσο σύμβολο καταργείται, όπως στον πολλαπλασιασμό xy, ή στη σύνθεση συναρτήσεων, που συχνά γράφουμε gf αντί για $g \circ f$.

Σε μια γενική διμελή πράξη δεν περιμένουμε να ισχύει $x \circ y = y \circ x$. Για παράδειγμα, η αφαίρεση: $2 - 1 \neq 1 - 2$.

Εάν $x \circ y = y \circ x$ για κάθε x, $y \in A$, λέμε οτι η διμελής πράξη είναι **μεταθετική**. Στα παραδείγματα 1, 2 και 4 οι διμελείς πράξεις είναι μεταθετικές. Στο παράδειγμα 5 δεν είναι μεταθετική εάν το X έχει περισσότερα από ένα στοιχεία.

Εάν δεν γνωρίζουμε οτι η πράξη είναι μεταθετική, είναι σημαντικό να διατηρούμε τη διάταξη των όρων στο γινόμενο. Μπορούμε να επεκτείνουμε τέτοια γινόμενα σε τρείς ή περισσότερους όρους. Εάν x, y, $z \in A$ το γινόμενο $x \circ y \in A$ και μπορούμε να πάρουμε το γινόμενο αυτού με το z. Σε αυτό το σημείο πρέπει να εισαγάγουμε παρενθέσεις, ώστε να διακρίνουμε το $(x \circ y) \circ z$ από το $x \circ (y \circ z)$. Παρ' όλον οτι στις δύο εκφράσεις οι όροι εμφανίζονται με την ίδια διάταξη, η δεύτερη είναι το αποτέλεσμα της πράξης μεταξύ του x και του $y \circ z$ και μπορεί ενδεχομένως να είναι διαφορετικό από το πρώτο. Για παράδειγμα $(3 - 2) - 1 \neq 3 - (2 - 1)$.

Εάν $(x \circ y) \circ z = x \circ (y \circ z)$ για όλα τα x, y, $z \in A$, ονομάζουμε την πράξη $\circ$ **προσεταιριστική**. Στα παραδείγματα 1, 2, 4, 5 οι πράξεις είναι προσεταιριστικές, ενώ στο 3 δεν είναι. Στην περίπτωση προσεταιριστικής πράξης συχνά γράφουμε $x \circ y \circ z$, χωρίς παρενθέσεις.

Στην ανάπτυξη της έννοιας των αριθμών, οι μεταθετικές και προσεταιριστικές πράξεις (η πρόσθεση και ο πολλαπλασιασμός) αποτελούν σημαντικά εργαλεία. Σε κλάδους των σύγχρονων Μαθηματικών εμφανίζονται σημαντικά παραδείγματα μη μεταθετικών ή μη προσεταιριστικών πράξεων.

Οικογένειες συνόλων

Στο τέλος του Κεφαλαίου 1 αναφερθήκαμε σε σύνολα των οποίων τα στοιχεία είναι σύνολα, όπως

$$S = \{S_1, S_2, \ldots, S_n\}$$

όπου κάθε S_r είναι ένα σύνολο. Χρησιμοποιώντας την έννοια της συνάρτησης μπορούμε να επεκτείνουμε αυτόν το συμβολισμό. Εάν $X_n = \{1, 2, \ldots, n\}$, έχουμε αμφιμονοσήμαντη συνάρτηση $f : X_n \to S$ όπου $f(r) = S_r$. Δεν υπάρχει λόγος να περιοριστούμε σε πεπερασμένα σύνολα, ούτε να υποθέσουμε οτι όλα τα S_r είναι διαφορετικά. Εάν A είναι οποιοδήποτε σύνολο και $f : A \to S$ είναι συνάρτηση, $f(a) = S_a$, όπου κάθε στοιχείο του S είναι ένα σύνολο, λέμε οτι έχουμε μια **οικογένεια συνόλων**,

$$S = \{S_\alpha |\, \alpha \in A\}\,.$$

Σε αυτήν την περίπτωση το A ονομάζεται **σύνολο δεικτών**.

Η ένωση μιας τέτοιας οικογένειας,

$$\bigcup S = \{x|\, x \in S_\alpha \text{ για κάποιο } \alpha \in A\}$$

συμβολίζεται επίσης

$$\bigcup_{\alpha \in A} S_\alpha$$

ενώ, εάν $A \neq \varnothing$, η τομή

$$\bigcap S = \{x|\, x \in S_\alpha \text{ για κάποιο } \alpha \in A\}$$

συμβολίζεται ανάλογα

$$\bigcap_{\alpha \in A} S_\alpha\,.$$

Οταν $A = X_n$, χρησιμοποιούμε και το συμβολισμό $\bigcup_{r=1}^{n} S_r$ και $\bigcap_{r=1}^{n} S_r$, ενώ όταν $A = \mathbb{N}$ χρησιμοποιείται ο συμβολισμός $\bigcup_{r=1}^{\infty} S_r$ και $\bigcap_{r=1}^{\infty} S_r$. Δεν υπάρχει λόγος να σας ανησυχήσει το '∞' σε αυτούς τους συμβολισμούς, που είναι κατάλοιπο της ιστορικής εξέλιξης των Μαθηματικών. Ο σύγχρονος συμβολισμός το αποφεύγει και χρησιμοποιεί $\bigcup_{r \in \mathbb{N}} S_r$ και $\bigcap_{r \in \mathbb{N}} S_r$.

Ασκήσεις

Άσκηση 3.11 Προσδιορίστε την εικόνα για τις ακόλουθες συναρτήσεις $f : \mathbb{R} \to \mathbb{R}$.

α′. $f(x) = x^2 + 2x + 2$

β′. $f(x) = |x|$

γ′. $f(x) = x^2 + x - |x|^2$

Άσκηση 3.12 Για κάθε μία από τις συναρτήσεις της Άσκησης 3.11, βρείτε εάν είναι

α′. ενεικονική

β′. επεικονική επί του $\mathbb{R}$

γ′. αμφιμονοσήμαντη.

Άσκηση 3.13 Οι παρακάτω συναρτήσεις έχουν πεδίο τιμών το $\mathbb{R}$, και πεδίο ορισμού κάποιο υποσύνολο του $\mathbb{R}$. Βρείτε σε κάθε περίπτωση πιο είναι το μεγαλύτερο δυνατό πεδίο ορισμού.

α′. $V(t) = \log(1 - t^2)$

β′. $y = \log(\sin^2 x)$

γ′. $\rho = \sqrt{(u-1)(u-2)(u-3)(u-4)}$.

Άσκηση 3.14 Εάν $A = \{1, 2\}$ και $B = \{a, b, c, \}$, πόσες διαφορετικές συναρτήσεις υπάρχουν από το A στο B; Πόσες από το B στο A; Πόσες σε κάθε περίπτωση είναι ενεικονικές; πόσες είναι επεικονικές; πόσες είναι αμφιμονοσήμαντες;

Άσκηση 3.15 Πρόβλημα για γερούς λύτες.
Εάν $A = \varnothing$ και $B \neq \varnothing$, δείξτε οτι υπάρχει ακριβώς μια συνάρτηση από το A στο B, και καμία συνάρτηση από το B στο A. Υπάρχει συνάρτηση από το $\varnothing$ στο $\varnothing$;

Άσκηση 3.16 Για τις ακόλουθες συναρτήσεις ελέγξτε εάν υπάρχει δεξιό αντίστροφο ή/και αριστερό αντίστροφο, και εάν υπάρχει βρείτε το.

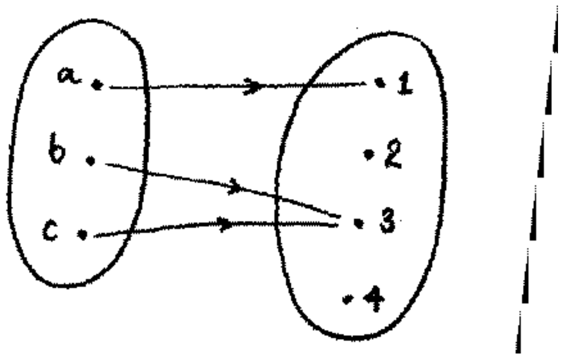
α′. $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = 4x + 2$

β′. $g : \mathbb{R} \to \mathbb{R}^+, \quad g(x) = x^2$.

Άσκηση 3.17 Για τις συναρτήσεις f και g της άσκησης 3.16, βρείτε τα σύνολα $f([-1, 1])$, $f^{-1}([0, 2])$, $g([-3, -2])$ και $g^{-1}([2, 4])$.

Άσκηση 3.18 Δίδεται η συνάρτηση $f : \{a, b, c\} \to \{1, 2, 3, 4\}$ όπως στο Σχήμα 3.15. (Υπενθυμίζεται οτι $f^{-1}(U)$ μπορεί να συμβολίζει την αντίστροφη εικόνα που συμβολίσαμε $f^{-}(U)$, ενώ, εάν η f δεν είναι αμφιμονοσήμαντη, $f^{-1}(x)$ μπορεί να συμβολίζει την αντίστροφη εικόνα του $\{x\}$.)

Βρείτε τα σύνολα



Σχήμα 3.15: Άσκηση 3.18

α΄. $f(\{a,\, b\})$

β΄. $f(\{b,\, c\})$

γ΄. $f^{-1}(\{1\})$

δ΄. $f^{-1}(\{2\})$

ε΄. $f^{-1}(3)$

ϛ΄. $f^{-1}(\{1,\, 2\})$

Άσκηση 3.19 Βρείτε το μεγαλύτερο υποσύνολο του $\mathbb{R} \times \mathbb{R}$ στο οποίο ορίζεται η συνάρτηση δύο μεταβλητών

$$f(x,\, y) = \frac{x^2 + 3xy}{(x-1)y}\,.$$

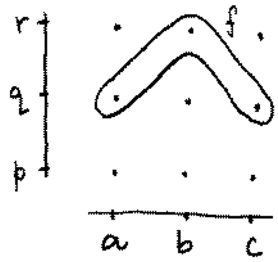
Άσκηση 3.20 Βρείτε την ένωση και την τομή των παρακάτω οικογενειών συνόλων με σύνολο δεικτών A.

α΄. $A = \{1,\, 2,\, 3,\, \ldots\, ,\, n\} \qquad S_\alpha = [0,\, \alpha + 1]$.

β΄. $A = \mathbb{N} \qquad S_n = (0,\, \frac{1}{n}) = \{x \in \mathbb{R} \,|\, 0 < x < \frac{1}{n}\}$.

Άσκηση 3.21 Δίδονται τα σύνολα $A = \{a,\, b,\, c\}$ και $B = \{p,\, q,\, r\}$, και η συνάρτηση $f\,:\, A \to B$ που ορίζεται στο Σχήμα 3.16.

α΄. Αλλάξτε το πεδίο τιμών της f, έτσι ώστε να μπορείτε να βρείτε δεξιό αντίστροφο της f. Βρείτε δύο διαφορετικά δεξιά αντίστροφα της f.



Σχήμα 3.16: Άσκηση 3.21

β'. Βρείτε δύο διαφορετικά σύνολα A_1 και A_2 τέτοια ώστε $A_1 \cup A_2 = A$ και $f|_{A_i}$ να είναι ένα προς ένα. Βρείτε σε κάθε περίπτωση το αριστερό αντίστροφο της $f|_{A_i}$.

γ'. Είναι το αριστερό αντίστροφο που βρήκατε αντίστροφη συνάρτηση της $f|_{A_i} : A_i \to B$;

Άσκηση 3.22 Δίδεται η συνάρτηση $f : \mathbb{R} \to \mathbb{R}$ που ορίζεται $f(x) = (x+1)^2$.

α'. Σχεδιάστε το γράφημα της f.

β'. Προσδιορίστε τα σύνολα $B = f(\mathbb{R})$, $f^{-1}([-1,\, 4])$, $f^{-1}(-2)$, $f^{-1}([-2,\, 0))$.

γ'. Βρείτε δύο διαφορετικά δεξιά αντίστροφα της $f : \mathbb{R} \to B$.

δ'. Βρείτε δύο υποσύνολα του $\mathbb{R}$, A_1 και A_2, τέτοια ώστε $A_1 \cup A_2 = \mathbb{R}$ και $f|_{A_i}$ για $i = 1,\, 2$, να είναι ένα προς ένα. Βρείτε σε κάθε περίπτωση ένα αριστερό αντίστροφο της $f|_{A_i} : A_i \to \mathbb{R}$.

Άσκηση 3.23 Ορίζουμε τις διμελείς πράξεις στο $\mathbb{Z}$:

α'. $x \circ y = x - y$

β'. $x \circ y = |x - y|$

γ'. $x \circ y = x + y + xy$

δ'. $x \circ y = \frac{1}{2}(x + y + \frac{1}{2}((-1)^{x+y} + 1) + 1)$.

Επαληθεύστε οτι είναι διμελείς πράξεις στο $\mathbb{Z}$, δηλαδή συναρτήσεις $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. Σε κάθε περίπτωση ελέγξτε εάν η πράξη είναι μεταθετική και προσεταιριστική.

Άσκηση 3.24 Μία ακολουθία συνόλων $(A_n)_{n \in \mathbb{N}_0}$ λέγεται φθίνουσα αν για κάθε $n \in \mathbb{N}_0$ ισχύει

$$A_{n+1} \subseteq A_n \,.$$

α΄. Αποδείξτε οτι αν $(A_n)_{n\in\mathbb{N}_0}$ είναι φθίνουσα, τότε για κάθε $k \in \mathbb{N}_0$:

$$\bigcap_{n=0}^{\infty} A_n = \bigcap_{n=k}^{\infty} A_n$$

β΄. Αποδείξτε οτι αν $(A_n)_{n\in\mathbb{N}_0}$, $(B_n)_{n\in\mathbb{N}_0}$ είναι φθίνουσες, τότε

$$\bigcap_{n=0}^{\infty}(A_n \cup B_n) = (\bigcap_{n=0}^{\infty} A_n) \cup (\bigcap_{n=0}^{\infty} B_n)$$

Άσκηση 3.25 Έστω $f : X \longrightarrow Y$. Έστω $(A_t)_{t\in T}$ οικογένεια υποσυνόλων του X. Αποδείξτε οτι:

α΄.

$$f\left(\bigcup_{t\in T} A_t\right) = \bigcup_{t\in T} f(A_t),$$

β΄.

$$f\left(\bigcap_{t\in T} A_t\right) \subseteq \bigcap_{t\in T} f(A_t),$$

γ΄. Αν η f είναι ενεικονική, τότε

$$f\left(\bigcap_{t\in T} A_t\right) = \bigcap_{t\in T} f(A_t)$$

Κεφάλαιο 4

Μαθηματική Λογική

Η βασική ιδιότητα των Μαθηματικών, που τα διακρίνει από άλλες μορφές γνώσης και ενοποιεί όλα τα μαθηματικά αποτελέσματα, είναι η χρήση μαθηματικών αποδείξεων για να συμπεράνουμε νέα αποτελέσματα από άλλα ήδη γνωστά. Ορισμένες τεχνικές μαθηματικής απόδειξης φαίνονται κάπως παράξενες. Ισως η πιό ενδιαφέρουσα από αυτές είναι η 'εις άτοπον απαγωγή': για να δείξουμε οτι κάτι είναι αληθές, υποθέτουμε οτι είναι ψευδές και αποδεικνύουμε οτι αυτή η υπόθεση οδηγεί σε αντίφαση. Ιδού ένα απλό παράδειγμα:

Πρόταση 4.1 *Το μικρότερο άνω φράγμα του συνόλου* $S = \{x \in \mathbb{R} | \, x < 1\}$ *είναι ο αριθμός* 1.

Απόδειξη. Ο 1 είναι σίγουρα άνω φράγμα του S. Υποθέτουμε οτι υπάρχει ένα άλλο άνω φράγμα K για το οποίο ισχύει $K < 1$. Από απλούς κανόνες της αριθμητικής συμπεραίνουμε οτι $K < \frac{1}{2}(K+1) < 1$. Αλλά τότε $\frac{1}{2}(K+1) \in S$ και $K < \frac{1}{2}(K+1)$ που αντιφάσκει με την υπόθεση οτι το K είναι άνω φράγμα του S. Αρα η υπόθεση οτι υπάρχει άνω φράγμα K με $K < 1$ είναι ψευδής. Συνεπώς κάθε άνω φράγμα του S είναι μεγαλύτερο από ή ίσο προς το 1.

□

Αυτή είναι μια χαρακτηριστική περίπτωση τέτοιου είδους επιχειρήματος. Αν P είναι η πρόταση 'Εάν K είναι άνω φράγμα του S τότε $K \geq 1$', μας ενδιαφέρει να αποδείξουμε οτι η P αληθεύει. Υποθέτουμε οτι η P είναι ψευδής, δηλαδή οτι υπάρχει άνω φράγμα K του S με $K < 1$, και, μετά από ένα απλό επιχείρημα, καταλήγουμε σε αντίφαση. Αν το επιχείρημα είναι σωστό, τότε η P δεν μπορεί να είναι ψευδής, άρα είναι αληθής.

Για να μπορούμε να χρησιμοποιήσουμε αυτήν τη μέθοδο, και να έχουμε εμπιστοσύνη στα αποτελέσματά της, πρέπει να εξασφαλίζουμε δύο προϋποθέσεις.

Πρώτα, η πρόταση P και όλες οι υπόλοιπες προτάσεις στο επιχείρημα, πρέπει να είναι σαφώς αληθείς ή σαφώς ψευδείς, ακόμη και αν κατά τη διάρκεια του επιχειρήματος δεν γνωρίζουμε ποιό από τα δύο ισχύει. Αυτό δεν συμβαίνει με πολλές προτάσεις της καθημερινής γλώσσας, που περιέχουν γενικότητες οι οποίες είναι αληθείς στις περισσότερες περιπτώσεις, αλλά ίσως όχι σε όλες. Στις μαθηματικές αποδείξεις δεν επιτρέπονται τέτοιες γενικότητες: κάθε πρόταση πρέπει να είναι σαφώς αληθής ή ψευδής.

Η δεύτερη προϋπόθεση σε μια απόδειξη με απαγωγή σε άτοπο είναι να μην περιέχονται κενά στα επιχειρήματα που χρησιμοποιούνται για να καταλήξουμε στην αντίφαση. Μόνο σε αυτήν την περίπτωση μπορούμε να είμαστε βέβαιοι οτι η αιτία της αντίφασης είναι η αρχική υπόθεση, οτι η P είναι ψευδής.

Προτάσεις

Οπως είδαμε, είναι απαραίτητο κάθε **πρόταση** που διατυπώνουμε στα Μαθηματικά να είναι σαφώς αληθής ή ψευδής. Για να διακρίνουμε μεταξύ αληθών και ψευδών προτάσεων, λέμε οτι κάθε πρόταση έχει μια *λογική τιμή* ή *τιμή αληθείας*, που τη συμβολίζουμε με τα γράμματα A = αληθές και Ψ = ψευδές. Συχνά χρησιμοποιούνται τα σύμβολα T ή $\mathbf{1}$ για 'αληθές' και F ή $\mathbf{0}$ για 'ψευδές'.

Εάν P είναι μια πρόταση, η φράση 'οχι P', (η άρνηση της P), είναι επίσης μια πρόταση, με την αντίθετη τιμή αληθείας από την P. Για παράδειγμα, εάν P είναι η ψευδής πρόταση '$2+2=5$', τότε 'όχι $2+2=5$' είναι μια αληθής πρόταση. Συμβολίζουμε τη φράση 'όχι P'

$$\neg P\,.$$

Οταν αντικαθιστούμε στη θέση του P μια συγκεκριμένη πρόταση, προσαρμόζουμε τον τρόπο που διαβάζουμε την πρόταση στους κανόνες του συντακτικού και της γραμματικής, αρκεί αυτό να μην αλλοιώνει το μαθηματικό νόημα. Στο προηγούμενο παράδειγμα, αντί 'όχι $2+2=5$' θα λέγαμε 'δεν ισχύει οτι $2+2=5$' ή '$2+2\neq 5$' ή '$2+2=5$ είναι ψευδής'.

Κατηγορήματα

Στο συντακτικό, 'κατηγόρημα' είναι το μέρος της πρότασης που 'φανερώνει εκείνο που λέγεται μέσα στην πρόταση για το υποκείμενο'. Στα μαθηματικά, **κατηγόρημα** ή **προτασιακός τύπος** είναι μια έκφραση που περιέχει ένα σύμβολο, για παράδειγμα το x, και η οποία είναι σαφώς αληθής ή σαφώς ψευδής πρόταση όταν αντικαταστήσουμε το x με στοιχείο ενός συνόλου S.

Παράδειγμα 4.1 Εάν $P(x)$ είναι το κατηγόρημα

'Ο πραγματικός αριθμός x είναι μεγαλύτερος από 2',

τότε $P(3)$ είναι αληθής πρόταση, ενώ $P(1)$ είναι ψευδής. Εάν βρούμε την τιμή αληθείας του $P(a)$ για κάθε $a\in\mathbb{R}$, έχουμε μια *συνάρτηση αληθείας* $T_P:\mathbb{R}\to\{\mathrm{A},\Psi\}$ για την οποία $T_P(a)=\mathrm{A}$ εάν $P(a)$ είναι αληθής, και $T_P(a)=\Psi$ εάν $P(a)$ είναι ψευδής.

Αυτή η έννοια ταιριάζει με τις ιδέες της θεωρίας συνόλων. Το κατηγόρημα $P(x)$ χωρίζει το σύνολο $\mathbb{R}$ σε δύο ξένα υποσύνολα, ένα όπου ανήκουν τα στοιχεία για τα οποία $P(x)$ είναι αληθής, και το άλλο όπου ανήκουν τα στοιχεία για τα οποία $P(x)$ είναι ψευδής. Το πρώτο το συμβολίζουμε $\{x\in\mathbb{R}|\,P(x)\}$. Στο παράδειγμα 4.1 αυτό γίνεται $\{x\in\mathbb{R}|\,x>2\}$. Το άλλο σύνολο το συμβολίζουμε $\{x\in\mathbb{R}|\,\neg P(x)\}$, που στο παράδειγμά μας είναι $\{x\in\mathbb{R}|\,x\leq 2\}$.

Γενικά, για κάθε κατηγόρημα $P(x)$ στο σύνολο S, έχουμε συνάρτηση αληθείας $T_P:\,S\to\{\mathrm{A},\,\Psi\}$ και

$$\begin{array}{ll} a\in\{x\in S|\,P(x)\} & \text{εάν και μόνον εάν } P(a) \text{ είναι αληθής,}\\ a\in\{x\in S|\,\neg P(x)\} & \text{εάν και μόνον εάν } P(a) \text{ είναι ψευδής.}\end{array}$$

Αντί να χρησιμοποιούμε ασαφείς εκφράσεις όπως 'κατηγόρημα είναι ένα είδος έκφρασης που …', θα μπορούσαμε να χρησιμοποιήσουμε την ιδέα της συνάρτησης αληθείας για να δώσουμε ένα συνολοθεωρητικό ορισμό του κατηγορήματος.

Εάν περισσότερες από μία μεταβλητές εμφανίζονται σε μια έκφραση, λέμε οτι έχουμε 'κατηγόρημα δύο μεταβλητών' ή 'τριών μεταβλητών' κ.ο.κ. Για παράδειγμα, η έκφραση '$x>$

y' είναι κατηγόρημα δύο μεταβλητών. Εάν το συμβολίσουμε $Q(x, y)$, τότε $Q(3, 2)$ είναι αληθές, ενώ $Q(15/2, 10+\sqrt{2})$ είναι ψευδές. Εδώ η συνάρτηση αληθείας είναι $T_Q : \mathbb{R}\times\mathbb{R} \to \{\mathrm{A}, \Psi\}$, όπου $T_Q(x, y) = \mathrm{A}$ εάν $Q(x, y)$ είναι αληθής και $T_Q(x, y) = \Psi$ εάν $Q(x, y)$ είναι ψευδής.

Στην πράξη, οι μαθηματικοί πολύ συχνά δεν αναφέρουν ρητά ποιό είναι το σύνολο στο οποίο ορίζεται ένα κατηγόρημα. Για παράδειγμα, θεωρείται προφανές οτι '$x > 3$' αναφέρεται σε πραγματικούς αριθμούς. Επίσης, κατά συνθήκη, ορισμένα γράμματα χρησιμοποιούνται για στοιχεία ενός συγκεκριμένου συνόλου. Για παράδειγμα το n χρησιμοποιείται συνήθως για να συμβολίσει ένα φυσικό αριθμό. Ετσι το κατηγόρημα $n > 3$ θα θεωρείτο οτι αναφέρεται μόνο σε φυσικούς αριθμούς.

Αυτή η πρακτική μπορεί να φαίνεται τσαπατσούλικη, όμως έχει μια καλή δικαιολογία. Οσο πιο αναλυτικά γράφουμε κάποια πράγματα στα μαθηματικά, τόσο πιο πολλά σύμβολα χρειαζόμαστε. Στο τέλος η σελίδα γεμίζει σύμβολα, και είναι δύσκολο να αντιληφθούμε το συνολικό νόημα, λόγω των υπερβολικών λεπτομερειών. Τότε πρέπει να επιλέξουμε το συμβολισμό που θα εκφράσει τις ιδέες με τη μεγαλύτερη δυνατή σαφήνεια αλλά και συντομία.

Ολα και κάποιο

Εάν έχουμε ένα κατηγόρημα $P(x)$ που ορίζεται σε κάποιο σύνολο S, μπορούμε να αναρωτηθούμε εάν αληθεύει για όλα τα στοιχεία του S, ή εάν αληθεύει τουλάχιστον για κάποιο στοιχείο του S. Μπορούμε να διατυπώσουμε την πρόταση 'για κάθε $x \in S$, ισχύει $P(x)$' ή την πρόταση 'υπάρχει κάποιο $x \in S$, για το οποίο ισχύει $P(x)$'. Αυτές οι προτάσεις μπορεί να είναι αληθείς ή ψευδείς. Τις γράφουμε με μαθηματικά σύμβολα, χρησιμοποιώντας τον **καθολικό ποσοδείκτη** $\forall$ και τον **υπαρξιακό ποσοδείκτη** $\exists$.

$\forall x \in S : P(x)$ διαβάζεται 'για κάθε $x \in S$, $P(x)$'.

$\exists x \in S : P(x)$ διαβάζεται 'υπάρχει (τουλάχιστον ένα) $x \in S$ τέτοιο ώστε $P(x)$'.

Εάν το κατηγόρημα $P(x)$ είναι αληθές για όλα τα $x \in S$, τότε η πρόταση '$\forall x \in S : P(x)$' είναι αληθής, αλλιώς είναι ψευδής. Εάν το κατηγόρημα $P(x)$ είναι αληθές για τουλάχιστον ένα $x \in S$, τότε η πρόταση '$\exists x \in S : P(x)$' είναι αληθής, αλλιώς είναι ψευδής. Οταν διαβάζουμε αυτά τα σύμβολα μπορούμε να χρησιμοποιήσουμε διαφορετικές εκφράσεις στα ελληνικά, που αποδίδουν το ίδιο νόημα: 'για κάθε $x \in S$, $P(x)$' ή 'για όλα τα $x \in S$, $P(x)$' και αντίστοιχα, 'υπάρχει $x \in S$ τέτοιο ώστε $P(x)$' ή 'για κάποιο $x \in S$, $P(x)$', κ.ο.κ.

Αξίζει να παρατηρήσουμε οτι η πρόταση 'για κάποιο $x \in S$, $P(x)$' στα μαθηματικά δεν υπονοεί οτι υπάρχει κάποιο άλλο $x \in S$ για το οποίο $P(x)$ είναι ψευδές. Στην καθημερινή γλώσσα, η φράση 'κάποιοι πολιτικοί είναι έντιμοι' μπορεί να υπονοεί οτι υπάρχουν και κάποιοι που δεν είναι. Στα μαθηματικά δεν υπάρχουν τέτοιες προεκτάσεις. Για παράδειγμα, η πρόταση

'κάποιος από τους αριθμούς 3677, 601, 19, 257, 11119, 12563 είναι πρώτος '

είναι αληθής, αφού εύκολα βλέπουμε οτι το 19 είναι πρώτος αριθμός. Το γεγονός οτι και όλοι οι άλλοι είναι πρώτοι δεν αλλάζει αυτό το συμπέρασμα. Ετσι, για να ελέγξουμε την αλήθεια της πρότασης $\exists x \in S : P(x)$ αρκεί να βρούμε μια τιμή του x για την οποία η $P(x)$ είναι αληθής.

Παράδειγμα 4.2 $\forall x \in \mathbb{R} : x^2 \geq 0$ σημαίνει 'για κάθε $x \in \mathbb{R}$, $x^2 \geq 0$' ή 'το τετράγωνο κάθε πραγματικού αριθμού είναι μη αρνητικό' ή κάποια άλλη ισοδύναμη διατύπωση. Η πρόταση είναι αληθής.

Παράδειγμα 4.3 $\exists x \in \mathbb{R} : x^2 \geq 0$ σημαίνει 'για κάποιο $x \in \mathbb{R}$, $x^2 \geq 0$' ή 'υπάρχει κάποιος πραγματικός αριθμός του οποίου το τετράγωνο είναι μη αρνητικό'. Και αυτή είναι αληθής.

Παράδειγμα 4.4 $\forall x \in \mathbb{R} : x^2 > 0$ είναι ψευδής, αφού $0^2 \not> 0$.

Παράδειγμα 4.5 $\exists x \in \mathbb{R} : x^2 > 0$ είναι αληθής, αφού $1^2 > 0$. Σε αυτήν την περίπτωση υπάρχουν πολλά άλλα στοιχεία του $\mathbb{R}$ εκτός από το 1 που επαληθεύουν το κατηγόρημα.

Παράδειγμα 4.6 $\exists x \in \mathbb{R} : x^2 < 0$ είναι ψευδής. Αντιθέτως, η πρόταση $\exists x \in \mathbb{R} : x^2 \leq 0$ είναι αληθής.

Εάν σε μία πρόταση με ποσοδείκτες αντικαταστήσουμε το σύμβολο της μεταβλητής x κάθε φορά που εμφανίζεται, με κάποιο άλλο σύμβολο, θεωρούμε οτι δεν αλλάζει η πρόταση.
$\exists x \in S : P(x)$ σημαίνει το ίδιο με $\exists y \in S : P(y)$.
$\forall x \in S : P(x)$ σημαίνει το ίδιο με $\forall y \in S : P(y)$.

Παράδειγμα 4.7 $\exists x \in \mathbb{R} : x^2 > 0$ είναι ισοδύναμο με το $\exists y \in \mathbb{R} : y^2 > 0$. Και οι δύο εκφράσεις λένε οτι ' υπάρχει ένας πραγματικός αριθμός του οποίου το τετράγωνο είναι θετικό'.

Περισσότεροι ποσοδείκτες

Εάν έχουμε ένα κατηγόρημα με δύο ή περισσότερες μεταβλητές, μπορούμε να χρησιμοποιήσουμε έναν ποσοδείκτη για κάθε μεταβλητή. Για παράδειγμα, εάν $P(x, y)$ είναι το κατηγόρημα '$x + y = 0$', τότε η πρόταση

$$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R} : P(x, y)$$

διαβάζεται 'για κάθε $x \in \mathbb{R}$ υπάρχει $y \in \mathbb{R}$ τέτοιο ώστε $x + y = 0$'.

Συνηθίζεται να γράφονται οι ποσοδείκτες στην αρχή της πρότασης στην οποία αναφέρονται, και να διαβάζονται στη σειρά. Για παράδειγμα, η πρόταση

$$\exists y \in \mathbb{R}\, \forall x \in \mathbb{R} : P(x, y)$$

θα διαβαζόταν 'υπάρχει $y \in \mathbb{R}$ τέτοιο ώστε για κάθε $x \in \mathbb{R}$, $x + y = 0$'.

Η διάταξη των ποσοδεικτών κάνει διαφορά. Από τις δύο προτάσεις που δώσαμε, η

$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R} : P(x, y)$$

είναι αληθής (για κάθε $x \in \mathbb{R}$ μπορούμε να πάρουμε $y = -x$ για να έχουμε $x + y = 0$), αλλά η

$$\exists y \in \mathbb{R}\, \forall x \in \mathbb{R} : P(x, y)$$

είναι ψευδής, γιατί υποστηρίζει οτι υπάρχει κάποιο $y \in \mathbb{R}$ που ικανοποιεί $x + y = 0$ για κάθε $x \in \mathbb{R}$, πράγμα που δεν μπορεί να επιτευχθεί από μια τιμή του y.

Η τοποθέτηση των ποσοδεικτών στη σωστή διάταξη σε μια πρόταση είναι ουσιώδης για τη σαφή μαθηματική σκέψη. Είναι ένα αρκετά κοινό λάθος, που κάνουν ακόμη και έμπειροι μαθηματικοί. Μια αιτία του προβλήματος εμφανίζεται όταν προσπαθούμε να γράψουμε μια, πιθανόν σαφώς διατυπωμένη, λογική πρόταση σε ομιλούμενη μαθηματική γλώσσα. Η διάταξη των λέξεων μπορεί να αλλάξει, για να γίνει πιό στρωτή η φράση, και αυτό να βλάψει τη σαφήνεια. Ειδικότερα, οι ποσοδείκτες μπορεί να τοποθετηθούν στο εσωτερικό της πρότασης αντί να βρίσκονται όλοι στην αρχή. (Το κάναμε αυτό πιο πάνω, όταν γράψαμε οτι '...υποστηρίζει οτι υπάρχει κάποιο $y \in \mathbb{R}$ που ικανοποιεί $x + y = 0$ για κάθε $x \in \mathbb{R}$'.)

Η πρόταση

'κάθε μη μηδενικός ρητός αριθμός έχει ρητό αντίστροφο'

σημαίνει οτι 'δοθέντος $x \in \mathbb{Q}$, με $x \neq 0$, υπάρχει στοιχείο $y \in \mathbb{Q}$ τέτοιο ώστε $x\,y = 1$'. Σε λογικό συμβολισμό η πρόταση είναι

$$(\forall x \in \mathbb{Q},\ x \neq 0)\ \exists y \in \mathbb{Q} :\ xy = 1\,.$$

Ένας μαθηματικός θα μπορούσε να αλλάζει τη σειρά της πρότασης και να πει 'υπάρχει ρητό αντίστροφο για κάθε μη μηδενικό ρητό αριθμό', αλλά αυτή η διατύπωση μπορεί να παρερμηνευτεί. Είναι σκόπιμο να προσπαθούμε να είναι όσο δυνατόν πιο σαφής η έννοια των μαθηματικών εκφράσεων που γράφουμε.

Το πρόβλημα αυτό υπάρχει μόνον όταν εμφανίζονται διαφορετικοί ποσοδείκτες σε μια πρόταση. Όταν όλοι οι ποσοδείκτες είναι ίδιου τύπου, δεν κάνει διαφορά η διάταξη με την οποία εμφανίζονται. Για παράδειγμα, εάν $P(x,\,y)$ είναι το κατηγόρημα '$(x + y)^2 = x^2 + 2xy + y^2$', τότε οι προτάσεις

$$\forall\, x \in \mathbb{R}\ \forall\, y \in \mathbb{R} : P(x,\,y)$$

και

$$\forall\, y \in \mathbb{R}\ \forall\, x \in \mathbb{R} : P(x,\,y)$$

σημαίνουν και οι δύο το ίδιο πράγμα

'για κάθε $x,\, y \in \mathbb{R}$, $(x + y)^2 = x^2 + 2xy + y^2$,'

το οποίο είναι βεβαίως μία αληθής πρόταση. Εάν οι μεταβλητές που εμφανίζονται προέρχονται από το ίδιο σύνολο, συνήθως απλοποιούμε τον συμβολισμό, γράφοντας

$$\forall\, x,\, y \in \mathbb{R} :\ P(x,\,y)\,.$$

Το ίδιο γίνεται με τον υπαρξιακό ποσοδείκτη. Για παράδειγμα, εάν $Q(x,\,y)$ είναι 'x, y είναι άρρητοι και $x + y$ είναι ρητός', τότε οι προτάσεις

$$\exists x \in (\mathbb{R} \setminus \mathbb{Q})\ \exists y \in (\mathbb{R} \setminus \mathbb{Q}) :\ Q(x,\,y)$$

και

$$\exists y \in (\mathbb{R} \setminus \mathbb{Q})\ \exists x \in (\mathbb{R} \setminus \mathbb{Q}) :\ Q(x,\,y)$$

σημαίνουν το ίδιο:

'υπάρχουν δύο άρρητοι αριθμοί x και y των οποίων το άθροισμα είναι ρητός'.

(Αυτή η πρόταση είναι αληθής, αφού οι αριθμοί $\sqrt{2}$ και $-\sqrt{2}$ είναι άρρητοι, αλλά $\sqrt{2} + (-\sqrt{2}) = 0$ είναι ρητός). Αυτό μπορούμε επίσης να το γράψουμε, για συντομία,

$$\exists\, x,\, y \in (\mathbb{R} \setminus \mathbb{Q}) :\ Q(x,\,y)\,.$$

Υπάρχει ακόμη μία μικρή παγίδα στα γραπτά μαθηματικά. Ο καθολικός ποσοδείκτης δεν αναφέρεται πάντοτε ρητά, συχνά εννοείται από τα συμφραζόμενα. Ας δούμε τον ορισμό της σύγκλισης μίας ακολουθίας: *Μία ακολουθία πραγματικών αριθμών συγκλίνει στο όριο ℓ εάν, για κάθε $\varepsilon > 0$, υπάρχει φυσικός αριθμός N τέτοιος ώστε $|a_n - \ell| < \varepsilon$ για κάθε $n > N$.* Στην προσπάθεια να συντομεύσουν τον ορισμό, πολλοί μαθηματικοί θα έγραφαν,

$$\textit{δοθέντος } \varepsilon > 0,\ \exists\, N \textit{ τέτοιο ώστε } n > N \textit{ συνεπάγεται } |a_n - \ell| < \varepsilon\,.$$

Θα συναντήσετε πολλές παραλλαγές αυτού του ορισμού, αλλά στην ουσία όλοι σημαίνουν το ίδιο πράγμα. Εάν το κατανοήσετε αυτό έχετε κάνει μεγάλη πρόοδο στην προσπάθεια να καταλάβετε το είδος των προβλημάτων που εμφανίζονται όταν θέλουμε να επικοινωνήσουμε μαθηματικά με τον κατάλληλο βαθμό ακριβείας.

Η άρνηση μιας πρότασης

Στη σελίδα 64 είδαμε την άρνηση $\neg P$ μιας πρότασης P. Η τιμή αληθείας της $\neg P$ μπορεί να παρασταθεί στον ακόλουθο πίνακα, ο οποίος ονομάζεται **πίνακας αληθείας**:

P	$\neg P$
Α	Ψ
Ψ	Α

Διαβάζοντας κατά μήκος των γραμμών, ο πίνακας λέει οτι όταν η P είναι αληθής , η $\neg P$ είναι ψευδής, και όταν η P είναι ψευδής, η $\neg P$ είναι αληθής. Με τον ίδιο τρόπο μπορούμε να εφαρμόσουμε την άρνηση σε ένα κατηγόρημα. Εάν $P(x)$ είναι το κατηγόρημα '$x > 5$', τότε $\neg P(x)$ διαβάζεται 'είναι ψευδές οτι $x > 5$', ή ισοδύναμα '$x \not> 5$'.

Η άρνηση μίας πρότασης που περιέχει ποσοδείκτες οδηγεί σε μία ενδιαφέρουσα κατάσταση. Εύκολα αντιλαμβανόμαστε οτι η πρόταση 'είναι ψευδές οτι $\forall x \in S : P(x)$', είναι το ίδιο με '$\exists\, x \in S : \neg P(x)$'. (Εάν είναι ψευδές οτι $P(x)$ αληθεύει για κάθε $x \in S$, τότε πρέπει να υπάρχει κάποιο $x \in S$ για το οποίο $P(x)$ είναι ψευδές, οπότε $\neg P(x)$ είναι αληθές). Αυτό γράφεται συμβολικά:

$$\neg\forall\, x\in S : P(x) \quad \text{σημαίνει το ίδιο με} \quad \exists\, x\in S : \neg P(x) \tag{4.1}$$

Παρόμοια

$$\neg\exists\, x\in S : P(x) \quad \text{σημαίνει το ίδιο με} \quad \forall\, x\in S : \neg P(x) \tag{4.2}$$

Η δεύτερη πρόταση λέει οτι η έκφραση 'δεν υπάρχει x για το οποίο $P(x)$ είναι αληθές' σημαίνει το ίδιο με 'για κάθε $x\in S$, $P(x)$ είναι ψευδές'.

Παράδειγμα 4.8

$$\neg\,\exists\, x\in\mathbb{R} : x^2 < 0 \quad \text{σημαίνει} \quad \textit{δεν υπάρχει } x\in\mathbb{R} \textit{ για το οποίο } x^2 < 0.$$

$$\forall\, x\in\mathbb{R} : \neg(x^2 < 0) \quad \text{σημαίνει} \quad \textit{για κάθε } x\in\mathbb{R} \textit{ ισχύει } x^2 \not< 0.$$

Αυτοί οι δύο απλοί κανόνες, οι οποίοι ονομάζονται **κανόνες του De Morgan** για ποσοδείκτες, έχουν μεγάλη σημασία στα μαθηματικά επιχειρήματα. Ο 4.1 σημαίνει οτι:

Για να δείξουμε οτι ένα κατηγόρημα $P(x)$ **δεν** *είναι αληθές για όλα τα $x \in S$, αρκεί να βρούμε ένα $x \in S$ για το οποίο $P(x)$ είναι ψευδές.*

Ο 4.2 λέει οτι

Για να δείξουμε οτι **δεν** *υπάρχει $x \in S$ για το οποίο αληθεύει το κατηγόρημα $P(x)$, είναι απαραίτητο να δείξουμε οτι $P(x)$ είναι ψευδές για κάθε $x \in S$.*

Άσκηση 4.1 Γράψτε την άρνηση της πρότασης

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}\ \forall y \in \mathbb{R} : [(|x-y| < \delta) \Rightarrow (|f(x) - f(y)| < \varepsilon)]$$

και διατυπώστε την σε στρωτά ελληνικά.

Ως απλοί κανόνες για την άρνηση προτάσεων που περιλαμβάνουν ποσοδείκτες, οι κανόνες του De Morgan είναι ιδιαίτερα χρήσιμοι όταν εμφανίζονται πολλοί ποσοδείκες σε μία πρόταση. Ένα χαρακτηριστικό παράδειγμα είναι ο ορισμός της σύγκλισης μίας ακολουθίας, σε λογικό συμβολισμό:

$$\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall n > N : (|a_n - \ell| < \varepsilon)\,.$$

Για να δείξουμε οτι η ακολουθία (a_n) δεν τείνει στο όριο ℓ, αποδεικνύουμε την άρνηση αυτής της πρότασης, δηλαδή

$$\neg\, [\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall n > N : (|a_n - \ell| < \varepsilon)]\ .$$

Εφαρμόζοντας του κανόνες 4.1 και 4.2 αυτή γίνεται, διαδοχικά,

$$\exists \varepsilon > 0\ \neg\, [\exists N \in \mathbb{N};, \forall n > N : (|a_n - \ell| < \varepsilon)]\ ,$$

κατόπιν

$$\exists \varepsilon > 0\ \forall N \in \mathbb{N} \neg\, [\forall n > N : (|a_n - \ell| < \varepsilon)]\ ,$$

και

$$\exists \varepsilon > 0\ \forall N \in \mathbb{N}\ \exists n > N : \neg(|a_n - \ell| < \varepsilon)\,,$$

το οποίο τελικά σημαίνει

$$\exists \varepsilon > 0\ \forall N \in \mathbb{N}\ \exists n > N : (|a_n - \ell| \not< \varepsilon)\,.$$

Για να επαληθεύσουμε οτι η ακολουθία (a_n) δεν συγκλίνει στο ℓ, πρέπει να δείξουμε αυτό το τελευταίο, δηλαδή οτι υπάρχει κάποιο συγκεκριμένο $\varepsilon > 0$ τέτοιο ώστε για κάθε φυσικό αριθμό N υπάρχει πάντα κάποιος μεγαλύτερος φυσικός αριθμός $n > N$ για τον οποίο ισχύει $|a_n - \ell| \not< \varepsilon$. Μεγάλο μέρος της δυσκολίας της μαθηματικής ανάλυσης οφείλεται στον χειρισμό τέτοιων προτάσεων. Με την πείρα και την εξάσκηση γίνεται πολύ πιο εύκολο, αλλά πάντα ανατρέχουμε στους κανόνες για την άρνηση ποσοδεικτών.

Λογικοί σύνδεσμοι

Στα Μαθηματικά χρησιμοποιούμε τους συνηθισμένους συνδέσμους όπως ‘ και’, ‘ή’, κλπ. με πολύ συγκεκριμένο νόημα. Για παράδειγμα, ο σύνδεσμος ‘ή’ χρησιμοποιείται με την ‘εγκλειστική’ έννοια, δηλαδή εάν P και Q είναι προτάσεις, τότε ‘P ή Q’ (που συμβολίζεται

$P \vee Q$) είναι πρόταση που θεωρείται αληθής εάν τουλάχιστον μία από τις P, Q, είναι αληθής. Αυτό παριστάνεται στον ακόλουθο πίνακα αληθείας:

P	Q	$P \vee Q$
Α	Α	Α
Α	Ψ	Α
Ψ	Α	Α
Ψ	Ψ	Ψ

Διαβάζουμε κατά μήκος των οριζόντιων γραμμών. Για παράδειγμα, η δεύτερη γραμμή λέει οτι εάν P είναι αληθής και Q είναι ψευδής, τότε $P \vee Q$ είναι αληθής.

Άλλοι σύνδεσμοι που χρησιμοποιούνται συχνά στα μαθηματικά είναι οι 'και', 'συνεπάγεται' και 'εάν και μόνον εάν', που συμβολίζονται αντίστοιχα, $\wedge$, $\Rightarrow$, $\Leftrightarrow$. Έχουν τους ακόλουθους πίνακες αληθείας:

P	Q	$P \wedge Q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Ψ
Ψ	Ψ	Ψ

P	Q	$P \Rightarrow Q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Α
Ψ	Ψ	Α

P	Q	$P \Leftrightarrow Q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Ψ
Ψ	Ψ	Α

Αυτοί οι πίνακες διαβάζονται με τον ίδιο τρόπο. Ο πρώτος και ο τελευταίος είναι αρκετά προφανείς. 'P και Q' θεωρείται αληθής μόνο όταν η P και η Q είναι αληθείς. 'P εάν και μόνον εάν Q' θεωρείται αληθής μόνον όταν οι P και Q έχουν τις ίδιες τιμές αληθείας.

Περισσότερο ενδιαφέρον παρουσιάζει ο πίνακας αληθείας της συνεπαγωγής. Εάν η P είναι αληθής, τότε από την πρώτη και τη δεύτερη γραμμή παρατηρούμε οτι η συνεπαγωγή $P \Rightarrow Q$ είναι αληθής όταν η Q είναι αληθής, ενώ είναι ψευδής όταν η Q είναι ψευδής. Αυτό δείχνει οτι όταν αληθεύει η $P \Rightarrow Q$, εάν η P είναι αληθής τότε η Q πρέπει να είναι αληθής. Αυτή είναι η κανονική ερμηνεία της συνεπαγωγής $\Rightarrow$, και γι'αυτό το λόγο η πρόταση $P \Rightarrow Q$ συχνά ερμηνεύεται 'εάν P, τότε Q'. Αλλά προσέξτε τι συμβαίνει όταν η P είναι ψευδής. Η τρίτη και η τέταρτη γραμμή δείχνουν οτι η συνεπαγωγή $P \Rightarrow Q$ θεωρείται αληθής, είτε είναι αληθής η Q είτε όχι. Συχνά ακούει κανείς πολλές ανοησίες γι'αυτήν την περίπτωση: 'πώς είναι δυνατόν το ψεύδος της P να συνεπάγεται την αλήθεια της Q;'

Μπορούμε να κατανοήσουμε καλύτερα αυτήν την περίπτωση εάν χρησιμοποιήσουμε τους συνδέσμους με κατηγορήματα αντί για προτάσεις. Εάν $P(x)$ και $Q(x)$ είναι κατηγορήματα που ορίζονται στο σύνολο S, τότε μπορούμε να χρησιμοποιήσουμε τους συνδέσμους για να πάρουμε τα κατηγορήματα $P(x) \vee Q(x)$, $P(x) \wedge Q(x)$, κλπ. Ειδικότερα έχουμε το κατηγόρημα $P(x) \Rightarrow Q(x)$. Υπάρχουν περιπτώσεις όπου το κατηγόρημα $P(x) \Rightarrow Q(x)$ είναι αληθές για κάθε $x \in S$. Αυτή είναι η περίπτωση που διασαφηνίζει τη σημασία του πίνακα αληθείας. Για παράδειγμα, εάν $P(x)$ είναι '$x > 5$' και $Q(x)$ είναι '$x > 2$', κάθε μαθηματικός θα συμφωνούσε οτι το κατηγόρημα $P(x) \Rightarrow Q(x)$ είναι αληθές για κάθε τιμή του $x \in \mathbb{R}$. Πολλοί θα το διάβαζαν 'εάν $x > 5$ τότε $x > 2$' και δεν θα έδιναν σημασία στο τι συμβαίνει όταν $x \not> 5$. Ας αντικαταστήσουμε διάφορες τιμές του x, να δούμε τι συμβαίνει:

$$\text{Για } x = 4, \quad P(4) \text{ είναι ψευδής και } Q(4) \text{ είναι αληθής.}$$

$$\text{Για } x = 2, \quad P(2) \text{ είναι ψευδής και } Q(2) \text{ είναι ψευδής.}$$

Αυτές είναι ακριβώς η τρίτη και η τέταρτη γραμμή του πίνακα αληθείας της συνεπαγωγής $\Rightarrow$, και βοηθάνε να κατανοήσουμε την ακόλουθη ερμηνεία του πίνακα:

$$\text{'}P \Rightarrow Q \text{ είναι αληθής'}$$

σημαίνει οτι
α′) εάν P είναι αληθής, τότε Q πρέπει να είναι αληθής
αλλά
β′) εάν P είναι ψευδής, τότε Q μπορεί να είναι είτε αληθής είτε ψευδής.

Άσκηση 4.2 Εστω οτι P συμβολίζει την πρόταση 'Η ύλη είναι ενδιαφέρουσα', Q συμβολίζει την πρόταση 'Οι ασκήσεις είναι δύσκολες' και R συμβολίζει την πρόταση 'Το μάθημα είναι ευχάριστο'. Γράψτε τις παρακάτω προτάσεις σε συμβολική μορφή.

α′. Η ύλη είναι ενδιαφέρουσα και οι ασκήσεις είναι δύσκολες.

β′. Εάν η ύλη δεν είναι ενδιαφέρουσα και οι ασκήσεις δεν είναι δύσκολες, τότε το μάθημα δεν είναι ευχάριστο.

γ′. Το οτι η ύλη είναι ενδιαφέρουσα σημαίνει οτι οι ασκήσεις είναι δύσκολες, και το αντίστροφο.

δ′. Είτε η ύλη είναι ενδιαφέρουσα είτε οι ασκήσεις δεν είναι δύσκολες, αλλά όχι και τα δύο.

Μπορούμε να θεωρήσουμε και άλλους συνδέσμους, όπως για παράδειγμα την *αποκλειστική διάζευξη*, που τη συμβολίζουμε $\veebar$, με πίνακα αληθείας

P	Q	$P \veebar Q$
Α	Α	Ψ
Α	Ψ	Α
Ψ	Α	Α
Ψ	Ψ	Ψ

Η $P \veebar Q$ είναι αληθής όταν μια από τις P, Q είναι αληθής, αλλά όχι και οι δύο, δηλαδή όταν αληθεύει ακριβώς μία από τις P, Q.

Θα μπορούσαμε να ορίσουμε πίνακες αληθείας και για άλλους συνδέσμους, αλλά αυτοί μπορούν να κατασκευασθούν συνθέτοντας τους βασικούς. Για παράδειγμα, η αποκλειστική διάζευξη μπορεί να εκφραστεί ως $(P \vee Q) \wedge \neg(P \wedge Q)$. Θα δούμε πιο αναλυτικά αυτό το θέμα σε επόμενη παράγραφο.

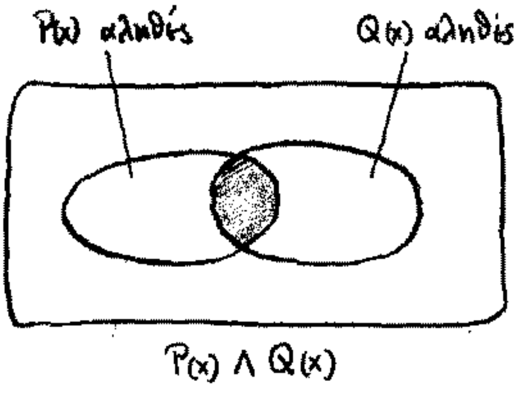
Όταν μία μαθηματικός γράφει Μαθηματικά, δεν περιορίζεται στους συνδέσμους που αναφέραμε. Χρησιμοποιεί και άλλους συνδέσμους της γλώσσας, όπως 'αλλά', 'επειδή', 'εφόσον', 'διότι', κλπ. Αυτές οι εκφράσεις έχουν μία, συνήθως προφανή, ερμηνεία. Για παράδειγμα, ο πίνακας αληθείας της πρότασης 'P αλλά Q' είναι ο ίδιος με αυτόν της πρότασης 'P και Q'. Η πρόταση '$\sqrt{2}$ είναι άρρητος αλλά $(\sqrt{2})^2$ είναι ρητός' σημαίνει το ίδιο με '$\sqrt{2}$ είναι άρρητος και $(\sqrt{2})^2$ είναι ρητός'. Παρόμοια, 'P επειδή Q' και 'Q άρα P' έχουν τον ίδιο πίνακα αληθείας με την '$Q \Rightarrow P$'.

Η σχέση με τη θεωρία συνόλων

Αν εφαρμόσουμε τους συνδέσμους και την άρνηση σε κατηγορήματα μίας μεταβλητής, έχουμε μία απλή σχέση με το συνολοθεωρητικό συμβολισμό. Υποθέτουμε οτι $P(x)$ και $Q(x)$ είναι κατηγορήματα που ορίζονται στο ίδιο σύνολο S, και εξετάζουμε τα υποσύνολα για τα οποία διάφορες σύνθετες εκφράσεις είναι αληθείς. Για το σύνδεσμο 'και' έχουμε:

$$\{x \in S \mid P(x) \wedge Q(x)\} = \{x \in S \mid P(x)\} \cap \{x \in S \mid Q(x)\},$$

δηλαδή την τομή των συνόλων στα οποία αληθεύουν τα κατηγορήματα $P(x)$ και $Q(x)$.



Σχήμα 4.1: Συνολοθεωρητική ερμηνεία του σύνδεσμου 'και'.

Παρόμοια, για το σύνδεσμο 'ή' έχουμε:

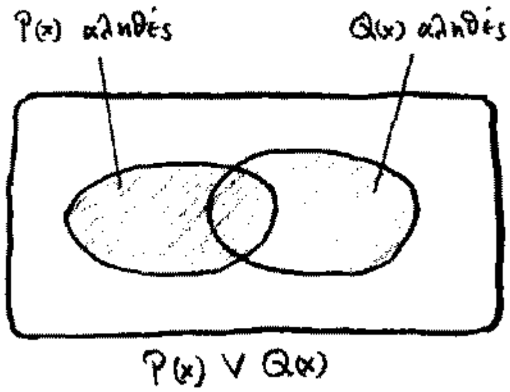
$$\{x \in S \mid P(x) \vee Q(x)\} = \{x \in S \mid P(x)\} \cup \{x \in S \mid Q(x)\},$$

δηλαδή την ένωση των συνόλων στα οποία αληθεύουν τα κατηγορήματα $P(x)$ και $Q(x)$.

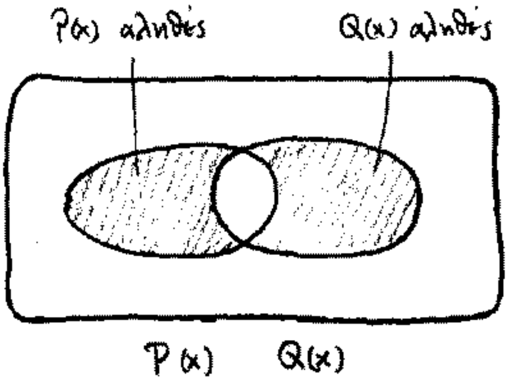
Αυτός είναι ένας λόγος για τον οποίο προτιμούμε να χρησιμοποιούμε την 'εγκλειστική διάζευξη', $\vee$, και όχι την 'αποκλειστική διάζευξη', $\veebar$, η οποία αντιστοιχεί στη συμμετρική διαφορά στη θεωρία συνόλων.

Η άρνηση $\neg$ εφαρμοζόμενη στο κατηγόρημα $P(x)$ αντιστοιχεί στο συνολοθεωρητικό συμπλήρωμα.

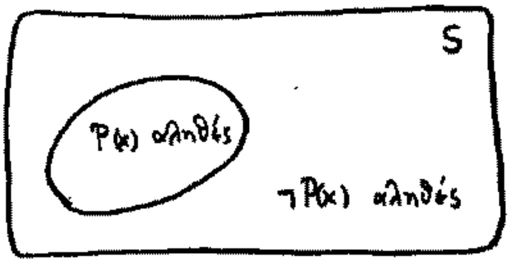
$$\{x \in S \mid \neg P(x)\} = S \setminus \{x \in S \mid P(x)\}$$



Σχήμα 4.2: Συνολοθεωρητική ερμηνεία του συνδέσμου 'ή'.



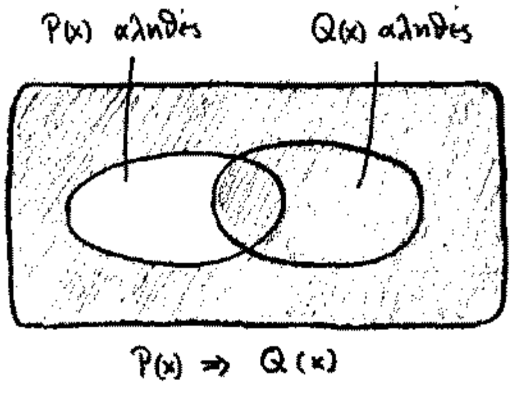
Σχήμα 4.3: Συνολοθεωρητική ερμηνεία της αποκλειστικής διάζευξης.



Σχήμα 4.4: Συνολοθεωρητική ερμηνεία της λογικής άρνησης.

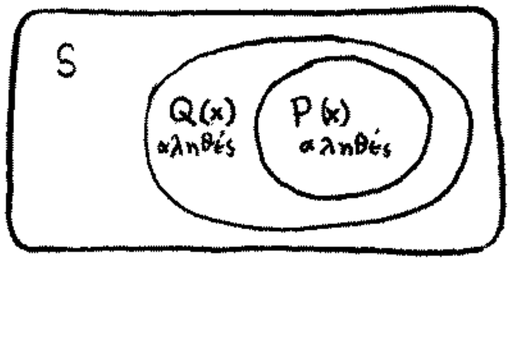
Είδαμε οτι $P(x) \Rightarrow Q(x)$ είναι αληθής όταν η $Q(x)$ είναι αληθής ή όταν η $P(x)$ είναι ψευδής,

$$\{x \in S \mid P(x) \Rightarrow Q(x)\} = (S \setminus \{x \in S \mid P(x)\}) \cup \{x \in S \mid Q(x)\}\,.$$



Σχήμα 4.5: Συνολοθεωρητική ερμηνεία της συνεπαγωγής.

Περισσότερο ενδιαφέρον παρουσιάζει η περίπτωση όπου $P(x) \Rightarrow Q(x)$ είναι αληθής για όλα τα x. Σε αυτή την περίπτωση, εάν $P(x)$ είναι αληθής, το ίδιο πρέπει να ισχύει για το $Q(x)$, δηλαδή εάν $a \in \{x \in S | P(x)\}$ τότε $a \in \{x \in S | Q(x)\}$, το οποίο σημαίνει οτι $\{x \in S | P(x)\} \subseteq \{x \in S | Q(x)\}$. Η αλήθεια της έκφρασης $P(x) \Rightarrow Q(x)$ για κάθε $x \in S$ αντιστοιχεί στο συνολοθεωρητικό εγκλεισμό.



Σχήμα 4.6: Λογική συνεπαγωγή και εγκλεισμός.

Παρόμοια, $P(x) \Leftrightarrow Q(x)$ για κάθε $x \in S$ αντιστοιχεί στην ισότητα

$$\{x \in S | P(x)\} = \{x \in S | Q(x)\}\,.$$

Σύνθετες εκφράσεις

Χρησιμοποιώντας συνδέσμους μπορούμε να κατασκευάσουμε πιο σύνθετες προτάσεις και κατηγορήματα από κάποια δεδομένα, όπως $(P \wedge Q) \vee R$. Αυτή η έκφραση περιλαμβάνει τρεις *προτασιακές μεταβλητές*, και ο πίνακας αληθείας της έχει $2^3 = 8$ γραμμές[1].

P	Q	R	Ενδιάμεσος Υπολογισμός $P \wedge Q$	$(P \wedge Q) \vee R$
Α	Α	Α	Α	Α
Α	Α	Ψ	Α	Α
Α	Ψ	Α	Ψ	Α
Α	Ψ	Ψ	Ψ	Ψ
Ψ	Α	Α	Ψ	Α
Ψ	Α	Ψ	Ψ	Ψ
Ψ	Ψ	Α	Ψ	Α
Ψ	Ψ	Ψ	Ψ	Ψ

Παρατηρήστε οτι η έκφραση '$(P \wedge Q) \vee R$' είναι στην πραγματικότητα μία συνταγή για να κατασκευάσουμε μία νέα πρόταση ή ένα νέο κατηγόρημα, από τρία δοθέντα. Την ονομάζουμε *σύνθετο τύπο* του προτασιακού λογισμού, και θεωρούμε τα P, Q, R ως μεταβλητές που αντιπροσωπεύουν απροσδιόριστες προτάσεις ή κατηγορήματα. Όταν αντικαταστήσουμε τις μεταβλητές P, Q, R με συγκεκριμένες προτάσεις, για παράδειγμα

$$(2 > 3 \ \wedge \ 2 > 6) \ \vee \ 2 > 1\,,$$

παίρνουμε μία *σύνθετη πρόταση*. Εάν τις αντικαταστήσουμε με συγκεκριμένα κατηγορήματα, ονομάζουμε το αποτέλεσμα *σύνθετο κατηγόρημα*. Για παράδειγμα,

$$(x > 3 \ \wedge \ x > 6) \ \vee \ 2 > 1$$

είναι ένα σύνθετο κατηγόρημα.

Ένα μεγάλο μέρος κάθε μαθηματικής απόδειξης έχει να κάνει με το χειρισμό σύνθετων προτάσεων και κατηγορημάτων. Όταν τα κατασκευάζουμε, είναι συχνά απαραίτητο να χρησιμοποιούμε παρενθέσεις για να φαίνεται η δομή τους. Για παράδειγμα ο σύνθετος τύπος $P \wedge (Q \vee R)$ είναι διαφορετικός από τον $(P \wedge Q) \vee R$. Αν κοιτάξουμε στην έβδομη γραμμή του πίνακα, βλέπουμε οτι όταν P είναι ψευδής, Q είναι ψευδής και R είναι αληθής, τότε $(P \wedge Q) \vee R$ είναι αληθής. Όμως μπορούμε να ελέγξουμε οτι σε αυτήν την περίπτωση $P \wedge (Q \vee R)$ είναι ψευδής. Ανάλογα ισχύουν και για κατηγορήματα. Πρέπει λοιπόν να τοποθετούμε τις παρενθέσεις στη σωστή θέση, για να μην δημιουργούνται ασάφειες. (Σε ορισμένες περιπτώσεις μπορούμε να παραλείπουμε παρενθέσεις. Για παράδειγμα, ο $(P \wedge Q) \wedge R$ έχει τον ίδιο πίνακα αληθείας με τον $P \wedge (Q \wedge R)$, άρα δεν προκαλείται σύγχυση αν γράψουμε $P \wedge Q \wedge R$.)

Καθώς κατασκευάζουμε σύνθετους τύπους χρησιμοποιώντας συνδέσμους, μπορεί να προκύψουν τύποι που έχουν διαφορετική εμφάνιση αλλά τον ίδιο πίνακα αληθείας. Για παράδειγμα, $P \Rightarrow Q$ και $(\neg Q) \Rightarrow (\neg P)$:

P	Q	$P \Rightarrow Q$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Α
Ψ	Ψ	Α

[1] Προσέξτε πώς γράφουμε συστηματικά τις τιμές αληθείας των μεταβλητών στον πίνακα, εξασφαλίζοντας οτι εξαντλούμε όλους τους δυνατούς συνδυασμούς.

P	Q	$\neg P$	$\neg Q$	$(\neg Q) \Rightarrow (\neg P)$
Α	Α	Ψ	Ψ	Α
Α	Ψ	Ψ	Α	Ψ
Ψ	Α	Α	Ψ	Α
Ψ	Ψ	Α	Α	Α

ή παραλείποντας τους ενδιάμεσους υπολογισμούς,

P	Q	$(\neg Q) \Rightarrow (\neg P)$
Α	Α	Α
Α	Ψ	Ψ
Ψ	Α	Α
Ψ	Ψ	Α

Σε αυτή την περίπτωση λέμε οτι οι δύο σύνθετοι τύποι είναι **λογικά ισοδύναμοι**.

Εάν συμβολίζουμε δύο σύνθετους τύπους με S_1 και S_2 γράφουμε

$$S_1 \equiv S_2$$

για να συμβολίσουμε οτι είναι λογικά ισοδύναμοι. Το προηγούμενο αποτέλεσμα συμβολίζεται

$$P \Rightarrow Q \;\equiv\; (\neg Q) \Rightarrow (\neg P)\,.$$

Μία ενδιαφέρουσα ιδιότητα των σύνθετων τύπων είναι οτι μερικές φορές δύο τύποι μπορεί να είναι ισοδύναμοι παρ'όλο που δεν περιέχουν τον ίδιο αριθμό μεταβλητών. Αυτό συμβαίνει όταν η αλλαγή της τιμής αληθείας μίας μεταβλητής δεν επηρεάζει το τελικό αποτέλεσμα. Για παράδειγμα, $P \wedge (\neg P)$ είναι πάντοτε ψευδής. Υπολογίζουμε τον πίνακα αληθείας του $(P \wedge (\neg P)) \vee (\neg Q)$

P	Q	$(P \wedge (\neg P)) \vee (\neg Q)$
Α	Α	Ψ
Α	Ψ	Α
Ψ	Α	Ψ
Ψ	Ψ	Α

και βλέπουμε οτι $(P \wedge (\neg P)) \vee (\neg Q)$ έχει πάντα την ίδια τιμή αληθείας με το $\neg Q$, ανεξάρτητα από την τιμή του P. Μπορούμε να θεωρήσουμε τυπικά το $\neg Q$ ως συνάρτηση του P και του Q, οπότε ο πίνακας αληθείας γίνεται

P	Q	$\neg Q$
Α	Α	Ψ
Α	Ψ	Α
Ψ	Α	Ψ
Ψ	Ψ	Α

Με αυτόν τον τρόπο έχουμε οτι

$$\neg Q \;\equiv\; (P \wedge (\neg P)) \vee (\neg Q).$$

Ένας σύνθετος τύπος ονομάζεται **ταυτολογία** εάν είναι αληθής για οποιεσδήποτε τιμές αληθείας των μεταβλητών του. Χαρακτηριστικά παραδείγματα είναι

$$\begin{gathered} P \vee (\neg P) \\ P \Rightarrow (P \vee Q) \\ (P \wedge Q) \Rightarrow P \\ (P \Rightarrow Q) \Leftrightarrow ((\neg Q) \Rightarrow (\neg P)) \\ (P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P)). \end{gathered}$$

Πρέπει να ελέγξετε οτι οι πίνακες αληθείας αυτών των τύπων δίδουν πάντοτε την τιμή Α.

Εάν ένας σύνθετος τύπος είναι ψευδής για οποιεσδήποτε τιμές αληθείας των μεταβλητών του, ονομάζεται **αντίφαση**. Για παράδειγμα, $P \wedge (\neg P)$ είναι αντίφαση.

Κάθε δύο ταυτολογίες είναι λογικά ισοδύναμες, και κάθε δύο αντιφάσεις είναι λογικά ισοδύναμες. Επίσης, ένας σύνθετος τύπος S είναι ταυτολογία εάν και μόνον εάν $\neg S$ είναι αντίφαση.

Συμβολίζουμε μία ταυτολογία με T, και μία αντίφαση με C. Έχουμε τότε κάποια ενδιαφέροντα αποτελέσματα. Για παράδειγμα, $(\neg P) \Rightarrow C$ είναι λογικά ισοδύναμο με το P. Οι πίνακες είναι:

P	$(\neg P) \Rightarrow C$
Α	Α
Ψ	Ψ

P	P
Α	Α
Ψ	Ψ

(Υπολογίζοντας τον πρώτο πίνακα, προσέξτε οτι C έχει πάντα τιμή αληθείας Ψ.)

Έχουμε το ίδιο αποτέλεσμα εάν αντικαταστήσουμε το C με οποιαδήποτε συγκεκριμένη αντίφαση:

P	Q	$(\neg P) \Rightarrow (Q \wedge (\neg Q))$
Α	Α	Α
Α	Ψ	Α
Ψ	Α	Ψ
Ψ	Ψ	Ψ

P	Q	P
Α	Α	Α
Α	Ψ	Α
Ψ	Α	Ψ
Ψ	Ψ	Ψ

Πρέπει να ελέγξετε όλους τους ενδιάμεσους υπολογισμούς στον πρώτο πίνακα, για να καταλάβετε τι ακριβώς συμβαίνει.

Αντί να συγκρίνουμε τους πίνακες αληθείας δύο σύνθετων τύπων S_1 και S_2 για να ελέγξουμε εάν είναι λογικά ισοδύναμοι, μπορούμε να εξετάσουμε μόνο τον πίνακα του $S_1 \Leftrightarrow S_2$. Εάν ο S_1 είναι λογικά ισοδύναμος με τον S_2 τότε ο $S_1 \Leftrightarrow S_2$ είναι ταυτολογία, και αντίστροφα, εάν $S_1 \Leftrightarrow S_2$ είναι ταυτολογία, τότε $S_1 \equiv S_2$. Για παράδειγμα, η λογική ισοδυναμία των $P \Rightarrow Q$ και $(\neg Q) \Rightarrow (\neg P)$ αντιστοιχεί στο οτι ο τύπος $[P \Rightarrow Q] \Leftrightarrow [(\neg Q) \Rightarrow (\neg P)]$ είναι ταυτολογία.

Λογικά συμπεράσματα

Η γενική στρατηγική μιας απόδειξης συχνά έγκειται στο να αποδειχθεί, αντί για την ισχύ της δοθείσας πρότασης, η ισχύς μιας πρότασης που είναι λογικά ισοδύναμη με τη δοθείσα. Σημαντικά τέτοια παραδείγματα είναι τα ακόλουθα.

1. *Αντιθετοαντίστροφη.*

   $$(P \Rightarrow Q) \equiv ((\neg Q) \Rightarrow (\neg P))$$

   Για να αποδείξουμε $P \Rightarrow Q$, επαληθεύουμε την πρόταση $(\neg Q) \Rightarrow (\neg P)$.

2. *Απαγωγή σε άτοπο.*

   $$P \equiv ((\neg P) \Rightarrow C)$$

   όπου C είναι μία αντίφαση. Για να αποδείξουμε το P, επαληθεύουμε την πρόταση $(\neg P) \Rightarrow C$.

3. *'Εάν και μόνον εάν'.*

$$(P \Leftrightarrow Q) \equiv ((P \Rightarrow Q) \wedge (Q \Rightarrow P)).$$

4. *'Εάν και μόνον εάν', δεύτερη εκδοχή.*

$$(P \Leftrightarrow Q) \equiv ((P \Rightarrow Q) \wedge ((\neg P) \Rightarrow (\neg Q))).$$

Για να αποδείξουμε την πρόταση $P \Leftrightarrow Q$, επαληθεύουμε τις προτάσεις $P \Rightarrow Q$ και $(\neg P) \Rightarrow (\neg Q)$.

Για να επαληθεύσουμε μία σύνθετη πρόταση, εξετάζουμε πως κατασκευάζεται η πρόταση από γνωστές προτάσεις, και χρησιμοποιούμε πίνακες αληθείας. Ας υποθέσουμε οτι γνωρίζουμε πως η P είναι αληθής, και πως η $(\neg Q) \Rightarrow (\neg P)$ είναι αληθής. Από αυτά τα δεδομένα μπορούμε να συμπεράνουμε οτι η Q είναι αληθής. Τα δοθέντα μπορεί να είναι σύνθετες προτάσεις, όπως η $(\neg Q) \Rightarrow (\neg P)$, και μπορεί να γνωρίζουμε οτι η σύνθετη πρόταση αληθεύει, χωρίς να έχουμε πληροφορίες για την αλήθεια των συνιστωσών της. Έτσι μπορεί να γνωρίζουμε οτι $(\neg Q) \Rightarrow (\neg P)$ είναι αληθής, χωρίς να γνωρίζουμε τις τιμές αληθείας των P και Q. Ακόμα και σε αυτήν την περίπτωση μπορούμε να βγάλουμε κάποιο συμπέρασμα, όπως, για παράδειγμα, οτι η λογικά ισοδύναμη πρόταση $P \Rightarrow Q$ είναι αληθής. Στον ακόλουθο πίνακα, εάν γνωρίζουμε οτι οι προτάσεις στην πρώτη στήλη αληθεύουν, μπορούμε να συμπεράνουμε οτι αληθεύει η πρόταση στη δεύτερη στήλη.

Εάν αληθεύουν αυτές οι προτάσεις...	*...τότε αληθεύει και αυτή*
$P,\ (\neg Q) \Rightarrow (\neg P)$	Q
$\neg P \Rightarrow C$, όπου C αντίφαση	P
$P,\ P \Rightarrow Q$	Q
$P \Rightarrow Q,\ Q \Rightarrow R$	$P \Rightarrow R$
$P \vee Q,\ \neg P$	Q
$P \wedge Q$	$P \vee Q$
$P \Rightarrow Q,\ Q \Rightarrow P$	$P \Leftrightarrow Q$
$P_1, P_2, \ldots, P_n$	$P_1 \wedge P_2 \wedge \ldots \wedge P_n$
$P_1, \ldots, P_n, (P_1 \wedge \ldots \wedge P_n) \Rightarrow Q$	Q

Αυτός ο πίνακας μπορεί να συνεχιστεί επ' άπειρον. Για να πάρουμε μία ακόμη γραμμή, γράφουμε έναν αριθμό από σύνθετους προτασιακούς τύπους $S_1, \ldots, S_n$ στην αριστερή στήλη. Στην αντίστοιχη θέση στη δεξιά στήλη βάζουμε κάποιο σύνθετο προτασιακό τύπο D, του οποίου η αλήθεια είναι εξασφαλισμένη όταν αληθεύουν οι $S_1, \ldots, S_n$. Για να το ελέγξουμε αυτό εξετάζουμε τους πίνακες αληθείας των $S_1, \ldots, S_n$ και D. Μπορούμε όμως να το ελέγξουμε εξετάζοντας τον πίνακα αληθείας της πρότασης

$$(S_1 \wedge S_2 \wedge \ldots \wedge S_n) \Rightarrow D.$$

Εάν αυτή είναι ταυτολογία, τότε εάν αληθεύουν οι $S_1, \ldots, S_n$ αληθεύει και η D.

Μια ταυτολογία της μορφής $(S_1 \wedge S_2 \wedge \ldots \wedge S_n) \Rightarrow D$ ονομάζεται **κανόνας εξαγωγής συμπερασμάτων** ή **κανόνας απαγωγής**. Εάν σε ένα τέτοιο κανόνα, όταν αντικαταστήσουμε συγκεκριμένες προτάσεις για τις μεταβλητές στους σύνθετους προτασιακούς τύπους, οι προτάσεις $S_1, \ldots, S_n$ είναι αληθείς, τότε μπορούμε να συμπεράνουμε οτι και η πρόταση D είναι αληθής.

Οταν οι προτάσεις που εμφανίζονται περιλαμβάνουν ποσοδείκτες, πρέπει να εξετάσουμε πως συνδέονται για να δούμε εάν η ισχύς μίας πρότασης είναι φυσική συνέπεια των δεδομένων. Σε μία απλή περίπτωση, εάν γνωρίζουμε οτι $\forall x \in S : P(x)$ είναι αληθής, μπορούμε να συμπεράνουμε οτι $\exists x \in S : P(x)$ είναι επίσης αληθής. Εάν γνωρίζουμε οτι αληθεύουν οι $\forall x \in S : P(x)$ και $\forall x \in S : Q(x)$, μπορούμε να συμπεράνουμε οτι αληθεύουν πολλές προτάσεις, όπως $\forall x \in S : (P(x) \wedge Q(x))$, $[\forall x \in S : P(x)] \vee [\forall x \in S : Q(x)]$, $P(a) \wedge Q(b)$, όπου $a, b \in S$, κλπ. Μπορούμε πάλι να γράψουμε ένα πίνακα κανόνων συμπερασμάτων που μπορούμε να βγάλουμε από προτάσεις με ποσοδείκτες.

Εάν αληθεύουν αυτές οι προτάσεις...	*...τότε αληθεύει και αυτή*
$\forall x \in S : P(x),\ \forall x \in S : Q(x)$	$\forall x \in S : [P(x) \wedge Q(x)]$
$\forall x \in S : P(x)$ (όπου $S \neq \varnothing$)	$\exists x \in S : P(x)$
$\forall x \in S : P(x)$	$P(a)$ για οποιοδήποτε $a \in S$
$P(a)$ (όπου $a \in S$)	$\exists x \in S : P(x)$
$\neg(\forall x \in S : P(x))$	$\exists x \in S : (\neg P(x))$
$\neg(\exists x \in S : P(x))$	$\forall x \in S : (\neg P(x))$

Αυτός ο πίνακας μπορεί να συνεχιστεί με πλήθος άλλων κανόνων συμπερασμάτων. Στην αριστερή στήλη γράφουμε προτάσεις $S_1, \ldots, S_n$ οι οποίες μπορεί να περιέχουν ποσοδείκτες, και στη δεξιά στήλη γράφουμε μία πρόταση D, η οποία είναι υποχρεωτικά αληθής, εάν όλες οι $S_1, \ldots, S_n$ είναι αληθείς. Αυτό μπορούμε να το ελέγξουμε εξετάζοντας την πρόταση $(S_1 \wedge S_2 \wedge \ldots \wedge S_n) \Rightarrow D$. Όμως οι σύνθετες εκφράσεις που περιέχουν κατηγορήματα με ποσοδείκτες είναι πολύ πιο πολύπλοκες από τις προτάσεις, και δεν θα διατυπώσουμε μία γενική μέθοδο ελέγχου σε αυτήν την περίπτωση, ανάλογη των πινάκων αληθείας για τις σύνθετες προτάσεις.

Απόδειξη

Για τη λογική παρουσίαση μίας απόδειξης ξεκινάμε με κάποιες προτάσεις, τις υποθέσεις $H_1, H_2, \ldots, H_r$, και θέλουμε να συμπεράνουμε την ισχύ μίας πρότασης D, του συμπεράσματος. Η διαδικασία μπορεί να είναι αρκετά πολύπλοκη, με την εισαγωγή άλλων βοηθητικών προτάσεων. Καταγράφουμε τη διαδικασία σε βήματα, γράφοντας ένα πεπερασμένο πλήθος γραμμών, με εκφράσεις $L_1, L_2, \ldots, L_n$ τέτοιες ώστε $L_n = D$, και όπου για κάθε $m = 1, \ldots, n$, η γραμμή L_m είτε είναι κάποια από τις υποθέσεις $H_1, H_2, \ldots, H_r$, είτε είναι λογική συνέπεια των *προηγούμενων γραμμών* $L_1, L_2, \ldots, L_{m-1}$. Με αυτόν τον τρόπο εξασφαλίζουμε οτι η τελευταία γραμμή D είναι αληθής εάν οι υποθέσεις $H_1, H_2, \ldots, H_r$ είναι αληθείς. Εάν η L_m δεν είναι κάποια από τις υποθέσεις, ελέγχουμε οτι είναι λογική συνέπεια των $L_1, L_2, \ldots, L_{m-1}$ εξετάζοντας την τιμή αληθείας της σύνθετης πρότασης $L_1 \wedge L_2 \wedge \ldots \wedge L_{m-1} \Rightarrow L_m$.

Όταν το τελικό συμπέρασμα D είναι της μορφής $P \Rightarrow Q$, τότε συχνά οι μαθηματικοί αλλάζουν τη διαδικασία της απόδειξης, γράφοντας γραμμές με εκφράσεις $L_1, \ldots, L_n$ όπου P είναι η πρώτη έκφραση L_1 και Q η τελευταία L_n. Κάθε ενδιάμεση γραμμή είτε είναι μία από τις υποθέσεις, είτε είναι συνέπεια των προηγούμενων γραμμών.

Παράδειγμα 4.9 Με τις υποθέσεις

$H_1 : 5 > 2$

$H_2 : \forall x, y, z \in \mathbb{R} : ((x > y) \wedge (y > z) \Rightarrow (x > z))$

μπορούμε να γράψουμε την απόδειξη της πρότασης $(x > 5) \Rightarrow (x > 2)$ ως εξής

$L_1 : x > 5$

$L_2 : 5 > 2$

$L_3 : \forall x, y, z \in \mathbb{R} : ((x > y) \wedge (y > z) \Rightarrow (x > z))$

$L_4 : x > 2$

Αν και το συγκεκριμένο συμπέρασμα δεν είναι εντυπωσιακό, δείχνει τη γενική μορφή της απόδειξης, την οποία αποκρυσταλλώνουμε στον ακόλουθο ορισμό.

Ορισμός. Μία **απόδειξη** της πρότασης $P \Rightarrow Q$, (όπου P και Q είναι πρόταση ή κατηγόρημα), με δεδομένες τις υποθέσεις $H_1, \ldots, H_r$ αποτελείται από ένα πεπερασμένο πλήθος γραμμών

$$\begin{array}{ccc} L_1 & : & P \\ L_2 & : & \ldots \\ & \vdots & \\ L_n & : & Q \end{array}$$

όπου κάθε γραμμή L_m, για $2 \leq m \leq n$, είτε είναι μία από τις υποθέσεις H_s, $1 \leq s \leq r$, είτε μία πρόταση ή ένα κατηγόρημα, τέτοιο ώστε

$$(L_1 \wedge L_2 \wedge \ldots \wedge L_{m-1}) \Rightarrow L_m$$

είναι αληθής πρόταση.

Υπό αυτές τις συνθήκες, εάν η P είναι αληθής, τότε κάθε επόμενη γραμμή είναι επίσης αληθής, και ειδικότερα η Q είναι αληθής. Από τον πίνακα αληθείας της συνεπαγωγής βλέπουμε οτι αυτό εξασφαλίζει την αλήθεια της $P \Rightarrow Q$.

Αξίζει να δούμε τι συμβαίνει όταν η P είναι ψευδής. Αυτό μπορεί να συμβεί, για παράδειγμα όταν η P είναι κατηγόρημα, οπότε η αντικατάσταση συγκεκριμένων τιμών δίδει ψευδή πρόταση. Έτσι, στο προηγούμενο παράδειγμα, $x > 5$ δεν είναι αληθές όταν $x = 1$, και η γραμμή L_4 γίνεται $1 > 2$, το οποίο είναι επίσης ψευδές. Από την άλλη, εάν $x = 3$, τότε η L_1 είναι ψευδής, $3 > 5$, αλλά η L_4 είναι $3 > 2$, αληθής. Με λίγα λόγια, εάν η P είναι ψευδής δεν μπορούμε να βγάλουμε κάποιο συμπέρασμα ως προς την αλήθεια ή το ψεύδος των επόμενων γραμμών. Γνωρίζουμε όμως οτι η σύνθετη πρόταση $P \Rightarrow Q$ είναι αληθής.

Είδαμε τον τυπικό ορισμό λογικών βημάτων σε μία απόδειξη. Τι όμως γράφουμε στην πράξη, όταν παρουσιάζουμε μία απόδειξη; Αυτό θα εξετάσουμε στο επόμενο κεφάλαιο.

Ασκήσεις

Άσκηση 4.3 Γράψτε μια σύνθετη πρόταση η οποία να είναι αληθής όταν ακριβώς δύο από τις τρεις προτάσεις P, Q και R είναι αληθείς.
Γράψτε μια σύνθετη πρόταση η οποία να είναι αληθής, όταν καμία, ή μια, ή δύο από τις τρεις προτάσεις P, Q και R είναι αληθείς.

Άσκηση 4.4 Κατασκευάστε πίνακες αληθείας για τις παρακάτω προτάσεις

α'. $(P \Rightarrow \neg P) \Rightarrow (P \Rightarrow P)$

β'. $(P \Rightarrow R) \wedge (Q \Rightarrow R) \Leftrightarrow ((P \wedge Q) \Rightarrow R)$

γ'. $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$

Άσκηση 4.5 Φτιάξτε έναν (κοινό) πίνακα αληθείας για τις προτάσεις

$$\alpha'. \quad (P \Rightarrow Q) \wedge (Q \Rightarrow P) \quad , \quad P \Leftrightarrow Q$$

Έχουν αυτές οι προτάσεις πάντα τις ίδιες λογικές τιμές;
Κάνετε το ίδιο και με τα ζεύγη προτάσεων

$$\begin{array}{lrcl} \beta'. & (P \Rightarrow Q) \Rightarrow R & , & P \Rightarrow (Q \Rightarrow R) \\ \gamma'. & (P \Rightarrow Q) \wedge (Q \Rightarrow R) & , & P \Rightarrow R \\ \delta'. & P \Rightarrow Q & , & \neg P \vee Q \end{array}$$

Άσκηση 4.6 Γράψτε τις παρακάτω προτάσεις με λογικά σύμβολα, και εξετάστε εάν είναι αληθείς.

α'. Για κάθε πραγματικό αριθμό x, υπάρχει πραγματικός αριθμός y, τέτοιος ώστε $y^3 = x$.

β'. Υπάρχει πραγματικός αριθμός y, τέτοιος ώστε, για κάθε πραγματικό αριθμό x, το άθροισμα $x + y$ είναι θετικό.

γ'. Για κάθε άρρητο αριθμό x, υπάρχει ακέραιος n τέτοιος ώστε $x < n < x + 1$.

δ'. Το τετράγωνο κάθε ακεραίου αφήνει υπόλοιπο 0 ή 1 όταν διαιρεθεί με το 4.

ε'. Το άθροισμα των τετραγώνων δύο πρώτων αριθμών διαφορετικών από το 2 είναι άρτιος αριθμός.

Άσκηση 4.7 Διατυπώστε τις παρακάτω προτάσεις στα ελληνικά.

α'. $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R} : x^2 - 3xy + 2y^2 = 0$

β'. $\exists y \in \mathbb{R}\ \forall x \in \mathbb{R} : x^2 - 3xy + 2y^2 = 0$

γ'. $\exists N \in \mathbb{N}\ \forall \varepsilon \in \mathbb{R} : ((\varepsilon > 0) \wedge (n > N)) \Rightarrow (\frac{1}{n} < \varepsilon)$

δ'. $\forall x \in \mathbb{N}\ \forall y \in \mathbb{N}\ \exists z \in \mathbb{N} : x + z = y$

ε′. $\forall x \in \mathbb{Z}\ \forall y \in \mathbb{Z}\ \exists z \in \mathbb{Z} : x + z = y$

Εκτός από την κατά σύμβολο μετάφραση, δώστε και μια διατύπωση σε πιο στρωτή γλώσσα, που να μην αλλοιώνει τη σημασία. Ποιές από τις προτάσεις είναι αληθείς;

Άσκηση 4.8 Γράψτε την άρνηση κάθε μιας από τις ακόλουθες προτάσεις

α′. $\forall x : (P(x) \wedge Q(x))$

β′. $\exists x : (P(x) \Rightarrow Q(x))$

γ′. $\forall x \in \mathbb{R}\ \exists y \in \mathbb{R} : (x \geq y)$

δ′. $\forall x \in \mathbb{R}\ \forall y \in \mathbb{R}\ \exists z \in \mathbb{Q} : (x + y \geq z)$

Άσκηση 4.9 Σχηματίστε τους πίνακες αληθείας των παρακάτω προτάσεων, και εξετάστε ποιές από αυτές είναι ταυτολογίες.

α′. $P \Rightarrow (\neg P)$

β′. $(P \Rightarrow R) \wedge (Q \Rightarrow R) \Leftrightarrow ((P \wedge Q) \Rightarrow R)$

γ′. $(P \wedge Q) \Rightarrow (P \vee Q)$

δ′. $(P \Rightarrow Q) \vee (Q \Rightarrow P) \vee (\neg Q)$

Άσκηση 4.10 Σχηματίστε τους πίνακες αληθείας των παρακάτω ζευγών προτάσεων, και εξετάστε εάν οι δύο προτάσεις είναι λογικά ισοδύναμες.

α′. $\neg(P \wedge Q) \quad , \quad (\neg P) \vee (\neg Q)$

β′. $\neg(P \vee Q) \quad , \quad (\neg P) \wedge (\neg Q)$

γ′. $\neg(P \wedge (\neg P)) \quad , \quad P \vee (\neg P)$

δ′. $P \Rightarrow R \quad , \quad (\neg P) \wedge R$

ε′. $P \Rightarrow R \quad , \quad (\neg R) \wedge P$

ϛ′. $(P \Rightarrow Q) \wedge R \quad , \quad P \Rightarrow (Q \wedge R)$

ζ′. $(P \wedge (\neg Q)) \Rightarrow (R \wedge (\neg R)) \quad , \quad P \Rightarrow Q$

Κεφάλαιο 5

Μαθηματική Απόδειξη

Στο προηγούμενο κεφάλαιο εξετάσαμε τη λογική χρήση της γλώσσας στα Μαθηματικά, και τον τρόπο με τον οποίο η αλήθεια μίας πρότασης προκύπτει από άλλες δεδομένες. Είδαμε οτι μπορούμε να θεωρήσουμε μία απόδειξη ως μία ακολουθία λογικών συμπερασμάτων. Στην πράξη δεν είναι ικανοποιητικό να γράφουμε αποδείξεις με αυτόν τον τρόπο: εάν συμπεριλάβουμε κάθε βήμα το αποτέλεσμα είναι εξαιρετικά μακροσκελές. Σε αυτό το κεφάλαιο εξετάζουμε τη γενική εικόνα μιας μαθηματικής απόδειξης, και βλέπουμε πως γράφουν αποδείξεις οι μαθηματικοί στην πράξη. Εκτός από το λογικό σκελετό, το γράψιμο μίας απόδειξης απαιτεί κρίση για την ποσότητα των λεπτομερειών που αρμόζουν στη συγκεκριμένη περίπτωση. Τι πρέπει να συμπεριληφθεί και τι μπορεί να παραληφθεί. Πολύ λίγα στοιχεία μπορεί να αφήσουν έξω σημαντικό μέρος του επιχειρήματος, ενώ πάρα πολλά στοιχεία μπορεί να συσκοτίσουν την συνολική εικόνα.

Ξεκινάμε παίρνοντας μία κανονική απόδειξη, γραμμένη σε συνηθισμένο μαθηματικό στυλ, την οποία συγκρίνουμε με την τυπική δομή της απόδειξης στο προηγούμενο κεφάλαιο.

Θεώρημα 5.1 *Εάν (a_n) και (b_n) είναι ακολουθίες, τέτοιες ώστε $a_n \to a$ και $b_n \to b$ καθώς $n \to \infty$, τότε $(a_n + b_n) \to a + b$.*

Απόδειξη. Έστω $\varepsilon > 0$. Αφού $a_n \to a$, υπάρχει N_1 τέτοιο ώστε

$$n > N_1 \Rightarrow |a_n - a| < \frac{1}{2}\,\varepsilon$$

Αφού $b_n \to b$, υπάρχει N_2 τέτοιο ώστε

$$n > N_2 \Rightarrow |b_n - b| < \frac{1}{2}\,\varepsilon$$

Θέτουμε $N = \max\{N_1, N_2\}$. Εάν $n > N$, τότε

$$|a_n - a| < \frac{1}{2}\,\varepsilon \quad \text{και} \quad |b_n - b| < \frac{1}{2}\,\varepsilon\,,$$

άρα, από την τριγωνική ανισότητα

$$\begin{aligned} |(a_n + b_n) - (a + b)| &\le |a_n - a| + |b_n - b| \\ &\le \frac{1}{2}\,\varepsilon + \frac{1}{2}\,\varepsilon \\ &= \varepsilon\,. \end{aligned}$$

Έπεται οτι $(a_n + b_n) \to a + b$.

$\square$

Για να αναλύσουμε τη δομή της απόδειξης, την ξαναγράφουμε, γραμμή – γραμμή, προσθέτοντας μερικά σχόλια που αποσαφηνίζουν το επιχείρημα.

Οι υποθέσεις του θεωρήματος είναι:
H_1: (a_n) είναι ακολουθία πραγματικών αριθμών, και $a_n \to a$ καθώς $n \to \infty$.
H_2: (b_n) είναι ακολουθία πραγματικών αριθμών, και $b_n \to b$ καθώς $n \to \infty$.
και το συμπέρασμα είναι
D: για την ακολουθία πραγματικών αριθμών $(a_n + b_n)$ έχουμε οτι $a_n + b_n \to a + b$ καθώς $n \to \infty$.

Η απόδειξη είναι:

1. Έστω $\varepsilon > 0$
2. Αφού $(a_n) \to a$, υπάρχει N_1 τέτοιο ώστε $n > N_1 \Rightarrow |a_n - a| < \frac{1}{2}\,\varepsilon$
3. Αφού $(b_n) \to b$, υπάρχει N_2 τέτοιο ώστε $n > N_2 \Rightarrow |b_n - b| < \frac{1}{2}\,\varepsilon$
4. Έστω $N = \max\{N_1, N_2\}$
5. Εάν $n > N$ τότε $|a_n - a| < \frac{1}{2}\,\varepsilon$ και $|b_n - b| < \frac{1}{2}\,\varepsilon$.
6. $|(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b|$ από την τριγωνική ανισότητα.
7. $|a_n - a| + |b_n - b| < \frac{1}{2}\,\varepsilon + \frac{1}{2}\,\varepsilon$
8. $\frac{1}{2}\,\varepsilon + \frac{1}{2}\,\varepsilon = \varepsilon$
9. (Υπάρχει $N = \max\{N_1, N_2\}$ τέτοιο ώστε) $n > N \Rightarrow |(a_n + b_n) - (a + b)| < \varepsilon$.
10. $(a_n + b_n) \to a + b$, ο.ε.δ.

Η γραμμή 1 είναι το κατηγόρημα: $P(\varepsilon) : \varepsilon > 0$, και κοιτώντας πιο κάτω βλέπουμε οτι στη γραμμή 9 καταλήγουμε στην ύπαρξη ενός N τέτοιου ώστε $n > N \Rightarrow |(a_n+b_n)-(a+b)| < \varepsilon$. Εάν $Q(\varepsilon)$ είναι το κατηγόρημα:

$$(\exists N \in \mathbb{N}) : ((n > N) \Rightarrow (|(a_n + b_n) - (a + b)| < \varepsilon))\,,$$

οι γραμμές 1 – 9 αποτελούν απόδειξη της συνεπαγωγής $P(\varepsilon) \Rightarrow Q(\varepsilon)$. Στη γραμμή 10 αυτό ερμηνεύεται ως το συμπέρασμα, οτι $(a_n + b_n) \to (a + b)$.

Στις γραμμές 2 και 3 οι υποθέσεις H_1, H_2, διατυπώνονται αναλυτικά, χρησιμοποιώντας τον ορισμό της σύγκλισης: $a_n \to a$ καθώς $n \to \infty$ σημαίνει

$$\text{Για κάθε } \varepsilon > 0 \text{ υπάρχει } N \text{ τέτοιο ώστε } n > N \Rightarrow |a_n - a| < \varepsilon.$$

Προσέξτε οτι παραλείπεται το επιπλέον βήμα, οτι εάν $\varepsilon > 0$ τότε $\frac{1}{2}\,\varepsilon > 0$. Στην πράξη, τέτοια μικρά βήματα, που αποτελούν μέρος της τεχνικής, παραλείπονται.

Στη γραμμή 4 εισάγεται ένας νέος ορισμός: ορίζουμε το σύμβολο N συναρτήσει των N_1 και N_2. Θα μπορούσαμε να παραλείψουμε αυτό τον ορισμό, και να αντικαταστήσουμε κάθε φορά στην απόδειξη το σύμβολο N με το $\max\{N_1, N_2\}$, χωρίς καμιά ουσιαστική διαφορά.

Συνηθίζεται όμως να χρησιμοποιούνται νέα σύμβολα για σύνθετες έννοιες που κατασκευάζονται από άλλες, για να διατηρείται πιό απλός ο συμβολισμός και να αναδεικνύονται σημαντικά στοιχεία της απόδειξης.

Η γραμμή 5 είναι συνέπεια των 2, 3, 4: $n > N \Rightarrow n > N_1 \Rightarrow |a_n - a| < \frac{1}{2}\varepsilon$ και $n > N \Rightarrow n > N_2 \Rightarrow |b_n - b| < \frac{1}{2}\varepsilon$. Προσέξτε οτι οι προφανείς συνεπαγωγές, οτι εάν $n > N = \max\{N_1, N_2\}$ τότε $n > N_1$ και $n > N_2$ παραλείπονται από την απόδειξη.

Στη γραμμή 6 παραλείπεται ο στοιχειώδης αλγεβρικός χειρισμός $|(a_n + b_n) - (a + b)| = |(a_n - a) + (b_n - b)|$, και κατόπιν εφαρμόζεται η τριγωνική ανισότητα για να πάρουμε το τελικό αποτέλεσμα. Αν και η πρόταση μοιάζει να είναι κατηγόρημα στο n, θεωρούμε οτι η μεταβλητή δεσμεύεται από τον (υπονοούμενο) ποσοδείκτη $\forall(n > N)$ στη γραμμή 5.

Η γραμμή 7 είναι συνέπεια των 5 και 6, εφαρμόζοντας (σιωπηρά) ιδιότητες πρόσθεσης ανισοτήτων.

Στη γραμμή 8 εκτελούνται απλές αριθμητικές πράξεις.

Τέλος η γραμμή 9 είναι συνέπεια των 2 – 8.

Τι παρατηρούμε από την ανάλυση αυτής της σχετικά απλής απόδειξης; Οι μαθηματικοί δεν γράφουν αποδείξεις ακριβώς με τον τρόπο που περιγράψαμε την τυπική απόδειξη. Οι κυριότερες διαφορές είναι οτι

1. Παραλείπονται υποθέσεις.

2. Παραλείπονται βήματα στην εξαγωγή συμπερασμάτων.

3. Εισάγονται ορισμοί νέων εννοιών.

Το αποτέλεσμα είναι να παρουσιάζεται η απόδειξη σε μία πιο ρευστή γραφή απ' οτι η ακολουθία προτάσεων της τυπικής απόδειξης.

Στόχος της απόδειξης είναι να κάνει κατανοητή την αλληλουχία των συμπερασμάτων. Η παράλειψη λεπτομερειών που θεωρούνται περιττές, και η εισαγωγή νέων συμβόλων, επιτρέπει να γίνει η απόδειξη πιο σύντομη και ευανάγνωστη.

Ο ανθρώπινος νούς κατασκευάζει θεωρίες αναγνωρίζοντας γνωστές χαρακτηριστικές μορφές στα επιχειρήματα, παραμερίζοντας λεπτομέρειες που είναι καλά κατανοητές. Ο βασικός περιοριστικός παράγων είναι η ποσότητα νέων πληροφοριών που μπορεί να συγκρατεί κάθε στιγμή στην προσοχή ο νους, και η 'συμπύκνωση' που προέρχεται από τον παραμερισμό λεπτομερειών και την ενοποίηση εννοιών, είναι απαραίτητη για τη σύλληψη της συνολικής εικόνας. Έτσι, βήματα της λογικής απόδειξης, τα οποία αποτελούν μέρος της βασικής τεχνικής, συντομεύονται, για να αναδειχθεί η συνολική εικόνα.

Όταν μία μαθηματικός αναπτύσσει μία νέα θεωρία, τείνει να διακρίνει μεταξύ των γνωστών αποτελεσμάτων, που αποτελούν μέρος της τεχνικής, και του νέου υλικού που αναπτύσσει. Τα γνωστά στοιχεία μπορούν να συντομευθούν σε μεγάλο βαθμό, καθώς θα μπορούσαν να αναλυθούν και να συμπληρωθούν εάν ετίθεντο υπό αμφισβήτηση. Νέα στοιχεία, που αποτελούν τον πυρήνα της αναπτυσσόμενης θεωρίας, αντιμετωπίζονται με μεγαλύτερη προσοχή. Αναφέρονται ρητά ως υπόθεση όταν χρειάζονται.

Σε τι βαθμό προχωράει αυτή η διαδικασία παράληψης και συντόμευσης, είναι ζήτημα ύφους και εξαρτάται από το κοινό στο οποίο απευθύνεται η απόδειξη: διαφορετικά θα γραφτεί μια απόδειξη σε ένα εγχειρίδιο, σε μία ερευνητική μονογραφία, ή σε ένα άρθρο σε επιστημονικό περιοδικό.

Η απόδειξη στο παράδειγμα, απευθύνεται σε φοιτητές μαθηματικών του 1ου ή του 2ου έτους. Ετσι, στη μελέτη της μαθηματικής ανάλυσης, οι κανόνες της αριθμητικής θεωρούνται εντελώς οικείοι, και δεν αναφέρονται. Οι νέες έννοιες, όπως τα όρια ακολουθιών, αναφέρονται ρητά. Η τριγωνική ανισότητα θεωρείται γνωστή, αλλά όχι τόσο οικεία, και γίνεται μία αναφορά σε αυτή.

Αξιωματικά συστήματα

Η διαδικασία της απόδειξης, όπως είδαμε, εξάγει κάποια συμπεράσματα από κάποιες υποθέσεις, οι οποίες μπορεί να είναι ρητά διατυπωμένες ή να προσδιορίζονται από το αντικείμενο της μελέτης. Για να έχει αυτή η διαδικασία στέρεες βάσεις, πρέπει να έχουμε κάποιες αρχικές υποθέσεις, τις οποίες δεχόμαστε ως **αξιώματα**, και από αυτές συμπεραίνουμε όλα τα άλλα αποτελέσματα της θεωρίας.

Αυτά τα αποτελέσματα τα ονομάζουμε *θεωρήματα, προτάσεις, λήμματα* ή *πορίσματα*. Αυτά τα διαφορετικά ονόματα βοηθούν να παρουσιάσουμε πιο ανάγλυφα τη δομή της θεωρίας και την αλληλεξάρτηση των αποτελεσμάτων. Συνήθως θεωρήματα ονομάζουμε τα πιο σημαντικά αποτελέσματα, ενώ προτάσεις τα λιγότερο σημαντικά. Για να διευκολυνθεί η παρουσίαση μίας μακροσκελούς απόδειξης, μπορούμε να διακρίνουμε αποτελέσματα που αποτελούν συστατικό της απόδειξης, και να προτάξουμε την απόδειξη της. Τέτοια αποτελέσματα τα ονομάζουμε λήμματα. Αντιθέτως, πόρισμα είναι ένα αποτέλεσμα που έπεται ενός άλλου αποτελέσματος από το οποίο αποδεικνύεται άμεσα.

Έχουμε αρκετές γνώσεις για τους φυσικούς αριθμούς. Για να τους μελετήσουμε αξιωματικά θα πρέπει να επιλέξουμε κάποιες ιδιότητες της αριθμητικής ως βασικά αξιώματα, και πάνω σε αυτά να οικοδομήσουμε όλη τη θεωρία, χρησιμοποιώντας τις αποδεικτικές διαδικασίες. Βεβαίως μπορούμε να χρησιμοποιήσουμε τη διαισθητική γνώση της αριθμητικής που έχουμε για να μας καθοδηγήσει στη αξιωματική μελέτη.

Στο επόμενο κεφάλαιο θα εξετάσουμε με αυτόν τον τρόπο τους φυσικούς αριθμούς. Σε άλλα μαθήματα, θεωρώντας δεδομένα τα αποτελέσματα για τους φυσικούς αριθμούς, θα εξετάσουμε άλλα αριθμητικά συστήματα.

Ασκήσεις

Άσκηση 5.1 Θα αποδείξουμε, με εις άτοπο απαγωγή, οτι 1 είναι ο μεγαλύτερος ακέραιος. Βρείτε το λάθος!

Απόδειξη. Υποθέτουμε οτι ο 1 δεν είναι μεγαλύτερος ακέραιος. Εστω n ο μεγαλύτερος ακέραιος. Τότε $n > 1$. Τότε n^2 είναι επίσης ακέραιος, και $n^2 = n \cdot n > n \cdot 1 = n$. Αρα $n^2 > n$, που αντιφάσκει με την υπόθεση οτι n ειναι ο μεγαλύτερος ακέραιος. Αρα 1 είναι ο μεγαλύτερος ακέραιος.

Άσκηση 5.2 Αποδείξτε με εις άτοπο απαγωγή οτι:

Εάν $x, y \in \mathbb{R}$ και $y \leq x + \varepsilon$ για κάθε $\varepsilon > 0, \varepsilon \in \mathbb{R}$, τότε $y \leq x$.

α'. Γράψτε την απόδειξη σε στρωτά μαθηματικά ελληνικά.

β'. Διατυπώστε την πρόταση σε τυπική γλώσσα, και αποδείξτε οτι η άρνηση της πρότασης συνεπάγεται μία αντίφαση.

Κεφάλαιο 6

Οι Φυσικοί Αριθμοί

Απόδειξη με επαγωγή

Η απόδειξη με επαγωγή δεν φαίνεται να ταιριάζει στο σχήμα που περιγράψαμε στο Κεφάλαιο 5. Ας δούμε ένα παράδειγμα.

Πρόταση 6.1 *Το άθροισμα των φυσικών αριθμών από το 1 έως το n είναι $\frac{1}{2}n(n+1)$.*

Απόδειξη. Για $n = 1$, το άθροισμα είναι απλώς 1, και είναι πράγματι ίσο με $\frac{1}{2}1(1+1)$.
Εάν αληθεύει για το k, δηλαδή εάν

$$1 + 2 + 3 + \cdots + k = \frac{1}{2}k(k+1)\,,$$

τότε, προσθέτοντας $k+1$ και στις δύο πλευρές έχουμε

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{1}{2}k(k+1) + (k+1) \\ &= \frac{1}{2}(k^2 + 3k + 2) \\ &= \frac{1}{2}(k+1)(k+2) \end{aligned}$$

Αρα ο τύπος αληθεύει για $k+1$. Επαγωγικά, ο τύπος αληθεύει για κάθε φυσικό αριθμό. □

Σε πολλούς ανθρώπους αυτό το επιχείρημα μοιάζει να βασίζεται σε ένα ‘και ούτω καθ'εξής’: αφού εξασφαλίσουμε την αλήθεια της πρότασης για $n = 1$, και το γενικό βήμα από το k στο $k+1$, εφαρμόζουμε αυτό το βήμα με $k = 1$, για να πάμε από 1 στο 2, κατόπιν το εφαρμόζουμε ξανά για να πάμε από το 2 στο 3, *και ούτω καθ'εξής*, όσες φορές θέλουμε. Για παράδειγμα, μετά από 592 εφαρμογές του γενικού βήματος θα φθάναμε το 593. Βεβαίως για να φθάσουμε μεγάλες τιμές του n απαιτούνται πολλές επαναλήψεις του γενικού βήματος. Το πρόβλημα είναι οτι με αυτόν τον τρόπο δεν είναι δυνατόν να καλύψουμε ποτέ όλους τους φυσικούς αριθμούς με μια απόδειξη πεπερασμένου μήκους

$$L_1,\, L_2,\, \ldots,\, L_m\,.$$

Η λύση σε αυτό το πρόβλημα είναι να βγάλουμε το ‘και ούτω καθ'εξής’ από την απόδειξη και να το τοποθετήσουμε στον ίδιο τον ορισμό των φυσικών αριθμών. Τότε η απόδειξη με επαγωγή θα ταιριάζει με το σχήμα που περιγράψαμε στο προηγούμενο κεφάλαιο.

Οι φυσικοί αριθμοί

Δεν είναι δυνατόν να περιγράψουμε το σύνολο των φυσικών αριθμών καταγράφοντας ένα–ένα όλα τα στοιχεία του. Χρειάζεται μια διαφορετική προσέγγιση. Ευτυχώς, η διαισθητική έννοια της απαρίθμησης εύκολα μπορεί να εκφραστεί με συνολοθεωρητικό τρόπο. Αρχίζουμε με το 1, μετά είναι το 2, μετά το 3, και συνεχίζουμε με αυτόν τον τρόπο, ονομάζοντας κάθε φορά τον επόμενο φυσικό αριθμό, όσο θέλουμε. Για αν συλλάβουμε όλη αυτήν τη διαδικασία της απαρίθμησης σε μια έννοια, θεωρούμε τον επόμενο αριθμό σαν μια συνάρτηση στο σύνολο $\mathbb{N}$,

$$\varepsilon : \mathbb{N} \to \mathbb{N}$$

με κατάλληλες ιδιότητες, ώστε $\varepsilon(n)$ να είναι ο επόμενος φυσικός, $\varepsilon(1) = 2$, $\varepsilon(2) = 3$, κλπ. Δύο προφανείς ιδιότητες είναι

- ε δεν είναι επεικόνιση επί του $\mathbb{N}$, αφού $\varepsilon(n) \neq 1$ για κάθε $n \in \mathbb{N}$.
- ε είναι ενεικόνιση, δηλαδή $m \neq n$ συνεπάγεται $\varepsilon(m) \neq \varepsilon(n)$.

Υπάρχει μια τρίτη σημαντική ιδιότητα, που επιτρέπει τις αποδείξεις με επαγωγή.

- Υποθέτουμε οτι $S \subseteq \mathbb{N}$ είναι τέτοιο ώστε $1 \in S$, και για κάθε $n \in \mathbb{N}$, εάν $n \in S$ τότε $\varepsilon(n) \in S$. Τότε $S = \mathbb{N}$.

Δηλαδή, εάν ένα σύνολο περιέχει το 1, και περιέχει το $\varepsilon(n)$ κάθε φορά που περιέχει το n, τότε το σύνολο καλύπτει όλους τους φυσικούς αριθμούς.

Είναι εντυπωσιακό οτι αυτές οι τρεις ιδιότητες αρκούν για να περιγράψουμε τους φυσικούς αριθμούς. Για μια αξιωματική προσέγγιση της Αριθμητικής αρκεί να απαιτήσουμε την ύπαρξη ενός συνόλου με τις τρεις αυτές ιδιότητες. Για πρακτικούς λόγους είναι συχνά προτιμότερο να αρχίσουμε με το 0 αντί το 1. Οταν χρησιμοποιούμε τους φυσικούς αριθμούς για να εκφράσουμε διάταξη, για παράδειγμα ως δείκτες σε μία ακολουθία, είναι πιο κατάλληλο το $\mathbb{N}$, χωρίς το 0. Αν όμως θέλουμε οι φυσικοί αριθμοί να εκφράζουν το πλήθος στοιχείων των πεπερασμένων συνόλων, τότε πιο βολικό είναι να έχουμε και το 0 ως φυσικό αριθμό, καθώς αυτό εκφράζει το πλήθος στοιχείων του $\varnothing$. Στην αριθμητική επίσης είναι χρήσιμο να έχουμε το στοιχείο 0. Γι'αυτούς και άλλους λόγους θα αρχίσουμε με το 0 στο αξιωματικό μας σύστημα, και θα χρησιμοποιήσουμε το σύμβολο $\mathbb{N}_0$ για να δηλώσουμε το σύνολο των φυσικών αριθμών που περιέχει το 0.

Εχουμε τα *αξιώματα Peano* για τους φυσικούς αριθμούς, από τον Ιταλό μαθηματικό που ανέπτυξε αυτήν την προσέγγιση των φυσικών αριθμών στο τέλος του 19ου αιώνα.

Θεωρούμε ένα σύνολο $\mathbb{N}_0$ και μια συνάρτηση $\varepsilon : \mathbb{N}_0 \to \mathbb{N}_0$ τέτοια ώστε:

(Φ1) Η συνάρτηση ε δεν είναι επεικόνιση επί του $\mathbb{N}_0$: υπάρχει στοιχείο $0 \in \mathbb{N}_0$ τέτοιο ώστε, για κάθε $n \in \mathbb{N}_0$, $\varepsilon(n) \neq 0$.

(Φ2) Η συνάρτηση ε είναι ενεικονική: εάν $\varepsilon(m) = \varepsilon(n)$ τότε $m = n$.

(Φ3) Εάν $S \subseteq \mathbb{N}_0$ είναι τέτοιο ώστε $0 \in S$ και για κάθε $n \in \mathbb{N}_0$:

$$(n \in S \Rightarrow \varepsilon(n) \in S)$$

τότε $S = \mathbb{N}_0$.

Δεν προκύπτει οτι υπάρχει ένα τέτοιο σύνολο $\mathbb{N}_0$, και πρέπει να θεωρήσουμε την ύπαρξή του ως ένα από τα βασικά αξιώματα των μαθηματικών μας.

Αξίωμα ύπαρξης των Φυσικών Αριθμών
Υπάρχει ένα σύνολο $\mathbb{N}_0$ και μια συνάρτηση $\varepsilon : \mathbb{N}_0 \to \mathbb{N}_0$ που ικανοποιούν τα αξιώματα ($\Phi 1$), ($\Phi 2$), ($\Phi 3$).

Από αυτά τα αξιώματα μπορούμε να αποδείξουμε όλα τα αποτελέσματα της αριθμητικής, να κατασκευάσουμε τους ακεραίους, τους ρητούς, τους πραγματικούς και τους μιγαδικούς αριθμούς. Θα δούμε επίσης οτι το αξίωμα ($\Phi 3$), που λέγεται **Αρχή Επαγωγής**, εμπεριέχει τη δυνατότητα απόδειξης με επαγωγή, όπως στο ακόλουθο παράδειγμα.

Πρόταση 6.2 *Εάν $n \in \mathbb{N}_0$, $n \neq 0$, τότε υπάρχει μοναδικό στοιχείο $m \in \mathbb{N}_0$ τέτοιο ώστε $n = \varepsilon(m)$.*

Απόδειξη. Θέτουμε

$$S = \{n \in \mathbb{N}_0 \,|\, n = 0 \text{ ή } n = \varepsilon(m) \text{ για κάποιο } m \in \mathbb{N}_0\}\,.$$

Θα δείξουμε οτι $S = \mathbb{N}_0$. Προφανώς $0 \in S$. Εάν $n \in S$, είτε $n = 0$, οπότε $\varepsilon(n) = \varepsilon(0) \in S$, είτε $n = \varepsilon(m)$ για κάποιο $m \in \mathbb{N}_0$, οπότε $\varepsilon(n) = \varepsilon(\varepsilon(m))$ και εφ'οσον $\varepsilon(m) \in \mathbb{N}_0$, $\varepsilon(n) \in S$. Συνεπώς, από το αξίωμα ($\Phi 3$), $S = \mathbb{N}_0$. Αρα, για κάθε $n \in \mathbb{N}_0 \setminus \{0\}$, υπάρχει $m \in \mathbb{N}_0$ τέτοιο ώστε $\varepsilon(m) = n$. Η μοναδικότητα είναι συνέπεια του αξιώματος ($\Phi 2$).

□

Η Πρόταση 6.2 δείχνει οτι το 0 είναι το μοναδικό στοιχείο που δεν είναι *επόμενο* κάποιου άλλου, μια ιδιότητα που το διακρίνει από όλα τα άλλα στοιχεία του $\mathbb{N}_0$. Ορίζουμε το σύνολο των *φυσικών αριθμών*, $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$. Συμβολίζουμε το $\varepsilon(0)$ με 1. Αυτό το στοιχείο ανήκει στο $\mathbb{N}$.

Η απόδειξη της Πρότασης 6.2 έχει την ακόλουθη δομή: ορίζουμε ένα σύνολο S, και

(α) δείχνουμε οτι $0 \in S$,

(β) δείχνουμε οτι: $n \in S \Rightarrow \varepsilon(n) \in S$,

(γ) επικαλούμαστε το αξίωμα ($\Phi 3$) για να συμπεράνουμε οτι $S = \mathbb{N}_0$.

Μια απόδειξη με επαγωγή έχει πάντα αυτήν τη δομή. Στην πράξη το σύνολο S είναι της μορφής

$$S = \{n \in \mathbb{N}_0 \,|\, P(n)\}$$

όπου $P(n)$ είναι ένα κατηγόρημα που ορίζεται (δηλαδή που είναι αληθές ή ψευδές) για κάθε $n \in \mathbb{N}_0$. Τα βήματα (α), (β), (γ) γίνονται

(αα) δείχνουμε οτι η πρόταση $P(0)$ είναι αληθής,

(ββ) δείχνουμε οτι εάν $P(n)$ είναι αληθής τότε $P(\varepsilon(n))$ είναι αληθής,

(γγ) επικαλούμαστε το αξίωμα ($\Phi 3$) για να συμπεράνουμε οτι $P(n)$ αληθεύει για κάθε $n \in \mathbb{N}_0$.

Η χρήση του αξιώματος (Φ3) ολοκληρώνει την απόδειξη χωρίς να χρειάζεται κανένα 'και ούτω καθ'εξής'. Η βασική δομή αυτής της απόδειξης χρησιμοποιήθηκε στην Πρόταση στην αρχή του Κεφαλαίου, με τη διαφορά οτι αρχίσαμε από το 1 αντί από το 0 και γράψαμε $n+1$ αντί $\varepsilon(n)$. Αργότερα θα δείξουμε οτι η ίδια μέθοδος εφαρμόζεται ξεκινώντας από οποιοδήποτε $k \in \mathbb{N}_0$, ειδικότερα από $k = 1$, και συνεπώς η Πρόταση στην αρχή του Κεφαλαίου είναι ένα απλό παράδειγμα απόδειξης με επαγωγή, βασισμένη στο αξίωμα (Φ3).

Στην πράξη το αξίωμα (Φ3) δεν αναφέρεται ρητά. Η απόδειξη διατυπώνεται σε σχέση με ένα κατηγόρημα $P(n)$, και όταν αποδειχθούν τα βήματα (αα) και (ββ), λέμε οτι 'με επαγωγή, το $P(n)$ αληθεύει για όλα τα n'. Αυτή η διατύπωση είναι μια αναφορά στο αξίωμα (Φ3), που ονομάζεται, γι'αυτόν το λόγο, *αξίωμα επαγωγής*. Κατά τη διάρκεια της απόδειξης, η υπόθεση οτι $P(n)$ αληθεύει ονομάζεται *επαγωγική υπόθεση* και η απόδειξη οτι $P(n) \Rightarrow P(\varepsilon(n))$ ονομάζεται *επαγωγικό βήμα*. Στην αρχή, όταν μελετάμε τις βασικές ιδιότητες του $\mathbb{N}_0$ θα αναφερόμαστε ρητά στο σύνολο S.

Αναδρομικοί ορισμοί

Θέλουμε να ορίσουμε την πρόσθεση φυσικών αριθμών ξεκινώντας από την έννοια του επομένου. Για κάθε $m \in \mathbb{N}_0$ θέτουμε

$$m + 0 = m$$

και κατόπιν ορίζουμε $m + \varepsilon(n)$ χρησιμοποιώντας το $m + n$ και θέτοντας

$$m + \varepsilon(n) = \varepsilon(m + n)\,.$$

Το αξίωμα επαγωγής φαίνεται να ταιριάζει σε μια τέτοια διαδικασία. Πράγματι, το επόμενο θεώρημα εξασφαλίζει οτι μπορούμε να ορίσουμε συναρτήσεις με μια τέτοια αναδρομική διαδικασία.

Θεώρημα 6.3 (Θεώρημα Αναδρομής) *Εάν X είναι ένα σύνολο, $f : X \to X$ μια συνάρτηση, και $c \in X$, τότε υπάρχει μοναδική συνάρτηση $\varphi : \mathbb{N}_0 \to X$ τέτοια ώστε*

α΄. $\varphi(0) = c$,

β΄. $\varphi(\varepsilon(n)) = f(\varphi(n))$ *για κάθε* $n \in \mathbb{N}_0$.

Υπενθυμίζουμε οτι από τη σκοπιά της θεωρίας συνόλων μια συνάρτηση $\varphi : \mathbb{N}_0 \to X$ είναι ένα υποσύνολο $\varphi \subseteq \mathbb{N}_0 \times X$ με τις ιδιότητες

i. Για κάθε $n \in \mathbb{N}_0$, υπάρχει $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$,

ii. Εάν (n, x) και $(n, y) \in \varphi$, τότε $x = y$.

Αρα για να ορίσουμε τη συνάρτηση φ αρκεί να προσδιορίσουμε το κατάλληλο υποσύνολο. Οι ιδιότητες της φ στη διατύπωση του Θεωρήματος σημαίνουν οτι αυτό το υποσύνολο πρέπει να ικανοποιεί

Α΄. $(0, c) \in \varphi$,

Β΄. Εάν $(n, x) \in \varphi$ τότε και $(\varepsilon(n), f(x)) \in \varphi$.

Υπάρχουν πολλά υποσύνολα με αυτές τις ιδιότητες, όπως για παράδειγμα όλο το $\mathbb{N}_0 \times X$. Το ζητούμενο είναι η τομή όλων αυτών των υποσυνόλων, γιατί μόνον αυτή θα ικανοποιεί τις ιδιότητες (i) και (ii).

Η απόδειξη του Θεωρήματος Αναδρομής δίδεται στο Παράρτημα, στο τέλος του Κεφαλαίου.

Σαν εφαρμογή του Θεωρήματος Αναδρομής δίδουμε τους ακόλουθους ορισμούς:

1. *Πρόσθεση*
   Ορίζουμε τη συνάρτηση $\varphi_m : \mathbb{N}_0 \to \mathbb{N}_0$, $\varphi_m(n) = m + n$ αναδρομικά με
   $$\begin{aligned} \varphi_m(0) &= m \\ \varphi_m(\varepsilon(n)) &= \varepsilon(\varphi_m(n)) \,. \end{aligned}$$
   Σε αυτήν την περίπτωση, $c = m$, $f = \varepsilon$.

2. *Πολλαπλασιασμός*
   Ορίζουμε τη συνάρτηση $\mu_m : \mathbb{N}_0 \to \mathbb{N}_0$, $\mu_m(n) = mn$ αναδρομικά με
   $$\begin{aligned} \mu_m(0) &= 0 \\ \mu_m(\varepsilon(n)) &= \mu_m(n) + m \,. \end{aligned}$$
   Εδώ $c = 0$, $f(r) = r + m$.

3. *Δυνάμεις*
   Ορίζουμε $\pi_m : \mathbb{N}_0 \to \mathbb{N}_0$, $\pi_m(n) = m^n$ με
   $$\begin{aligned} \pi_m(0) &= 1 \\ \pi_m(\varepsilon(n)) &= m\pi_m(n) \,. \end{aligned}$$
   Εδώ $c = 1$, $f(r) = rm$.

4. *Επαναλαμβανόμενη σύνθεση*
   μιας συνάρτησης $f : X \to X$, ορίζεται με
   $$\begin{aligned} f^0(x) &= x \\ f^{\varepsilon(n)}(x) &= f(f^n(x)) \text{ για όλα τα } x \in X. \end{aligned}$$

Οι κανόνες της Αριθμητικής

Εχοντας ορίσει την πρόσθεση και τον πολλαπλασιασμό, είναι τώρα σχετικά απλό να αποδείξουμε τους συνηθισμένους κανόνες της αριθμητικής. Οι αποδείξεις δεν είναι εντελώς τετριμμένες: η κύρια δυσκολία βρίσκεται στην εύρεση της καταλληλότερης σειράς με την οποία να γίνουν οι αποδείξεις. Σε κάθε περίπτωση το κύριο εργαλείο είναι η επαγωγή.

Υπενθυμίζουμε τους ορισμούς:

$$\begin{array}{llll} (\text{πρ}1) & m + 0 = m \,, & (\text{πρ}2) & m + \varepsilon(n) = \varepsilon(m + n) \,, \\ (\text{πλ}1) & m0 = 0 \,, & (\text{πλ}2) & m\varepsilon(n) = mn + m \,. \end{array}$$

Από τα (πρ2) και (πρ1) βλέπουμε οτι $m + \varepsilon(0) = \varepsilon(m + 0) = \varepsilon(m)$. Συμβολίζουμε το $\varepsilon(0)$ με 1, άρα έχουμε $\varepsilon(m) = m + 1$.

Λήμμα 6.4 *Για κάθε* $m \in \mathbb{N}_0$,

1. $0 + m = m$,
2. $1 + m = \varepsilon(m)$,
3. $0m = 0$,
4. $1m = m$.

Απόδειξη. Σε κάθε περίπτωση χρησιμοποιούμε επαγωγή στο m. Δίδουμε για παράδειγμα την απόδειξη του (1). Θέτουμε

$$S = \{m \in \mathbb{N}_0 \,|\, 0 + m = m\} .$$

Προφανώς, από το (πρ1), $0 \in S$. Εάν $m \in S$, τότε $0 + m = m$, άρα από την (πρ2), $0 + \varepsilon(m) = \varepsilon(0 + m) = \varepsilon(m)$. Συνεπώς $\varepsilon(m) \in S$, και από το (Φ3), $S = \mathbb{N}_0$.

□

Θεώρημα 6.5 (Κανόνες της αριθμητικής) *Για όλα τα* m, n, $p \in \mathbb{N}_0$,

1. *Προσεταιριστική ιδιότητα της πρόσθεσης:*
$$(m + n) + p = m + (n + p) ,$$
2. *Μεταθετική ιδιότητα της πρόσθεσης:*
$$m + n = n + m ,$$
3. *Προσεταιριστική ιδιότητα του πολλαπλασιασμού:*
$$(mn)p = m(np) ,$$
4. *Μεταθετική ιδιότητα του πολλαπλασιασμού:*
$$mn = nm ,$$
5. *Επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση:*
$$m(n + p) = mn + mp .$$

Η απόδειξη των κανόνων της αριθμητικής δίδεται στο Παράρτημα.

Αφού έχουμε αποδείξει αυτά τα θεμελιώδη αποτελέσματα, μπορούμε να εφαρμόζουμε ελεύθερα τους κανόνες της αριθμητικής από εδώ και πέρα. Πρώτα, αντικαθιστούμε το $\varepsilon(n)$ με το $n + 1$. Ετσι το αξίωμα επαγωγής (Φ3) παίρνει την πιο συνηθισμένη μορφή

$$\text{Εάν } S \subseteq \mathbb{N}_0,\ 0 \in S \text{ και } (n \in S \Rightarrow n + 1 \in S), \text{ τότε } S = \mathbb{N}_0,$$

ενώ το αξίωμα (Φ2) γίνεται

$$m + 1 = n + 1 \Rightarrow m = n ,$$

και αυτό μπορεί να επεκταθεί επαγωγικά, όπως στην ακόλουθη Πρόταση.

Πρόταση 6.6 *Για κάθε* m, n, $q \in \mathbb{N}_0$,

1. $m + q = n + q \;\Rightarrow\; m = n$
2. $q \neq 0$, $mq = nq \;\Rightarrow\; m = n$.

Απόδειξη. Για να αποδείξουμε το (1) χρησιμοποιούμε επαγωγή στο q. Θέτουμε

$$S = \{q \in \mathbb{N}_0 \,|\, m + q = n + q \Rightarrow m = n\}\,.$$

Προφανώς $0 \in S$. Εάν $q \in S$, υποθέτουμε οτι

$$m + (q + 1) = n + (q + 1)$$

και τότε, από το Θεώρημα 6.5,

$$(m + q) + 1 = (n + q) + 1$$

και από το (Φ2)

$$m + q = n + q$$

και εφ'οσον $q \in S$,

$$m = n\,.$$

Συνεπώς $q + 1 \in S$, και επαγωγικά $S = \mathbb{N}_0$.

Για το (2) θέτουμε

$$S = \{m \in N_0 \,|\, q \neq 0,\, mq = nq \Rightarrow m = n\}\,.$$

Για να δείξουμε οτι $0 \in S$, υποθέτουμε οτι $q \neq 0$, και

$$nq = 0q = 0\,.$$

Τότε $q = p+1$ για κάποιο p. Εάν $n \neq 0$ τότε $n = r+1$ για κάποιο r, και $nq = (pr+p+r)+1$ άρα δεν είναι 0. Συνεπώς $n = 0$, και $0 \in S$.

Τώρα υποθέτουμε οτι $m \in S$, και $q \neq 0$, ενώ

$$(m + 1)q = nq\,.$$

Οπως προηγουμένως, $n \neq 0$, άρα $n = r + 1$ για κάποιο $r \in N_0$. Τότε $mq + q = rq + q$. Από το (1) έχουμε οτι $mq = rq$, και από την επαγωγική υπόθεση $m = r$. Δηλαδή $m + 1 = n$, που ολοκληρώνει την απόδειξη.

□

Τώρα μπορούμε να αναφερθούμε στην *αφαίρεση*. Υποθέτουμε οτι $p = r + q$. Από την Πρόταση 6.6, το r προσδιορίζεται με μοναδικό τρόπο από τα p και q, και συνεπώς μπορούμε να το συμβολίζουμε $p - q$. Για οποιαδήποτε m, $n \in \mathbb{N}_0$ ορίζουμε τη σχέση $\geq$ με

$$m \geq n \;\text{ σημαίνει }\; \exists r \in \mathbb{N}_0\,(m = r + n)\,.$$

Για δεδομένα m, $n \in \mathbb{N}_0$, η *διαφορά* $m - n$ ορίζεται μόνον όταν $m \geq n$. Μπορούμε εύκολα να επαληθεύσουμε διάφορους κανόνες της αφαίρεσης, όπως

$$\begin{aligned} m - (n - r) &= (m - n) + r \qquad && \text{όταν } m \geq n \geq r\,,\\ m + (n - r) &= (m + n) - r && \text{όταν } n \geq r\,,\\ m(n - r) &= mn - mr && \text{όταν } n \geq r\,. \end{aligned}$$

Για τον τελευταίο, για παράδειγμα, εφ'οσον $n \geq r$, γράφουμε $n = s + r$, και έχουμε

$$mn = m(s + r) = ms + mr\,.$$

Από τον ορισμό,

$$mn - mr = ms = m(n - r)$$

εφ'οσον $s = n - r$.

Μπορούμε επίσης να εξετάσουμε τη διαίρεση, και στην περίπτωση που $m = rn$, $(n \neq 0)$ να συμβολίσουμε το r με m/n.

Η διάταξη των φυσικών αριθμών

Εχουμε ήδη ορίσει τη σχέση $\geq$ στο $\mathbb{N}_0$. Οι άλλες σχέσεις διάταξης ορίζονται ως εξής:

$$\begin{aligned} m > n &\iff m \geq n \text{ και } m \neq n, \\ m \leq n &\iff n \geq m, \\ m < n &\iff n > m \end{aligned}$$

Θέλουμε να δείξουμε οτι αυτές είναι πράγματι σχέσεις διάταξης, με την έννοια του Κεφαλαίου 2. Δείχνουμε πρώτα οτι η σχέση $\geq$ είναι μεταβατική, (ΑΔ1), και αντισυμμετρική, (ΑΔ3).

Πρόταση 6.7 *$m \geq n$, $n \geq p \Rightarrow m \geq p$ γιά κάθε m, n, $p \in \mathbb{N}_0$.*

Απόδειξη. Υπάρχουν r και s στο $\mathbb{N}_0$ τέτοια ώστε $m = r + n$ και $n = s + p$. Αρα $m = r + (s + p) = (r + s) + p$, και συνεπώς $m \geq p$.

□

Πρόταση 6.8 *Εάν m, $n \in \mathbb{N}_0$ και $m \geq n$, $n \geq m$, τότε $m = n$.*

Απόδειξη. Υπάρχουν r, $t \in \mathbb{N}_0$ τέτοια ώστε $m = r + n$, $n = t + m$, άρα $m = r + t + m$. Από τη Πρόταση 6.6 (1), $r + t = 0$. Εάν $t \neq 0$, τότε $t = q + 1$ για κάποιο $q \in N_0$ από την Πρόταση 6.2, και τότε $0 = (r + q) + 1$, το οποίο αντιφάσκει προς το Αξίωμα Φ1. Αρα $t = 0$ και συνεπώς $n = m$.

□

Η απόδειξη οτι η σχέση $\geq$ ικανοποιεί την ιδιότητα (ΑΔ2) μίας ασθενούς διάταξης είναι πιο πολύπλοκη, και την αφήνουμε για αργότερα. Είναι πάντως εύκολο να ελέγξουμε οτι η σχέση $\geq$ συμπεριφέρεται καλά ως προς τις αριθμητικές πράξεις στο $\mathbb{N}_0$.

Πρόταση 6.9 *Για όλα τα m, n, p, $q \in \mathbb{N}_0$,*

1. *Εάν $m \geq n$, $p \geq q$, τότε $m + p \geq n + q$.*
2. *Εάν $m \geq n$, $p \geq q$, τότε $mp \geq nq$.*

Απόδειξη. Για το (1), παρατηρούμε οτι υπάρχουν r, $s \in \mathbb{N}_0$, τέτοια ώστε $m = r + n$, $p = s + q$. Αρα, μετά από απλοποίηση, βρίσκουμε οτι $m + p = (r + s) + (n + q)$. Για το (2), παρόμοια, $mp = nq + (rs + ns + rq)$.

□

Το 0 είναι το μικρότερο στοιχείο του $\mathbb{N}_0$, με την ακόλουθη έννοια:

Λήμμα 6.10 *Εάν $m \in \mathbb{N}_0$, τότε $m \geq 0$.*

Απόδειξη. $m = m + 0$.

□

Το 1 είναι το επόμενο μικρότερο:

Λήμμα 6.11 *Εάν $m \in \mathbb{N}_0$ και $m > 0$, τότε $m \geq 1$.*

Απόδειξη. Εάν $m \neq 0$, τότε $m = q + 1$ για κάποιο $q \in \mathbb{N}_0$. Αρα $m \geq 1$.

□

Γενικότερα, ισχύει το ακόλουθο:

Πρόταση 6.12 *Εάν $m, n \in \mathbb{N}_0$ και $m > n$, τότε $m \geq n + 1$.*

Απόδειξη. Εχουμε $m = r + n$ για κάποιο $r \in \mathbb{N}_0$, και $r \neq 0$, εφόσον $m \neq n$. Αρα $r = q + 1$ για κάποιο $q \in \mathbb{N}_0$, και $m = q + (n + 1)$, δηλαδή $m \geq n + 1$.

□

Τώρα μπορούμε να ολοκληρώσουμε την απόδειξη οτι $\geq$ είναι μία σχέση διάταξης:

Πρόταση 6.13 *Η σχέση $\geq$ είναι σχέση ασθενούς διάταξης στο $\mathbb{N}_0$.*

Απόδειξη. Από τον ορισμό της ασθενούς διάταξης, πρέπει να αποδείξουμε οτι για όλα τα $m, n, p \in \mathbb{N}_0$

(ΑΔ1) $m \geq n$ και $n \geq p$ συνεπάγονται $m \geq p$,

(ΑΔ2) Για κάθε δύο στοιχεία m και n του $\mathbb{N}_0$, ισχύει ένα από τα $m \geq n$ ή $n \geq m$, ή και τα δύο,

(ΑΔ3) $m \geq n$ και $n \geq m$ συνεπάγονται $m = n$.

Εχουμε ήδη αποδείξει οτι ισχύουν τα (ΑΔ1) και (ΑΔ3), στις Προτάσεις 6.7 και 6.8. Για να αποδείξουμε το (ΑΔ2) θεωρούμε το σύνολο

$$S(m) = \{n \in \mathbb{N}_0 \,|\, m \geq n \text{ ή } n \geq m\}\,.$$

Στοχεύουμε να δείξουμε οτι $S(m) = \mathbb{N}_0$ για κάθε $m \in \mathbb{N}_0$. Για οποιοδήποτε δοθέν m, έχουμε $0 \in S(m)$, εφόσον $m \geq 0$. Υποθέτουμε οτι $n \in S(m)$. Τότε είτε $m \geq n$ είτε $n \geq m$. Εάν $n \geq m$ τότε $n + 1 \geq m$. Εάν $m \geq n$ τότε είτε $m = n$ και $n + 1 \geq m$, είτε $m > n$ οπότε $m \geq n + 1$ από την Πρόταση 6.12. Σε κάθε περίπτωση, $n + 1 \in S(m)$ και από επαγωγή $S(m) = \mathbb{N}_0$.

□

Από τα αποτελέσματα του Κεφαλαίου 2, έπεται οτι $>$ είναι σχέση γνήσιας διάταξης: ικανοποιεί τη μεταβατική ιδιότητα

$$m > n \text{ και } n > p \Rightarrow m > p$$

και την τριχοτομία

$$\text{Αληθεύει ακριβώς ένα από τα } m > n,\ m = m,\ n > m\,.$$

Η ακόλουθη Πρόταση είναι σχεδόν το αντίστροφο της Πρότασης 6.6.

Πρόταση 6.14 *Για όλα τα m, n, $q \in \mathbb{N}_0$,*

1. $m + q > n + q \Rightarrow m > n$

2. $q \neq 0$, $mq > nq \Rightarrow m > n$.

Απόδειξη. Εάν $m \not> n$, τότε από την τριχοτομία $m \leq n$. Αλλά $m \leq n$ συνεπάγεται οτι $m + q \leq n + q$ από την Πρόταση 6.9. Αυτό αντιφάσκει προς την υπόθεση, και αποδεικνύει το πρώτο μέρος. Το δεύτερο μέρος αποδεικνύεται με παρόμοιο τρόπο.

□

Εάν στην Πρόταση 6.14 αντικαταστήσουμε τη σχέση $>$ με τη $\geq$, έχουμε ακριβώς το αντίστροφο της Πρότασης 6.6, το οποίο αληθεύει.

Αλλες μορφές επαγωγής

Σε μερικές περιπτώσεις, η υπόθεση οτι αληθεύει η $P(n)$ δεν αρκεί για να αποδείξουμε την $P(n+1)$. Μπορεί να χρειάζεται η υπόθεση οτι όλες οι προτάσεις $P(0)$, $P(1)$, …, $P(n)$ αληθεύουν. Σε αυτήν την περίπτωση ανατρέχουμε στη λεγόμενη 'Ισχυρή μορφή της Αρχής Επαγωγής'.

- Εάν η υπόθεση οτι αληθεύουν οι $P(m)$ για κάθε $m < n$, συνεπάγεται οτι η $P(n)$ αληθεύει,

- Τότε η $P(n)$ αληθεύει για κάθε $n \in \mathbb{N}_0$.

Αρχικά φαίνεται οτι αυτό αποτελεί μια ουσιαστική γενίκευση της Αρχής της Επαγωγής, αλλά εάν θεωρήσουμε το κατηγόρημα

$$Q(n): \text{ για κάθε } m \in \mathbb{N}_0, \text{ τέτοιο ώστε } m \leq n, \text{ αληθεύει η } P(m)$$

βλέπουμε οτι η 'Ισχυρή μορφή της Αρχής Επαγωγής' γίνεται

$Q(0)$ αληθεύει

Εάν αληθεύει η $Q(n)$ τότε αληθεύει η $Q(n+1)$.

Αρα η Ισχυρή μορφή της Αρχής Επαγωγής είναι απλώς επαγωγή για το κατηγόρημα Q, και θεωρητικά δεν είναι πιό γενική από την επαγωγή. Στην πράξη συχνά βοηθάει να απλοποιήσουμε αποδείξεις. Τη χρησιμοποιούμε για να αποδείξουμε μια άλλη σημαντική ιδιότητα των φυσικών αριθμών, που μπορεί να χρησιμοποιηθεί εναλλακτικά προς την Αρχή της Επαγωγής.

Θεώρημα 6.15 (Αρχή Ελαχίστου) *Κάθε μη κενό υποσύνολο του $\mathbb{N}_0$ έχει ένα ελάχιστο στοιχείο, δηλαδή ένα στοιχείο που ανήκει στο υποσύνολο αυτό και είναι μικρότερο ή ίσο από κάθε άλλο στοιχείο του υποσυνόλου.*

Απόδειξη. Πρέπει να δείξουμε οτι εάν $S \subseteq \mathbb{N}_0$, $S \neq \varnothing$, τότε υπάρχει $a \in S$ τέτοιο ώστε για κάθε $s \in S$, ισχύει $a \leq s$.

Υποθέτουμε οτι δεν υπάρχει τέτοιο a και καταλήγουμε σε αντίφαση. Θεωρούμε το κατηγόρημα $P(n): n \notin S$. Τότε $P(0)$ είναι αληθές: εάν $0 \in S$ τότε το 0 είναι το ελάχιστο στοιχείο του S, αλλά υποθέσαμε οτι δεν υπάρχει ελάχιστο στοιχείο του S, άρα $0 \notin S$.

Υποθέτουμε οτι $P(m)$ αληθεύει για κάθε $m \leq n$, δηλαδή εάν $m \leq n$ τότε $m \notin S$. Εάν $s \in S$ τότε $s > n$, άρα $s \geq n+1$. Εάν $n+1 \in S$ τότε $n+1$ είναι το ελάχιστο στοιχείο του S. Από την υπόθεση έχουμε οτι $n+1 \notin S$, και συνεπώς $P(n+1)$ αληθεύει. Από την Ισχυρή μορφή της Αρχής Επαγωγής, $P(n)$ αληθεύει για κάθε $n \in \mathbb{N}_0$, άρα $S = \varnothing$. Αυτό αντιφάσκει προς τις υποθέσεις του Θεωρήματος. Αρα υπάρχει ελάχιστο στοιχείο στο S.

□

Διαιρετότητα

Εάν m, $n \in \mathbb{N}_0$ και $n \neq 0$, δεν είναι δυνατό να διαιρέσουμε το m με το n και να πάρουμε ένα φυσικό αριθμό. Αυτό συμβαινει μόνον εάν m είναι πολλαπλάσιο του n, δηλαδή εάν $m = qn$ για κάποιο $q \in \mathbb{N}_0$. Εάν δεν ισχύει αυτό, τότε η διαδικασία της διαίρεσης αφήνει υπόλοιπο.

Θεώρημα 6.16 (Αλγόριθμος διαίρεσης) *Εάν m, $n \in \mathbb{N}_0$ και $n \neq 0$, τότε υπάρχουν μοναδικοί φυσικοί αριθμοί, q, $r \in \mathbb{N}_0$, τέτοιοι ώστε $m = qn + r$ και $r < n$.*

Απόδειξη. Εφαρμόζουμε επαγωγη στο m. Έστω

$$S = \{m \in \mathbb{N}_0 \,:\, m = qn + r \text{ με } q,\, r \in \mathbb{N}_0,\, r < n\}\,.$$

Αφού $0 = 0n + 0$, ισχύει $0 \in S$.

Υποθέτουμε $m \in S$. Τότε $m = qn + r$, με $r < n$, και

$$m + 1 = qn + r + 1\,.$$

Αφού $r < n$, ισχύει $r + 1 \leq n$. Εάν $r + 1 = n$, τότε

$$m + 1 = (q + 1)n + 0\,,$$

ενώ εάν $r + 1 < n$, τότε

$$m + 1 = qn + (r + 1) \quad \text{με} \quad r + 1 < n\,.$$

Σε κάθε περίπτωση, $m + 1 \in S$ και, επαγωγικά, $S = N_0$.

Για να δείξουμε οτι q και r είναι μοναδικοί, υποθέτουμε οτι

$$m = qn + r = q'n + r' \quad \text{με} \quad r < n \text{ και } r' < n\,.$$

Τότε

$$qn \leq m < (q + 1)n\,,$$

$$qn' \leq m < (q' + 1)n\,.$$

Από μεταβατικότητα της διάταξης, $qn < (q' + 1)n$, από την Πρόταση 6.14, $q < q' + 1$ και συνεπώς από την Πρόταση 6.12 $q \leq q'$. Αλλά ισχύει επίσης $q'n < (q + 1)n$ και συνεπώς $q' \leq q$. Άρα $q = q'$, και από την Πρόταση 6.6, $r = r'$.

□

Παραγοντοποίηση

Τώρα μπορούμε να ασχοληθούμε με την παραγοντοποίηση σε πρώτους αριθμούς, και ειδικότερα να αποδείξουμε τη μοναδικότητα. Στο υπόλοιπο αυτού του Κεφαλαίου, θα ασχοληθούμε μόνο με μη μηδενικούς φυσικούς αριθμούς, και θα εργαζόμαστε στο $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$. Αρχίζουμε με κάποιους βασικούς ορισμούς.

Λέμε οτι $k \in \mathbb{N}$ είναι **παράγοντας** ή **διαιρέτης** του $m \in \mathbb{N}$, και το συμβολίζουμε $k|m$, εάν υπάρχει $s \in \mathbb{N}$ τέτοιος ώστε $m = ks$. Το 1 και το m είναι τετριμμένα διαιρέτες του m. Κάθε άλλος διαιρέτης ονομάζεται **γνήσιος διαιρέτης**. Ονομάζουμε έναν αριθμό m **πρώτο** εάν $m > 1$ και ο m δεν έχει γνήσιους διαιρέτες. (Είναι πιο βολικό να μην θεωρούμε τον 1 πρώτο, όπως θα δούμε, για παράδειγμα, στο θεώρημα Μοναδικής Παραγοντοποίησης.) Εύκολα βλέπουμε οτι ένας διαιρέτης k του m πρέπει να ικανοποιεί $1 \leq k \leq m$: εάν $k > m$, τότε, αφού $s \geq 1$, έχουμε $ks > m$. Άρα ένας γνήσιος διαιρέτης k ικανοποιεί $1 < k < m$.

Πρόταση 6.17 *Κάθε φυσικός αριθμός $m > 1$ είναι γινόμενο πρώτων αριθμών.*

Απόδειξη. Έστω M το σύνολο των φυσικών αριθμών οι οποίοι είναι μεγαλύτεροι από το 1 και δεν είναι γινόμενο πρώτων αριθμών. Εάν $M \neq \varnothing$, από την Αρχή Ελαχίστου υπάρχει ελάχιστο στοιχείο $m \in M$. Ο m είναι μεγαλύτερος από το 1 και δεν είναι πρώτος (αφού δεν είναι γινόμενο πρώτων). Συνεπώς υπάρχουν φυσικοί αριθμοί r και s τέτοιοι ώστε $1 < r < m$, $1 < s < m$ και $m = rs$. Αφού m είναι το ελάχιστο στοιχείο του M, οι r και s δεν ανήκουν στο M, και συνεπώς είναι γινόμενα πρώτων αριθμών. Αλλά τότε $m = rs$ είναι επίσης γινόμενο πρώτων αριθμών· άτοπο. Άρα $M = \varnothing$, και κάθε φυσικός αριθμός μεγαλύτερος από τον 1 είναι γινόμενο πρώτων αριθμών.

□

Θεώρημα 6.18 *Υπάρχουν άπειροι πρώτοι αριθμοί.*

Απόδειξη. Υποθέτουμε οτι το σύνολο των πρώτων αριθμών είναι πεπερασμένο, έστω $\{p_1, p_2, \ldots, p_r\}$. Ο ακέραιος $m = p_1 p_2 \cdots p_r + 1$ έχει ένα πρώτο διαιρέτη, σύμφωνα με την Πρόταση 6.17, έστω p_i. Τότε ο p_i διαιρεί τον m και τον $m - 1 = p_1 p_2 \cdots p_r$, συνεπώς ο p_i διαιρεί τον 1· άτοπο.

□

Εάν k είναι διαιρέτης δύο αριθμών $m, n \in \mathbb{N}$, ονομάζεται **κοινός διαιρέτης**. Ο 1 είναι πάντα κοινός διαιρέτης. Εάν δεν υπάρχει άλλος, λέμε οτι οι m και n είναι **πρώτοι μεταξύ τους**. Αντί να χαρακτηρίσουμε τον μέγιστο κοινό διαιρέτη ως τον μεγαλύτερο από τους κοινούς διαιρέτες, προτιμούμε να τον ορίσουμε με ένα πιο χρήσιμο τρόπο. Λέμε οτι $h \in \mathbb{N}$ είναι ο **μέγιστος κοινός διαιρέτης** των $m, n \in \mathbb{N}$, εάν h είναι κοινός διαιρέτης των m, n και έχει την ιδιότητα οτι κάθε άλλος διαιρέτης των m, n είναι διαιρέτης του h. Συμβολίζουμε τον μέγιστο κοινό διαιρέτη $h = \text{μκδ}\,(m, n)$.

Ο απλούστερος τρόπος να δείξουμε οτι δύο οποιοιδήποτε μη μηδενικοί φυσικοί αριθμοί έχουν μέγιστο κοινό διαιρέτη, είναι να τον υπολογίσουμε. Αυτό μπορεί να γίνει με έναν αλγόριθμο, τον Ευκλείδιο Αλγόριθμο, ο οποίος βασίζεται στις δύο ακόλουθες ιδιότητες.

1. Εάν $r_1 = q r_2$, τότε $\text{μκδ}\,(r_1, r_2) = r_2$

2. Εάν $r_1 = q r_2 + r_3$, με $r_3 \neq 0$, τότε $\text{μκδ}\,(r_1, r_2) = \text{μκδ}\,(r_2, r_3)$.

Οι ιδιότητες αποδεικνύονται εύκολα, χρησιμοποιώντας τον ορισμό του μέγιστου κοινού διαιρέτη. Ειδικότερα, η 2 ισχύει γιατί η ισότητα $r_1 = qr_2 + r_3$ δείχνει οτι ένας κοινός διαιρέτης των r_1 και r_2, πρέπει να διαιρεί τον r_3, ενώ ένας κοινός διαιρέτης των r_2 και r_3 πρέπει να διαιρεί τον r_1.

Ο Ευκλείδιος Αλγόριθμος

Για να βρούμε τον μέγιστο κοινό διαιρέτη των r_1 και r_2, χρησιμοποιούμε επανειλημμένα τον αλγόριθμο της διαίρεσης και βρίσκουμε q_i, r_i τέτοια ώστε

$$\begin{array}{rcl@{\qquad\qquad}c} r_1 &=& q_1r_2 + r_3 & r_3 < r_2 \\ r_2 &=& q_2r_3 + r_4 & r_4 < r_3 \\ \vdots & & & \vdots \\ r_i &=& q_ir_{i+1} + r_{i+2} & r_{i+2} < r_{i+1} \end{array}$$

Αφού $r_2 > r_3 > r_4 > \cdots > r_i$, αυτή η διαδικασία δεν μπορεί να συνεχιστεί επ΄ αόριστον γιατί, από την Αρχή Ελαχίστου, το σύνολο αυτών των αριθμών έχει ένα ελάχιστο στοιχείο. Εάν αυτό το ελάχιστο στοιχείο είναι $r_k \neq 0$, τότε από τον αλγόριθμο της διαίρεσης έχουμε $r_{k-1} = q_{k-1}r_k + r_{k+1}$, με $r_{k+1} < r_k$, άτοπο. Άρα το ελάχστο στοιχείο $r_k = 0$, και r_{k-1} είναι το μικρότερο θετικό υπόλοιπο που προκύπτει από αυτή τη διαδικασία. Θέτουμε $h = r_{k-1}$ και χρησιμοποιώντας τις παραπάνω ιδιότητες έχουμε

$$\begin{aligned} h &= \text{μκδ}\,(r_{k-2},\, r_{k-1}) \\ &= \text{μκδ}\,(r_{k-3},\, r_{k-2}) \\ &= \ldots \\ &= \text{μκδ}\,(r_1,\, r_2). \end{aligned}$$

Παράδειγμα 6.1 Υπολογίζουμε τον μέγιστο κοινό διαιρέτη των αριθμών 612 και 221:

$$\begin{array}{rcrcr} 612 &=& 2\cdot 221 &+& 170 \\ 221 &=& 1\cdot 170 &+& 51 \\ 170 &=& 3\cdot 51 &+& 17 \\ 51 &=& 3\cdot 17 & & \end{array}$$

Άρα $17 = \text{μκδ}\,(612,\, 221)$.

Προσέξτε οτι αυτή η μέθοδος βρίσκει τον μκδ χωρίς να χρειάζεται παραγοντοποίηση των αριθμών σε πρώτους παράγοντες.

Παράδειγμα 6.2 Υπολογίζουμε το μέγιστο κοινό διαιρέτη των $n^{10} - 1$ και $n^6 - 1$:

$$\begin{aligned} n^{10} - 1 &= n^4(n^6 - 1) + n^4 - 1 \\ n^6 - 1 &= n^2(n^4 - 1) + n^2 - 1 \\ n^4 - 1 &= (n^2 + 1)(n^2 - 1) \end{aligned}$$

Άρα

$$\begin{aligned} \text{μκδ}\,(n^{10} - 1,\, n^6 - 1) &= \text{μκδ}\,(n^6 - 1,\, n^4 - 1) \\ &= \text{μκδ}\,(n^4 - 1,\, n^2 - 1) \\ &= n^2 - 1\,. \end{aligned}$$

Πρόταση 6.19 *Εάν h είναι ο μκδ των $r_1, r_2 \in \mathbb{N}$, και $n \in \mathbb{N}$, τότε ο μκδ των nr_1 και nr_2 είναι nh.*

Απόδειξη. Εάν θεωρήσουμε τα βήματα του Ευκλείδειου Αλγόριθμου για τον μκδ (r_1, r_2), και πολλαπλασιάσουμε κάθε ισότητα με n, έχουμε

$$\begin{array}{rcll} nr_1 & = & q_1 nr_2 + nr_3 & \qquad nr_3 < nr_2 \\ nr_2 & = & q_2 nr_3 + nr_4 & \qquad nr_4 < nr_3 \\ \vdots & & \vdots & \\ nr_{k-2} & = & q_{k-2} nr_{k-1} & \end{array}$$

αφού $r_k = 0$. Η μοναδικότητα των υπολοίπων στον αλγόριθμο της διαίρεσης, συνεπάγεται οτι αυτές οι ισότητες δίδουν τον Ευκλείδειο Αλγόριθμο για τον μκδ (nr_1, nr_2), και οτι

$$\begin{array}{rcl} \text{μκδ}\,(nr_1, nr_2) & = & nr_{k-1} \\ & = & n\text{μκδ}\,(r_1, r_2) \end{array}$$

□

Αυτή η παρατήρηση οδηγεί στο επόμενο σημαντικό αποτέλεσμα.

Λήμμα 6.20 *Εάν $m, n \in \mathbb{N}$ και p είναι πρώτος αριθμός που διαιρεί το γινόμενο mn, τότε είτε ο p διαιρεί τον m είτε ο p διαιρεί τον n.*

Απόδειξη. Υποθέτουμε οτι ο p δεν διαιρεί τον m. Τότε, αφού ο p είναι πρωτος, οι μόνοι διαιρέτες του είναι ο 1 και ο p, και ο μκδ $(m, p) = 1$. Από την Πρόταση 6.19 ο μκδ του mn και του pn είναι ο n. Αλλά ο p διαιρεί τον mn και τον pn. Από τον ορισμό του μκδ, συμπεραίνουμε οτι ο p διαιρεί τον n.

□

Το ακόλουθο πόρισμα αποδεικνύεται με επαγωγή στο $k \geq 2$.

Πόρισμα 6.21 *Εάν ο p είναι πρώτος αριθμός που διαιρεί το γινόμενο $m_1 m_2 \dots m_k$, τότε ο p διαιρεί τουλάχιστον ένα από τους $m_1, m_2, \dots m_k$.*

Το Λήμμα 6.20 χρησιμοποιείται στην απόδειξη οτι ο αριθμός $\sqrt{2}$ δεν είναι ρητός. Πράγματι, εάν $\sqrt{2} = p/q$, όπου p και q είναι φυσικοί αριθμοί, και μκδ $(p, q) = 1$, τότε $p^2 = 2q^2$. Τότε ο 2 διαιρεί τον p^2, και από το Λήμμα 6.20, ο 2 διαιρεί τον p. Αλλά τότε ο 2 διαιρεί το q^2 και συνεπώς ο 2 διαιρεί τον q. Άτοπο, αφού υποθέσαμε οτι μκδ $(p, q) = 1$.

Κλείνουμε αυτό το Κεφάλαιο με το Θεώρημα Μοναδικής Παραγοντοποίησης, ή Θεμελιώδες Θεώρημα Αριθμητικής: η παραγοντοποίηση ενός φυσικού αριθμού σε γινόμενο πρώτων είναι μοναδική, εκτός από αναδιάταξη των παραγόντων.

Θεώρημα 6.22 (Θεώρημα Μοναδικής Παραγοντοποίησης) *Υποθέτουμε οτι $m \in \mathbb{N}, m \geq 2$ και οτι υπάρχουν πρώτοι αριθμοί $p_1, p_2, \dots, p_r$ και $q_1, q_2, \dots q_s$ τέτοιοι ώστε*

$$m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s\,.$$

Τότε $r = s$ και υπάρχει αμφιμονοσήμαντη απεικόνιση $\varphi : \{1, \dots, r\} \to \{1, \dots, s\}$ τέτοια ώστε $p_1 = q_{\varphi(i)}$ για κάθε $i = 1, \dots, r$

Απόδειξη. Έστω φυσικός αριθμός $m \geq 2$, και πρώτοι $p_1, \ldots, p_r$ και $q_1, \ldots, q_s$ τέτοιοι ώστε

$$m = p_1 \cdots p_r = q_1 \cdots q_s$$

Υποθέτουμε οτι $r \leq s$, και εφαρμόζουμε επαγωγή στο r. Εάν $r = 1$, τότε $m = p_1 = q_1 \cdots q_s$. Από το Πόρισμα 6.21, ο p_1 διαιρεί κάποιον από τους $q_1, \ldots, q_s$, έστω τον q_i. Αλλά ο q_i είναι πρώτος, και συνεπώς $p_1 = q_i$. Εάν $s > 1$, από την Πρόταση 6.6 έχουμε $1 = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s$, άτοπο αφού οι πρώτοι αριθμοί $q_j > 1$. Συμπεραίνουμε οτι $s = 1$ και $m = p_1 = q_1$.

Εάν $r > 1$ και $m = p_1 \cdots p_r = q_1 \cdots q_s$, ο πρώτος αριθμός p_r διαιρεί γινόμενο $q_1 \cdots q_s$, και συνεπώς διαιρεί κάποιον από τους $q_1, \ldots, q_s$, έστω τον q_i. Αλλά ο q_i είναι πρώτος, και συνεπώς $p_r = q_i$. Συμπεραίνουμε οτι

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s.$$

Από την επαγωγική υπόθεση, $r - 1 = s - 1$ και υπάρχει αμφιμονοσήμαντη $\psi : \{1, \ldots, r - 1\} \to \{1, \ldots, i-1, i+1, \ldots, s\}$ τέτοια ώστε $p_j = q_{\psi(j)}$. Άρα $r = s$, και η ζητούμενη αμφιμονοσήμαντη απεικόνιση είναι

$$\varphi(j) = \begin{cases} \psi(j) & \text{εάν } j = 1, \ldots, r-1 \\ i & \text{εάν } j = r \end{cases}$$

□

Ασκήσεις

Άσκηση 6.1 Ορίστε m^n, για $m, n \in \mathbb{N}_0$, αναδρομικά με

$$m^0 = 1 \ , \ m^{n+1} = m^n m.$$

Θεωρώντας γνωστές τις ιδιότητες της πρόσθεσης και του πολλαπλασιασμού, δείξτε, με κατάλληλα επαγωγικά επιχειρήματα, οτι

α'. $m^{n+r} = m^n m^r$

β'. $m^{nr} = (m^n)^r$

γ'. $(mn)^r = m^r n^r$

Άσκηση 6.2 Έστω $\alpha \in \mathbb{R}$, $\beta \in \mathbb{R}$ με $\alpha + \beta > 0$. Αποδείξτε οτι για κάθε $n \in \mathbb{N}_0$:

$$\frac{\alpha^n + \beta^n}{2} \geq \left(\frac{\alpha+\beta}{2}\right)^n .$$

Άσκηση 6.3 Ορίζουμε αναδρομικά το $n!$ με $0! = 1$ και $(n+1)! = n!\,(n+1)$.

α'. Δείξτε με επαγωγή οτι $(n-r)!\,r!$ διαιρεί το $n!$ για όλα τα r με $0 \leq r \leq n$.

β'. Από το α' έχουμε οτι $\dfrac{n!}{(n-r)!\,r!}$ είναι φυσικός αριθμός. Τον ονομάζουμε *διωνυμικό συντελεστή* και τον συμβολίζουμε $\binom{n}{r}$. Δείξτε οτι

(i) $\binom{n}{0} = 1$

(ii) $\binom{n}{1} = n$

(iii) $\binom{n}{r} = \binom{n}{n-r}$

γ'. Δείξτε οτι

$$\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r} .$$

δ'. Δείξτε με επαγωγή οτι οι διωνυμικοί συντελεστές είναι ακριβώς οι συντελεστές στο ανάπτυγμα του διωνύμου $(a+b)^n$:

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{r} a^{n-r} b^r + \cdots + \binom{n}{n} b^n .$$

Στο Κεφάλαιο 7 θα δούμε μία άλλη ερμηνεία των διωνυμικών συντελεστών.

Άσκηση 6.4 Αντιστρέφοντας τη διαδικασία του Ευκλείδειου Αλγόριθμου, μπορούμε να βρούμε ακέραιους αριθμούς $a,\, b \in \mathbb{Z}$, τέτοιους ώστε

$$\text{μκδ}\,(p,\, q) = ap + bq.$$

Χρησιμοποιήστε αυτή την παρατήρηση για να γράψετε το 17 στη μορφή $612a + 221b$, με $a,\, b \in \mathbb{Z}$.

Άσκηση 6.5 Δείξτε οτι εάν $p,\, q,\, r \in \mathbb{N}$, $p|r$, $q|r$ και $\text{μκδ}\,(p,\, q) = 1$, τότε $pq|r$.

Άσκηση 6.6 Υπολογίστε τον μέγιστο κοινό διαιρέτη των αριθμών 2244 και 2145,

α΄. χρησιμοποιώντας τον Ευκλείδιο Αλγόριθμο.

β΄. παραγοντοποιώντας τους δύο αριθμούς σε πρώτους παράγοντες.

Άσκηση 6.7 Δείξτε οτι εάν p, q και n είναι φυσικοί αριθμοί, $p^n|q^n$ εάν και μόνον εάν $p|q$.

Άσκηση 6.8 Δείξτε οτι εάν p είναι πρώτος αριθμός και $p|q^n$, τότε $p^n|q^n$.

Παράρτημα

Θεώρημα (Θεώρημα Αναδρομής) *Εάν X είναι ένα σύνολο, $f : X \to X$ μια συνάρτηση, και $c \in X$, τότε υπάρχει μοναδική συνάρτηση $\varphi : \mathbb{N}_0 \to X$ τέτοια ώστε*

α΄. $\varphi(0) = c$,

β΄. $\varphi(\varepsilon(n)) = f(\varphi(n))$ *για κάθε* $n \in \mathbb{N}_0$.

Απόδειξη. Από τη σκοπιά της θεωρίας συνόλων μια συνάρτηση $\varphi : \mathbb{N}_0 \to X$ είναι ένα υποσύνολο $\varphi \subseteq \mathbb{N}_0 \times X$ με τις ιδιότητες

i. Για κάθε $n \in \mathbb{N}_0$, υπάρχει $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$,

ii. Εάν (n, x) και $(n, y) \in \varphi$, τότε $x = y$.

Αρα για να ορίσουμε τη συνάρτηση φ αρκεί να προσδιορίσουμε το κατάλληλο υποσύνολο. Οι ιδιότητες της φ στη διατύπωση του Θεωρήματος σημαίνουν οτι αυτό το υποσύνολο πρέπει να ικανοποιεί

Α΄. $(0, c) \in \varphi$,

Β΄. Εάν $(n, x) \in \varphi$ τότε και $(\varepsilon(n), f(x)) \in \varphi$.

Υπάρχουν πολλά υποσύνολα με αυτές τις ιδιότητες, όπως για παράδειγμα όλο το $\mathbb{N}_0 \times X$. Το ζητούμενο είναι η τομή όλων αυτών των υποσυνόλων, γιατί μόνον αυτή θα ικανοποιεί τις ιδιότητες (i) και (ii). Θεωρούμε το σύνολο $\mathcal{V}$ όλων των υποσυνόλων $U \subseteq \mathbb{N}_0 \times X$ για τα οποία ισχύουν

$$(0, c) \in U\,,$$
$$(n, x) \in U \;\Rightarrow\; (\varepsilon(n), f(x)) \in U\,.$$

Έχουμε $\mathcal{V} \neq \varnothing$, αφού $\mathbb{N}_0 \times X \in \mathcal{V}$. Θέτουμε $\varphi = \bigcap \mathcal{V}$. Τότε φ ικανοποιεί τις (Α΄) και (Β΄), είναι μάλιστα το μικρότερο σύνολο που τις ικανοποιεί. Απομένει να δείξουμε οτι φ ικανοποιεί τις (i) και (ii).

Θέτουμε

$$S = \{n \in \mathbb{N}_0 \,|\, (n, x) \in \varphi \text{ για κάποιο } x \in X\}\,.$$

Από το (Α΄), $0 \in S$ και από το (Β΄) $n\S \Rightarrow \varepsilon(n) \in S$. Με επαγωγή έχουμε $S = \mathbb{N}_0$, και η (i) ικανοποιείται.

Για να δείξουμε την (ii), θέτουμε

$$T = \{n \in \mathbb{N}_0 \,|\, (n, x) \in \varphi \text{ για μοναδικό } x \in X\}\,.$$

Γνωρίζουμε οτι $(0, c) \in \varphi$. Εάν $(0, d) \in \varphi$ και $c \neq d$, ορίζουμε $\varphi^- = \varphi \backslash \{(0, d)\}$. Τότε φ^- ικανοποιεί την (Α΄). Εάν $(n, x) \in \varphi^-$, τότε $(\varepsilon(n), f(x)) \in \varphi$ και δεν είναι ίσο με $(0, d)$ εφ'όσον $\varepsilon(n) \neq 0$. Άρα $(\varepsilon(n), f(x)) \in \varphi^-$ και φ^- ικανοποιεί την (Β΄). Αλλά το φ είναι το μικρότερο σύνολο που ικανοποιεί τις (Α΄) και (Β΄). Αρα δεν υπάρχει τέτοιο d, και $0 \in T$.

Για το επαγωγικό βήμα: εάν $n \in T$ τότε υπάρχει μοναδικό $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$, άρα, για να δείξουμε οτι $\varepsilon(n) \in T$ πρέπει να δείξουμε οτι δεν υπάρχει $y \neq f(x)$ τέοιο ώστε $(\varepsilon(n), y) \in \varphi$. Εάν υπήρχε τέτοιο ζεύγος, θεωρήστε το $\varphi^* = \varphi \backslash \{(\varepsilon(n), y)\}$. Οπως προηγουμένως, εφ'οσον $0 \neq \varepsilon(n)$, φ^* ικανοποιεί την (A′). Για να δείξουμε οτι ικανοποιεί την (B′) ελέγχουμε οτι

$$(m, z) \in \varphi^* \Rightarrow (\varepsilon(m), f(z)) \in \varphi^* \text{ για κάθε } m \in \mathbb{N}_0 .$$

Για $m = n$ αυτό ισχύει, αφού υπάρχει μόνον ένα $x \in X$ τέτοιο ώστε $(n, x) \in \varphi$, και γιάυτό το x, $(\varepsilon(n), f(x)) \in \varphi$ από το (B′), και δεν είναι $(\varepsilon(n), y)$, αφού $y \neq f(x)$. Για $m \neq n$, έχουμε $(\varepsilon(m), f(z)) \in \varphi$, από το (B′), και $\varepsilon(m) \neq \varepsilon(m)$. Άρα $(\varepsilon(m), f(x)) \neq (\varepsilon(n), y)$, και συνεπώς $(\varepsilon(m), f(z)) \in \varphi^*$. Και στις δύο περιπτώσεις, φ^* ικανοποιεί τη (B′), και έχουμε αντίφαση, καθώς φ είναι ελάχιστο. Επαγωγικά, $T = \mathbb{N}_0$, που ολοκληρώνει την απόδειξη.

□

Θεώρημα (Κανόνες της αριθμητικής) *Για όλα τα m, n, $p \in \mathbb{N}_0$, ισχύουν τα ακόλουθα:*

1. *Προσεταιριστική ιδιότητα της πρόσθεσης:*

$$(m + n) + p = m + (n + p) ,$$

2. *Μεταθετική ιδιότητα της πρόσθεσης:*

$$m + n = n + m ,$$

3. *Προσεταιριστική ιδιότητα του πολλαπλασιασμού:*

$$(mn)p = m(np) ,$$

4. *Μεταθετική ιδιότητα του πολλαπλασιασμού:*

$$mn = nm ,$$

5. *Επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση:*

$$m(n + p) = mn + mp .$$

Απόδειξη. Το (1) αποδεικνύεται με επαγωγή στο p, χρησιμοποιώντας το σύνολο

$$S = \{p \in \mathbb{N}_0 \,|\, (m + n) + p = m + (n + p)\} .$$

Πρώτον

$$\begin{aligned} (m + n) + 0 &= m + n \text{ από την (πρ1)} \\ &= m + (n + 0) \text{ από την (πρ1)}, \end{aligned}$$

άρα $0 \in S$.

Κατόπιν, εάν $p \in S$, τότε

$$(m + n) + p = m + (n + p) , \tag{6.1}$$

άρα

$$\begin{aligned}(m+n)+\varepsilon(p) &= \varepsilon((m+n)+p) \text{ από την (πρ2)}\\ &= \varepsilon(m+(n+p)) \text{ από την 6.1}\\ &= m+\varepsilon(n+p) \text{ από την (πρ2)}\\ &= m+(n+\varepsilon(p) \text{ από την (πρ2)}\end{aligned}$$

που συνεπάγεται οτι $\varepsilon(p) \in S$. Επαγωγικά, $S = \mathbb{N}_0$.

Το (2) αποδεικνύεται με επαγωγή στο n, χρησιμοποιώντας το

$$S = \{n \in \mathbb{N}_0 \,|\, m+n = n+m\}\,.$$

Το Λήμμα 6.4 (1) δείχνει οτι $0 \in S$. Εάν $n \in S$, τότε

$$m+n = n+m \tag{6.2}$$

και

$$\begin{aligned}m+\varepsilon(n) &= \varepsilon(m+n) \text{ από την (πρ2)}\\ &= \varepsilon(n+m) \text{ από την 6.2}\\ &= n+\varepsilon(m) \text{ από την (πρ2)}\\ &= n+(1+m) \text{ από το Λήμμα 6.4(2)}\\ &= (n+1)+m \text{ από το Θεώρημα 6.5(1)}\\ &= \varepsilon(n)+m\,,\end{aligned}$$

και συνεπώς $\varepsilon(n) \in S$. Επαγωγικά $S = \mathbb{N}_0$.

Είναι προτιμότερο να αποδείξουμε κατόπιν το (5), χρησιμοποιώντας επαγωγή στο p. Θέτουμε

$$S = \{p \in \mathbb{N}_0 \,|\, m(n+p) = mn+mp\}\,.$$

Τότε

$$\begin{aligned}m(n+0) &= mn \text{ από την (πρ1)}\\ &= mn+0 \text{ από την (πρ1)}\\ &= mn+m0 \text{ από την (πλ1)},\end{aligned}$$

και συνεπώς $0 \in S$.

Εάν $p \in S$, τότε

$$m(n+p) = mn+mp \tag{6.3}$$

και συνεπώς

$$\begin{aligned}m(n+\varepsilon(p)) &= m\varepsilon(n+p) \text{ από την (πρ2)}\\ &= m(n+p)+m \text{ από την (πλ2)}\\ &= (mn+mp)+m \text{ από την 6.3}\\ &= mn+(mp+m) \text{ από την (1)}\\ &= mn+m\varepsilon(p) \text{ από την (πλ2)},\end{aligned}$$

άρα $\varepsilon(p) \in S$ και επαγωγικά, $S = \mathbb{N}_0$.

Η απόδειξη του (3) είναι τώρα σχετικά εύκολη και όμοια με τις προηγούμενες. Απομένει να αποδείξουμε το (4), που είναι κάπως πιο πολύπλοκο. Θέτουμε

$$S = \{n \in \mathbb{N}_0 \,|\, mn = nm\}\,.$$

Από το Λήμμα 6.4(3), $0 \in S$. Εάν $n \in S$, τότε

$$mn = nm \tag{6.4}$$

και έχουμε

$$\begin{aligned} m\varepsilon(n) &= mn + m \text{ από την (πλ2)} \\ &= nm + m \text{ από την 6.4.} \end{aligned}$$

Εάν γνωρίζαμε οτι αυτό είναι ίσο με $\varepsilon(n)m$ θα είχαμε τελειώσει, αλλά δυστυχώς αυτό δεν το γνωρίζουμε ακόμη. Μπορούμε όμως να το αποδείξουμε, με μια δεύτερη επαγωγή, στο m. Θέτουμε

$$T = \{m \in \mathbb{N}_0 \,|\, nm + m = \varepsilon(n)m\}\,.$$

Τότε $0 \in T$, και εάν $m \in T$ τότε

$$nm + m = \varepsilon(n)m \tag{6.5}$$

και συνεπώς

$$\begin{aligned} n\varepsilon(m) + \varepsilon(m) &= n(m+1) + (m+1) \\ &= (nm+n) + (m+1) \text{ από την (5)} \\ &= nm + (n + (m+1)) \text{ από την (1)} \\ &= nm + ((n+m)+1) \text{ από την (1)} \\ &= nm + ((m+n)+1) \text{ από την (2)} \\ &= nm + (m + (n+1)) \text{ από την (1)} \\ &= (nm+m) + (n+1) \text{ από την (1)} \\ &= \varepsilon(n)m + \varepsilon(n) \text{ από την 6.5} \\ &= \varepsilon(n)\varepsilon(m) \text{ από την (πλ2),} \end{aligned}$$

άρα $\varepsilon(m) \in T$ και $T = \mathbb{N}_0$. Επιστρέφοντας στην προηγούμενη επαγωγή, έχουμε οτι $\varepsilon(n) \in S$ και $S = \mathbb{N}_0$. Ετσι ολοκληρώνεται η απόδειξη του (4).

□

Κεφάλαιο 7

Συνδυαστική

Απαρίθμηση σε πεπερασμένα σύνολα

Για να απαριθμήσουμε τα στοιχεία ενός συνόλου, δηλαδή να μετρήσουμε πόσα είναι, τα συγκρίνουμε με συγκεκριμένα υποσύνολα των φυσικών αριθμών. Πρώτα ορίζουμε αυτά τα υποσύνολα, για κάθε $k \in \mathbb{N}_0$:

$$\begin{aligned} \mathbb{N}(0) &= \varnothing \\ \mathbb{N}(k) &= \{n \in \mathbb{N} \,|\, n \leq k\}, \text{ για κάθε } k \in \mathbb{N}\,. \end{aligned}$$

Λήμμα 7.1 *Υπάρχει αμφιμονοσήμαντη συνάρτηση* $f : \mathbb{N}(k) \to \mathbb{N}(m)$ *εάν και μόνον εάν* $k = m$.

Απόδειξη. Το αποτέλεσμα είναι προφανώς αληθές εάν $m = 0$: τότε $\mathbb{N}(m) = \varnothing$, και η μοναδική αμφιμονοσήμαντη συνάρτηση από το κενό σύνολο είναι η κενή συνάρτηση $\varnothing \to \varnothing$.

Υποθέτουμε οτι το αποτέλεσμα ισχύει για κάποιο $m \in \mathbb{N}_0$ και θεωρούμε μια αμφιμονοσήμαντη συνάρτηση

$$\vartheta : \mathbb{N}(m+1) \to \mathbb{N}(k).$$

Εάν $k = 0$, τότε $\mathbb{N}(k) = \varnothing$, και συνεπώς $m+1 = 0$, που αντιφάσκει προς το Φ1. Άρα $k \neq 0$, και $k = n + 1$ για κάποιο $n \in \mathbb{N}_0$. Τώρα κατασκευάζουμε μια αμφιμονοσήμαντη συνάρτηση $\vartheta^* : \mathbb{N}(m+1) \to \mathbb{N}(n+1)$ για την οποία ισχύει $\vartheta^*(m+1) = n+1$.

Εάν για τη ϑ ισχύει οτι $\vartheta(m+1) = n+1$, θέτουμε $\vartheta^* = \vartheta$.

Εάν όχι, τότε υπάρχει κάποιο $q \leq n$ για το οποίο $\vartheta(q) = n+1$, και ορίζουμε τη ϑ^* ως εξής:

$$\begin{aligned} \vartheta^*(q) &= \vartheta(m+1) \\ \vartheta^*(m+1) &= n+1 \\ \vartheta^*(r) &= \vartheta(r) \text{ για } r \neq q,\ r \neq m+1. \end{aligned}$$

Τώρα περιορίζουμε την ϑ^* στη συνάρτηση

$$\vartheta^*|_{\mathbb{N}(m)} : \mathbb{N}(m) \to \mathbb{N}(n).$$

Αυτή είναι προφανώς αμφιμονοσήμαντη, και από την επαγωγική υπόθεση, $m = n$. Άρα $m+1 = n+1$, και με επαγωγή έχουμε το ζητούμενο.

□

Ορισμός. Λέμε οτι ένα σύνολο A *έχει k στοιχεία*, για $k \in \mathbb{N}_0$, εάν υπάρχει μία αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}(k) \to A$. Ενα σύνολο είναι **πεπερασμένο** εάν έχει k

στοιχεία για κάποιο $k \in \mathbb{N}_0$. Τον αριθμό των στοιχείων ενός πεπερασμένου συνόλου A τον συμβολίζουμε $|A|$ ή $\mathrm{card}\,(A)$.

Το Λήμμα 7.1 εξασφαλίζει οτι ο αριθμός των στοιχείων ενός πεπερασμένου συνόλου είναι καλά ορισμένος: εάν υπάρχουν αμφιμονοσήμαντες συναρτήσεις $f : \mathbb{N}(k) \to A$ και $g : \mathbb{N}(m) \to A$, τότε η $g^{-1} \circ f : \mathbb{N}(k) \to \mathbb{N}(m)$ είναι αμφιμονοσήμαντη, και άρα $k = m$.

Παράδειγμα 7.1 Το $\varnothing$ έχει 0 στοιχεία, $|\varnothing| = 0$. Το $\{\varnothing\}$ έχει ένα στοιχείο: υπάρχει αμφιμονοσήμαντη απεικόνιση από το $\{\varnothing\}$ στο $\{1\}$, άρα $|\{\varnothing\}| = 1$.

Ο αριθμός των στοιχείων πεπερασμένων συνόλων έχει ορισμένες απλές ιδιότητες.

$$\begin{aligned} |A \cup B| &\leq |A| + |B| \\ |A \cap B| &\leq \min\{|A|, |B|\}\,. \end{aligned}$$

Η ακριβής σχέση ανάμεσα στους τέσσερεις αριθμούς δίδεται στην ακόλουθη ταυτότητα:

Πρόταση 7.2 *Εάν A και B είναι σύνολα, τότε*

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

Δεν θα δώσουμε αυστηρή απόδειξη της παραπάνω ταυτότητας. Παραπέμπουμε στο διάγραμμα Venn, και την παρατήρηση οτι τα στοιχεία στην τομή $A \cap B$ απαριθμούνται μια φορά στο $|A \cup B|$, ενώ στο $|A| + |B|$ απαριθμούνται δύο φορές.

Πόρισμα 7.3 *Εάν $A \cap B = \varnothing$ τότε $|A \cup B| = |A| + |B|$.*

Με λίγη σκέψη επεκτείνουμε τον τύπο για την ένωση τριών συνόλων.

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| \\ &\quad -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\quad +|A_1 \cap A_2 \cap A_3| \end{aligned}$$

Παράδειγμα 7.2 Πόσοι αριθμοί από το 1 έως το 100 διαιρούνται με το 2, το 3 ή το 5; 50 αριθμοί διαιρούνται με το 2, 33 διαιρούνται με το 3 και 20 διαιρούνται με το 5. Οι αριθμοί που διαιρούνται με το 2 και το 3 είναι αυτοί που διαιρούνται με το 6 και είναι 16. Οι αριθμοί που διαιρούνται με το 2 και το 5 είναι αυτοί που διαιρούνται με το 10 και είναι 10. Οι αριθμοί που διαιρούνται με το 3 και το 5 είναι αυτοί που διαιρούνται με το 15 και είναι 6. Τέλος οι αριθμοί που διαιρούνται με το 2, το 3 και το 5 είναι τα πολλαπλάσια του 30 και είναι 3. Αντικαθιστώντας στον τύπο έχουμε:

$$50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

Αρα υπάρχουν 74 αριθμοί από το 1 έως το 100 που διαιρούνται με το 2 το 3 ή το 5.

Το επόμενο Θεώρημα δίδει το γενικό τύπο για τον αριθμό στοιχείων στην ένωση r συνόλων. Η διατύπωσή του αποτελεί άσκηση στη χρήση του συμβολισμού του αθροίσματος.

Θεώρημα 7.4 (Αρχή Εγκλεισμού και Αποκλεισμού) *Εάν* $A_1, A_2, \ldots, A_r$ *είναι πεπερασμένα σύνολα, τότε*

$$\begin{aligned}
&|A_1 \cup A_2 \cup \cdots \cup A_r| = \\
&= \sum_{i_1=1}^{r} |A_{i_1}| - \sum_{i_1=1}^{r-1} \sum_{i_2=i_1+1}^{r} |A_{i_1} \cap A_{i_2}| + \cdots \\
&\quad +(-1)^{k+1} \sum_{i_1=1}^{r-k+1} \sum_{i_2=i_1+1}^{r-k+2} \cdots \sum_{i_j=i_{j-1}+1}^{r-k+j} \cdots \sum_{i_k=i_{k-1}+1}^{r} |A_{i_1} \cap \cdots \cap A_{i_k}| + \cdots \\
&\quad +(-1)^{r+1} |A_1 \cap A_2 \cap \cdots \cap A_r|
\end{aligned}$$

Το Θεώρημα αποδεικνύεται με χρήση της Ισχυρής μορφής της Αρχής Επαγωγής στο r, ξεκινώντας από $r = 2$. Για να αποφύγουμε τον πολύπλοκο συμβολισμό, δεν θα αποδείξουμε το γενικό επαγωγικό βήμα, αλλά θα υποθέσουμε οτι ο τύπος ισχύει για 2 και 3, και θα αποδείξουμε οτι ισχύει για 4.

$$\begin{aligned}
&|A_1 \cup A_2 \cup A_3 \cup A_4| = \\
&= |(A_1 \cup A_2 \cup A_3) \cup A_4| \\
&= |A_1 \cup A_2 \cup A_3| + |A_4| - |(A_1 \cup A_2 \cup A_3) \cap A_4| \qquad (7.1)
\end{aligned}$$

Αλλά

$$\begin{aligned}
&|(A_1 \cup A_2 \cup A_3) \cap A_4| = \\
&= |(A_1 \cap A_4) \cup (A_2 \cap A_4) \cup (A_3 \cap A_4)| \\
&= |A_1 \cap A_4| + |A_2 \cap A_4| + |A_3 \cap A_4| \\
&\quad -|(A_1 \cap A_4) \cap (A_2 \cap A_4)| - |(A_1 \cap A_4) \cap (A_3 \cap A_4)| \\
&\quad -|(A_2 \cap A_4) \cap (A_3 \cap A_4)| + |(A_1 \cap A_4) \cap (A_2 \cap A_4) \cap (A_3 \cap A_4)| \\
&= |A_1 \cap A_4| + |A_2 \cap A_4| + |A_3 \cap A_4| \\
&\quad -|A_1 \cap A_2 \cap A_4| - |A_1 \cap A_3 \cap A_4| - |A_2 \cap A_3 \cap A_4| \\
&\quad +|A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

Αντικαθιστώντας στην 7.1 έχουμε το ζητούμενο.

Θεώρημα 7.5 (Αρχή Αθροίσματος) *Εάν* $A_1, A_2, \ldots, A_r$ *είναι σύνολα, ανα δύο ξένα μεταξύ τους, δηλαδή* $A_i \cap A_j = \varnothing$ *εάν* $i \neq j$*, τότε*

$$|A_1 \cup A_2 \cup \ldots \cup A_r| = |A_1| + |A_2| + \cdots + |A_r|\,.$$

Θεώρημα 7.6 *Εάν* A *και* B *είναι πεπερασμένα σύνολα, τότε* $A \times B$ *είναι πεπερασμένο, και*

$$|A \times B| = |A|\,|B|\,.$$

Απόδειξη. Εστω $|A| = k$, $|B| = r$. Εάν $A = \{a_1, a_2, \ldots, a_k\}$, θέτουμε $A_i = \{a_i\}$, για $i = 1, 2, \ldots, k$. Τότε $A = A_1 \cup A_2 \cup \cdots \cup A_k$, και $A \times B = (A_1 \times B) \cup (A_2 \times B) \cup \cdots \cup (A_k \times B)$. Τα σύνολα $A_i \times B$ και $A_j \times B$ είναι ξένα μεταξύ τους εάν $i \neq j$, αφού $(A_i \times B) \cap (A_j \times B) = (A_i \cap A_j) \times B = \varnothing \times B = \varnothing$. Αρα $|A \times B| = |A_1 \times B| + |A_2 \times B| + \cdots + |A_k \times B|$. Αλλά τα στοιχεία του $A_i \times B$ είναι ζεύγη (a_i, b), $b \in B$, και υπάρχει αμφιμονοσήμαντη συνάρτηση $A_i \times B \to B$, άρα $|A_i \times B| = |B| = r$. Καθώς υπάρχουν $|A| = k$ όροι στο άθροισμα,

$$|A \times B| = \sum_{i=1}^{k} r = k \cdot r = |A|\,|B|\,.$$

□

Θεώρημα 7.7 (Αρχή Γινομένου) *Εάν $A_1, A_2, \ldots, A_r$ είναι πεπερασμένα σύνολα, τότε*

$$|A_1 \times A_2 \times \cdots \times A_{r+1}| = |A_1|\,|A_2| \cdots |A_r|\,.$$

Απόδειξη. Με επαγωγή στο r, ξεκινώντας από $r = 2$. Θεωρούμε $r + 1$ πεπερασμένα υποσύνολα $A_1, A_2, \ldots, A_{r+1}$. Θέτουμε $A = A_1 \times A_2 \times \cdots \times A_r$ και $B = A_{r+1}$. Τότε $|A_1 \times A_2 \times \cdots \times A_r| = |A \times B| = |A|\,|B|$, και από την επαγωγική υπόθεση αυτό είναι ίσο με $(|A_1|\,|A_2| \cdots |A_r|)|A_{r+1}|$.

□

Θεώρημα 7.8 *Εάν A είναι πεπερασμένο σύνολο,*

$$|\mathfrak{P}(A)| = 2^{|A|}\,.$$

Απόδειξη. Με επαγωγή στο $r = |A|$. Όταν $r = 0$, $A = \varnothing$ και $|\mathfrak{P}(\varnothing)| = |\{\varnothing\}| = 1 = 2^0$.

Εάν $A = \{a_1, a_2, \ldots, a_{r+1}\}$, θεωρούμε τα σύνολα

$$S_1 = \{X \subseteq A \,|\, a_{r+1} \notin X\}$$

και

$$S_2 = \{X \subseteq A \,|\, a_{r+1} \in X\}\,.$$

Τότε $\mathfrak{P}(A) = S_1 \cup S_2$ και $S_1 \cap S_2 = \varnothing$. Θέτουμε $B = A \setminus \{a_{r+1}\}$. Τότε $S_1 = \mathfrak{P}(B)$. Από το S_2 ορίζουμε αμφιμονοσήμαντη συνάρτηση $f : S_2 \to S_1$ με $f(X) = X \setminus \{a_{r+1}\}$. Άρα $|S_1| = |S_2|$. Από την επαγωγική υπόθεση, $|S_1| = 2^r$, άρα

$$|\mathfrak{P}(A)| = |S_1| + |S_2| = 2|S_1| = 2 \cdot 2^r = 2^{r+1}\,.$$

□

Συνδυαστική

Ορισμός. **Πείραμα** στη συνδυαστική ονομάζουμε μία φυσική διαδικασία που έχει ένα πεπερασμένο σύνολο από δυνατά παρατηρήσιμα αποτελέσματα.

Παραδείγματα τέτοιων διαδικασιών είναι

1. Επιλέγουμε k από τα n στοιχεία ενός συνόλου.

2. Τοποθετούμε k κέρματα σε n κουτιά.

3. Κατανέμουμε γραφεία στους μεταπτυχιακούς φοιτητές του Τμήματος.

4. Ρίχνουμε δύο ζάρια και καταγράφουμε το αποτέλεσμα.

5. 'Στρίβουμε' ένα νόμισμα 20 φορές και καταγράφουμε τα αποτελέσματα.

6. Μοιράζουμε μία τράπουλα σε τέσσερεις παίκτες.

Στόχος της *συνδυαστικής* είναι να απαριθμήσουμε όλα τα δυνατά αποτελέσματα ενός πειράματος, ή αυτά από τα αποτελέσματα που έχουν κάποια συγκεκριμένα χαρακτηριστικά.

Θα διατυπώσουμε τις δύο βασικές αρχές απαρίθμησης για την περίπτωση δύο πειραμάτων.

Αρχή Γινομένου: Εάν ένα πείραμα έχει k δυνατά αποτελέσματα και ένα άλλο πείραμα έχει r δυνατά αποτελέσματα, τότε υπάρχουν kr δυνατά αποτελέσματα όταν γίνονται και τα δύο αυτά πειράματα.

Αρχή Αθροίσματος: Εάν ένα πείραμα έχει k δυνατά αποτελέσματα και ένα άλλο πείραμα έχει r δυνατά αποτελέσματα, τότε υπάρχουν $k+r$ δυνατά αποτελέσματα όταν γίνεται ακριβώς ένα από τα δύο πειράματα.

Για παράδειγμα, εάν υπάρχουν 7 μαθήματα που διδάσκονται το πρωί και 5 μαθήματα που διδάσκονται το απόγευμα, θα υπάρχουν $35 = 7 \cdot 5$ επιλογές για φοιτητές που θέλουν να γραφτούν σε ένα μάθημα που διδάσκεται το πρωί και σε ένα μάθημα που διδάσκεται το απόγευμα. Ενώ θα υπάρχουν $12 = 7 + 5$ επιλογές για φοιτητές που θέλουν να γραφτούν σε ένα μάθημα, είτε το πρωί είτε το απόγευμα.

Η ανάλυση πολλών διαφορετικών πειραμάτων είναι, από μαθηματική άποψη, η ίδια. Για παράδειγμα, το να ρίξουμε δύο ζάρια είναι από μαθηματική άποψη το ίδιο με το να τοποθετήσουμε δύο κέρματα σε 6 κουτιά, αριθμημένα από το 1 έως το 6. Να στρίψουμε ένα κέρμα 20 φορές είναι ουσιαστικά το ίδιο με το να μοιράσουμε 20 αντικείμενα σε δύο κουτιά.

Θα μελετήσουμε αναλυτικά ορισμένες παραλλαγές του πρώτου προβλήματος, του *πειράματος επιλογής*: Επιλέγουμε k από τα n στοιχεία ενός συνόλου.

Διάταξη και επανάληψη

Στο πείραμα επιλογής k αντικειμένων από τα n αντικείμενα ενός συνόλου, υπάρχουν δύο βασικοί παράγοντες που καθορίζουν τις δυνατές παραλλαγές.

- Εάν καταγράφουμε τη σειρά με την οποία επιλέγουμε τα στοιχεία ή όχι

- Εάν επιτρέπεται να επιλέξουμε το ίδιο στοιχείο περισσότερες φορές ή όχι.

Το βασικό πείραμα που θα εκτελούμε είναι το ακόλουθο: Μία σακούλα περιέχει n μπάλες, αριθμημένες $1, 2, 3, \ldots, n$. Από αυτές επιλέγουμε k μπάλες, με τον τρόπο που περιγράφεται σε κάθε περίπτωση.

I. Στην περίπτωση που μας ενδιαφέρει η σειρά με την οποία γίνεται η επιλογή των k στοιχείων από τα n στοιχεία του συνόλου, και επιτρέπεται να επιλέξουμε το ίδιο στοιχείο περισσότερες φορές, λέμε οτι απαριθμούμε **διατάξεις των n στοιχείων ανά k με επανάληψη**.

II. Στην περίπτωση που μας ενδιαφέρει η σειρά με την οποία γίνεται η επιλογή των k στοιχείων από τα n στοιχεία του συνόλου, και δεν επιτρέπεται να επιλέξουμε το ίδιο στοιχείο περισσότερες φορές, λέμε οτι απαριθμούμε **διατάξεις των n στοιχείων ανά k (χωρίς επανάληψη)**. Σε αυτήν την περίπτωση έχουμε $k \leq n$.

III. Στην περίπτωση που δεν μας ενδιαφέρει η σειρά με την οποία γίνεται η επιλογή των k στοιχείων από τα n στοιχεία του συνόλου, και δεν επιτρέπεται να επιλέξουμε το ίδιο στοιχείο περισσότερες φορές, λέμε οτι απαριθμούμε **συνδυασμούς των n στοιχείων ανά k (χωρίς επανάληψη)**. Σε αυτήν την περίπτωση έχουμε $k \leq n$.

IV. Στην περίπτωση που δεν μας ενδιαφέρει η σειρά με την οποία γίνεται η επιλογή των k στοιχείων από τα n στοιχεία του συνόλου, και επιτρέπεται να επιλέξουμε το ίδιο στοιχείο περισσότερες φορές, λέμε οτι απαριθμούμε **συνδυασμούς των n στοιχείων ανά k με επανάληψη**.

Αυτές είναι οι τέσσερεις βασικές παραλλαγές του πειράματος επιλογής που θα μελετήσουμε. Ειδικότερες παραλλαγές θα δούμε σε συγκεκριμένα παραδείγματα.

I. Διατάξεις n στοχείων ανά k με επανάληψη.

Από τη σακούλα που περιέχει n αριθμημένες μπάλες, επιλέγουμε διαδοχικά k μπάλες, καταγράφοντας γιά κάθε επιλογή τον αριθμό της μπάλας και επανατοποθετώντας τη μπάλα στη σακούλα πριν την επόμενη επιλογή. Ετσι καταλήγουμε σε μία διατεταγμένη k-άδα αριθμών από το 1 έως το n. Από την Αρχή Γινομένου, ο αριθμός των δυνατών αποτελεσμάτων είναι το γινόμενο των αριθμών δυνατών αποτελεσμάτων για κάθε επιλογή. Για κάθε επιλογή έχουμε n δυνατά αποτελέσματα, άρα συνολικά έχουμε n^k διαφορετικά δυνατά αποτελέσματα.

Πρόταση 7.9 *Ο αριθμός των διατάξεων n στοιχείων ανά k είναι* n^k.

Παραδείγματα

Εάν ρίξουμε ένα ζάρι 5 φορές, έχουμε 6^5 διαφορετικά δυνατά αποτελέσματα, εάν λαμβάνεται υπ'οψιν η σειρά με την οποία έρχονται οι αριθμοί.

Εάν στρίψουμε ένα νόμισμα 20 φορές, έχουμε 2^{20} διαφορετικά δυνατά αποτελέσματα, εάν λαμβάνεται υπ'οψιν η σειρά με την οποία εμφανίζονται κορώνα ή γράμματα.

II. Διατάξεις n στοχείων ανά k χωρίς επανάληψη, k ≤ n.

Επιλέγουμε κάθε μπάλα από τη σακούλα όπως στην περίπτωση I, αλλά μετά την καταγραφή δεν επιστρέφουμε τη μπάλα στη σακούλα. Σε αυτήν την περίπτωση πρέπει να ισχύει $k \leq n$. Για να επιλέξουμε την πρώτη μπάλα έχουμε n δυνατότητες. Μετά την επιλογή της πρώτης μπάλας, απομένουν $n-1$ μπάλες στη σακούλα. Ποιές είναι αυτές εξαρτάται από την πρώτη επιλογή, αλλά ο αριθμός τους είναι σε κάθε περίπτωση $n-1$. Αρα για την επιλογή της δεύτερης μπάλας έχουμε $n-1$ δυνατότητες. Μετά την επιλογή της δεύτερης μπάλας υπάρχουν $n-2$ μπάλες στη σακούλα, άρα για την επιλογή της τρίτης μπάλας έχουμε $n-2$ δυνατότητες. Από την Αρχή Γινομένου, για την επιλογή των τριών μπαλών υπάρχουν

$$n(n-1)(n-2)$$

διαφορετικές δυνατότητες. Συνεχίζοντας με αυτόν τον τρόπο, έχουμε $n-3$ δυνατότητες για την επιλογή της τέταρτης μπάλας, κ.ο.κ. καταλήγοντας με $n-k+1$ δυνατότητες για την επιλογή της τελευταίας k-οστής μπάλας. Εφαρμόζοντας πάλι την Αρχή Γινομένου, έχουμε συνολικά

$$\begin{aligned} n(n-1)(n-2)\cdots(n-k+1) &= \\ &= \frac{n(n-1)(n-2)\cdots(n-k+1)(n-k)\cdots 1}{(n-k)(n-k-1)\cdots 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

δυνατότητες να επιλέξουμε k από τις n μπάλες στη σακούλα. Αυτός ο αριθμός συμβολίζεται $P(n, k)$.

Πρόταση 7.10 *Ο αριθμός των διατάξεων n στοιχείων ανά k χωρίς επανάληψη είναι*

$$P(n, k) = \frac{n!}{(n-k)!}\,.$$

Παράδειγμα 7.3 Με πόσους τρόπους μπορούν να κληρωθούν 5 διαφορετικά δώρα σε 100 λαχνούς;
Εφόσον τα δώρα είναι διαφορετικά μεταξύ τους μπορούμε να θεωρήσουμε οτι έχουμε μια διάταξη, 1ο δώρο, 2ο δώρο, κ.ο.κ. Αρα το πρόβλημα αφορά τους τρόπους με τους οποίους μπορούμε να επιλέξουμε μια διατεταγμένη 5-αδα, από το σύνολο των 100 λαχνών, χωρίς επανάληψη αφού υποθέτουμε οτι ένας λαχνός που κληρώνεται δεν ξαναμπαίνει στην κληρωτίδα. Αρα ο ζητούμενος αριθμός είναι $P(100, 5) = \frac{100!}{95!} = 9\,034\,502\,400$.

Μία ειδική υποπερίπτωση της περίπτωσης ΙΙ είναι όταν $k = n$. Τότε λέμε οτι έχουμε μία **μετάθεση** των n αντικειμένων.

ΙΙ.α. Μεταθέσεις n διαφορετικών αντικειμένων.

Επιλέγουμε διαδοχικά όλες τις μπάλες, χωρίς επανατοποθέτηση. Τα δυνατά αποτελέσματα είναι όλες οι μεταθέσεις του συνόλου $\{1, 2, 3, \ldots, n\}$.

Πρόταση 7.11 *Ο αριθμός των μεταθέσεων n αντικειμένων είναι $n!$.*

ΙΙΙ. Συνδυασμοί n στοιχείων ανά k, χωρίς επανάληψη.

Σε αυτήν την περίπτωση δεν επανατοποθετούμε τις μπάλες στη σακούλα, ούτε καταγράφουμε τη σειρά με την οποία τις επιλέγουμε. Μπορούμε να υποθέσουμε οτι παίρνουμε k από τις n μπάλες σε μία επιλογή, και οτι εξετάζουμε τα υποσύνολα μεγέθους k ενός συνόλου μεγέθους n. Για να απαριθμήσουμε αυτό το σύνολο το συγκρίνουμε με το σύνολο των διατάξεων n στοιχείων ανά k. Από ένα υποσύνολο k στοιχείων μπορούμε να πάρουμε $k!$ διαφορετικές διατάξεις των k στοιχείων. Αρα, εάν συμβολίσουμε $\binom{n}{k}$ τον αριθμό των διαφορετικών υποσυνόλων με k στοιχεία, και $P(n, k)$ τον αριθμό των διατάξεων n στοιχείων ανά k, έχουμε:

$$k!\binom{n}{k} = P(n, k)\,.$$

Αντικαθιστώντας $P(n,\, k) = \frac{n!}{(n-k)!}$ έχουμε

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

Πρόταση 7.12 *Ο αριθμός των συνδυασμών n στοιχείων ανά k, χωρίς επανάληψη, είναι*

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

Ο αριθμός $\binom{n}{k}$ ονομάζεται **διωνυμικός συντελεστής**, επειδή εμφανίζεται ως ο συντελεστής του όρου $a^{n-k}b^k$ στο ανάπτυγμα του διωνύμου $(a+b)^n$.

Από τον τρόπο που υπολογίσαμε τον αριθμό $\binom{n}{k}$ είναι φανερό οτι $\sum_{k=0}^{n}\binom{n}{k}$ πρέπει να είναι ίσο με τον αριθμό όλων των υποσυνόλων ενός συνόλου με n στοιχεία:

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n\,.$$

Εχουμε δει στην Άσκηση 6.3 άλλες ιδιότητες των διωνυμικών συντελεστών:

$$\binom{n}{k} = \binom{n}{n-k} \quad , \quad \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}\,.$$

Τα επιχειρήματα που χρησιμοποιήσαμε στην περίπτωση III επιτρέπουν να γενικεύσουμε το αποτέλεσμα II.α.

III.α. Μεταθέσεις n αντικειμένων, που διακρίνονται κατά ομάδες.

Υποθέτουμε οτι έχουμε n μπάλες, χρωματισμένες με r διαφορετικά χρώματα: n_1 μπάλες χρώματος 1, n_2 μπάλες χρώματος 2, …, n_r μπάλες χρώματος r, έτσι ώστε

$$n = n_1 + n_2 + \cdots + n_r\,.$$

Πόσες διαφορετικές διατάξεις των n μπαλών υπάρχουν εάν μπορούμε να διακρίνουμε τα διαφορετικά χρώματα αλλά όχι τις διαφορετικές μπάλες του ιδίου χρώματος;

Παράδειγμα 7.4 Εάν έχουμε μπάλες δύο διαφορετικών χρωμάτων, με $n_1 = 2$, $n_2 = 2$, τότε οι διαφορετικές διατάξεις είναι οι ακόλουθες 6:

$$\begin{array}{ccc} \bullet\ \bullet\ \circ\ \circ & \bullet\ \circ\ \bullet\ \circ & \bullet\ \circ\ \circ\ \bullet \\ \circ\ \bullet\ \bullet\ \circ & \circ\ \bullet\ \circ\ \bullet & \circ\ \circ\ \bullet\ \bullet \end{array}$$

Για να υπολογίσουμε τον αριθμό στη γενική περίπτωση, υποθέτουμε οτι οι μπάλες είναι όλες διαφορετικές: αριθμούμε τις μπάλες του χρώματος 1 από 1 έως n_1, τις μπάλες του χρώματος 2 από 1 έως n_2 κ.ο.κ. Τότε ο αριθμός των διαφορετικών διατάξεων είναι ο αριθμός των μεταθέσεων n στοιχείων $n!$. Θέλουμε να υπολογίσουμε πόσες από αυτές τις $n!$ διαφορετικές διατάξεις δεν διακρίνονται αν αγνοήσουμε την αρίθμηση των μπαλών κάθε χρώματος. Οι n_1 μπάλες του χρώματος 1, μπορούν να αναδιαταχθούν σε $n_1!$ διαφορετικούς τρόπους, που θα δίδουν το ίδιο αποτέλεσμα όταν αγνοήσουμε την αρίθμηση. Παρόμοια, οι n_2 μπάλες χρώματος 2, μπορούν να αναδιαταχθούν σε $n_2!$ διαφορετικούς τρόπους, κ.ο.κ. Εάν συμβολίσουμε $M(n_1, n_2, \ldots, n_r)$ τον αριθμό των μεταθέσεων n αντικειμένων που διακρίνονται σε r ομάδες μεγέθους $n_1, n_2, \ldots, n_r$, $n = n_1 + n_2 + \ldots + n_r$, τότε από τα προηγούμενα έχουμε

$$n_1!\, n_2! \ldots n_r!\, M(n_1, n_2, \ldots, n_r) = n!$$

Πρόταση 7.13 *Ο αριθμός των μεταθέσεων n αντικειμένων που διακρίνονται σε r ομάδες μεγέθους $n_1, n_2, \ldots, n_r$, $n = n_1 + n_2 + \ldots + n_r$, είναι*

$$M(n_1, n_2, \ldots, n_k) = \frac{n!}{n_1!\, n_2! \ldots n_r!}$$

Παράδειγμα 7.5 Με πόσους διαφορετικούς τρόπους μπορούν να διαταχθούν τα γράμματα της λέξης

ΜΙΣΣΙΣΣΙΠΠΗΣ;

Έχουμε 5 διαφορετικά γράμματα, Μ, Ι, Σ, Π, Η. Τα Μ, Η εμφανίζονται μία φορά, το Π εμφανίζεται 2 φορές, το Ι τρείς φορές και το Σ πέντε φορές. Άρα $n = 12$, $n_1 = n_2 = 1$, $n_3 = 2$, $n_4 = 3$, $n_5 = 5$. Έχουμε $M(1, 1, 2, 3, 5)$ διαφορετικές διατάξεις,

$$M(1, 1, 2, 3, 5) = \frac{12!}{2 \cdot 3! \cdot 5!} = 332640.$$

IV. Συνδυασμοί n στοιχείων ανά k, με επανάληψη.

Υποθέτουμε οτι έχουμε μία σακούλα με n μπάλες, αριθμημένες από το 1 έως το n, και ένα πίνακα με n στήλες:

1	2	...	n

Επιλέγουμε μία μπάλα από τη σακούλα και σημειώνουμε ένα σταυρό στη στήλη που αντιστοιχεί στον αριθμό της. Κατόπιν επιστρέφουμε τη μπάλα στη σακούλα. Επαναλαμβάνουμε τη διαδικασία k φορές (όπου k μπορεί να είναι μεγαλύτερο από το n). Το αποτέλεσμα μπορεί να είναι ένας πίνακας σαν τον ακόλουθο, όπου $n = 4$ και $k = 5$:

1	2	3	4
× ×		× ×	×

Σε αυτή την περίπτωση επιλέξαμε 2 φορές τη μπάλα 1, 2 φορές τη μπάλα 3, και μία φορά τη μπάλα 4, ενώ δεν επιλέξαμε τη μπάλα 2. Μπορούμε να συμπτύξουμε τον πίνακα, χωρίς να χάσουμε την πληροφορία που περιέχει, αν γράψουμε μία σειρά από σταυρούς × και γραμμές |:

$$\times\ \times\ |\,|\ \times\ \times\,|\,\times$$

Βλέπουμε οτι υπάρχει μία αμφιμονοσήμαντη συνάρτηση από τους συνδυασμούς n στοιχείων ανά k με επανάληψη, στις διατάξεις k σταυρών και $n-1$ γραμμών. Από την περίπτωση III.α. γνωρίζουμε οτι ο αριθμός αυτών των διατάξεων είναι

$$M(k,\, n-1) = \frac{(n+k-1)!}{k!\,(n-1)!} = \binom{n+k-1}{k}$$

Πρόταση 7.14 *Ο αριθμός των συνδυασμών n στοιχείων ανά k με επανάληψη δίδεται από το διωνυμικό συντελεστή* $\binom{n+k-1}{k}$

Πείραμα Κατανομής

Εξετάζουμε το πείραμα τοποθέτησης k κερμάτων σε n κουτιά. Δεν είναι δύσκολο να αντιληφθούμε οτι υπάρχει μία αντιστοιχία ανάμεσα σε αυτό το πείραμα και το πείραμα επιλογής. Υποθέτουμε οτι έχουμε n κουτιά, αριθμημένα από το 1 έως το n, και k κέρματα, αριθμημένα από το 1 έως το k. Τοποθετούμε τα k κέρματα στα n κουτιά. Οι παραλλαγές που σχετίζονται με τη διάταξη και την επανάληψη στο πείραμα επιλογής, στο πείραμα κατανομής έχουν να κάνουν με το εάν σημειώνουμε τους αριθμούς των κερμάτων, και εάν επιτρέπεται να τοποθετήσουμε περισσότερα από ένα κέρματα σε κάθε κουτί.

Η μετάφραση ανάμεσα στα δύο πειράματα είναι απλή:

ΕΠΙΛΟΓΗ	ΚΑΤΑΝΟΜΗ
μπάλα	κουτί
αριθμός επιλογής	αριθμός κέρματος
j επιλογή είναι μπάλα i	κέρμα j τοποθετείται στο κουτί i

Οι τέσσερεις βασικές παραλλαγές του πειράματος επιλογής αντιστοιχούν στα ακόλουθα πειράματα κατανομής.

I. Κάθε κουτί μπορεί να περιέχει απεριόριστο αριθμό κερμάτων, και σημειώνουμε τους αριθμούς στα κέρματα.

II. Κανένα κουτί δεν μπορεί να περιέχει περισσότερα από ένα κέρμα, και σημειώνουμε τους αριθμούς στα κέρματα.

III. Κανένα κουτί δεν μπορεί να περιέχει περισσότερα από ένα κέρμα, και δεν σημειώνουμε τους αριθμούς στα κέρματα.

IV Κάθε κουτί μπορεί να περιέχει απεριόριστο αριθμό κερμάτων, και δεν σημειώνουμε τους αριθμούς στα κέρματα.

Σε ορισμένες περιπτώσεις, οι επιπλέον συνθήκες που θέλουμε να επιβάλουμε σε ένα πείραμα, εκφράζονται πιο φυσιολογικά για το πείραμα κατανομής παρά για το πείραμα επιλογής.

Παράδειγμα 7.6 Με πόσους τρόπους μπορούμε να χωρίσουμε 4 άτομα σε δύο ζεύγη;

Το πρόβλημα αντιστοιχεί στο πείραμα κατανομής 4 κερμάτων σε δύο κουτιά, έτσι ώστε να τοποθετηθούν ακριβώς δύο κέρματα σε κάθε κουτί, και λαμβάνοντας υπ' όψιν τους αριθμούς στα κέρματα. Βρίσκουμε 3 δυνατότητες:

1 2	3 4	1 3	2 4	1 4	2 3

Αυτό είναι σωστό εάν δεν ενδιαφέρει η διάταξη των δύο ζευγών. Εάν όμως ενδιαφέρει (για παράδειγμα, το πρώτο ζεύγος έχει το σερβίς σε αγώνα τένις) τότε έχουμε άλλες τρείς δυνατότητες, που προκύπτουν από μεταθέσεις των ζευγών:

3 4	1 2	2 4	1 3	1 4	2 3

Γενικότερα, εξετάζουμε το πρόβλημα κατανομής k αριθμημένων κερμάτων, σε n αριθμημένα κουτιά, έτσι ώστε να τοποθετηθούν k_j κέρματα στο κουτί j, $k_1 + k_2 + \ldots + k_n = k$. Έχουμε $\binom{k}{k_1}$ τρόπους να επιλέξουμε τα k_1 κέρματα που θα τοποθετηθούν στο κουτί 1. Κατόπιν έχουμε $\binom{k-k_1}{k_2}$ τρόπους να επιλέξουμε τα k_2 κέρματα του κουτιού 2, κ.ο.κ. Ο αριθμός των τρόπων να κατανείμουμε τα κέρματα είναι:

$$
\begin{aligned}
&\binom{k}{k_1}\binom{k-k_1}{k_2}\binom{k-k_1-\ldots-k_{n-1}}{k_n} = \\
=\;& \frac{k!}{k_1!(k-k_1)!}\,\frac{(k-k_1)!}{k_2!(k-k_1-k_2)!}\,\frac{(k-k_1-k_2)!}{k_3!(k-k_1-k_2-k_3)!} \\
&\ldots\frac{(k-k_1-k_2-\ldots-k_{n-1})!}{k_n!\,0!} \\
=\;& \frac{k!}{k_1!\,k_2!\,\ldots\,k_n!} \\
=\;& M(k_1, k_2, \ldots, k_n)\,.
\end{aligned}
$$

Ασκήσεις

Υποδείξεις για Ασκήσεις Συνδυαστικής

α΄. Εάν δεν βλέπετε πως να προσεγγίσετε ένα πρόβλημα, δοκιμάστε κάποια περίπτωση με σχετικά μικρούς αριθμούς. Αυτό θα σας βοηθήσει να επισημάνετε τι πρέπει να μετρηθεί, καθώς και τυχόν επαναλήψεις ή παραλείψεις.

β΄. Σπάστε το πρόβλημα σε μικρότερα, εάν αυτά είναι απλούστερα στο χειρισμό. Συχνά βοηθά να σταθεροποιήσετε μία 'μεταβλητή' και κατόπιν να μετρήσετε τις όμοιες περιπτώσεις.

γ΄. Δεν είναι πάντα σκόπιμο να επιχειρήσετε μια βήμα προς βήμα προσέγγιση. Οι περιπλοκές μπορεί να αυξάνουν απότομα.

Άσκηση 7.1 Θέλετε να αγοράσετε για δώρο ένα πουκάμισο ή/ και μία γραβάτα.Υπάρχουν τρία διαφορετικά ποκάμισα και δύο διαφορετικές γραβάτες.

α΄. Πόσες δυνατότητες έχετε να αγοράσετε ένα ποκάμισο ή μία γραβάτα;.

β΄. Πόσες δυνατότητες έχετε να αγοράσετε ένα ποκάμισο και μια γραβάτα;

Άσκηση 7.2 Πόσα διαφορετικά αρχικά μπορείτε να γράψετε με 2 ή 3 γράμματα του ελληνικού αλφαβήτου;

Άσκηση 7.3 Με πόσους διαφορετικούς τρόπους μπορείτε να επιλέξετε μία επιτροπή 3 ατόμων από 20 άτομα;
Με πόσους τρόπους μπορείτε να επιλέξετε πρόεδρο, γραμματέα και ταμία από 20 άτομα;

Άσκηση 7.4 Εάν έχετε 2 κέρματα του 1 ευρώ, 2 εικοσάλεπτα και 3 πεντάλεπτα, πόσα διαφορετικά ποσά μπορείτε να πληρώσετε, χωρίς να χρειαστείτε ρέστα;

Άσκηση 7.5 Με πόσους τρόπους μπορείτε να διαλέξετε 4 παπούτσια από 5 διαφορετικά ζευγάρια;
Σε πόσους από αυτούς έχετε τουλάχιστον ένα ζευγάρι;

Άσκηση 7.6 Με πόσους τρόπους μπορείτε να μοιράσετε 10 βιβλία σε δύο στοίβες, έτσι ώστε κάθε στοίβα να έχει τουλάχιστον 1 βιβλίο; Εξετάστε τις τέσσερεις διαφορετικές περιπτώσεις, ανάλογα με το αν τα βιβλία και οι στοίβες θεωρούνται διαφορετικά ή όχι.

Άσκηση 7.7 Με πόσους διαφορετικούς τρόπους μπορούν να 'ανακατωθούν' τα 52 χαρτιά της τράπουλας;
Σε πόσους από αυτούς βρίσκονται οι τέσσερεις άσσοι σε διαδοχικές θέσεις;
Σε πόσους τα 5 πρώτα χαρτιά έχουν το ίδιο 'χρώμα';
(Στην τράπουλα υπάρχουν 4 διαφορετικά 'χρώματα'.)

Άσκηση 7.8 Με πόσους τρόπους μπορούμε να τοποθετήσουμε n μπάλες σε n κουτιά, έτσι ώστε να μείνει ακριβώς ένα κουτί άδειο. Εξετάστε δύο περιπτώσεις: εάν οι μπάλες είναι όλες ίδιες ή όλες διαφορετικές.

Κεφάλαιο 8

Το άπειρο

Πληθικοί αριθμοί

'Τι είναι το άπειρο;' Μία πιθανή απάντηση που θα δώσει ένας μη ειδικός σε αυτό το ερώτημα είναι 'κάτι μεγαλύτερο από κάθε φυσικό αριθμό'. Με μία αυστηρή έννοια, αυτό είναι σωστό. Ένας από τους θριάμβους της θεωρίας συνόλων είναι οτι η έννοια του απείρου μπορεί να λάβει σαφές νόημα. Βρίσκουμε οτι δεν υπάρχει μόνο ένα, αλλά πολλά, μία τεράστια ιεραρχία από άπειρα. Μπορούμε να απαντήσουμε ένα ερώτημα όπως 'πόσοι πολλοί ρητοί αριθμοί υπάρχουν;' με την απρόσμενη απάντηση 'τόσοι όσοι είναι οι φυσικοί αριθμοί'. Τα πιο χρήσιμα ερωτήματα είναι αυτού του τύπου. Αντί να ρωτάμε 'πόσα' στοιχεία υπάρχουν σε ένα σύνολο, είναι πολύ πιο αποτελεσματικό να συγκρίνουμε δύο σύνολα, και να ρωτάμε εάν υπάρχει το ίδιο πλήθος στοιχείων στα δύο. Λέμε οτι 'υπάρχει το ίδιο πλήθος στοιχείων' στα σύνολα A και B εάν υπάρχει μία αμφιμονοσήμαντη συνάρτηση $f : A \to B$. Αντί να αρχίσουμε με όλη την ιεραρχία των απείρων, ας αρχίσουμε με αυτό που, όπως θα δούμε, είναι το μικρότερο. Ως βασικό σύνολο για σύγκριση θα θεωρήσουμε τους φυσικούς αριθμούς $\mathbb{N}$. Είναι προτιμότερο να χρησιμοποιήσουμε το $\mathbb{N}$ αντί για το $\mathbb{N}_0$, επειδή η αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to B$ βάζει τα στοιχεία του B σε μία ακολουθία: ονομάζουμε $f(1)$ το πρώτο στοιχείο του B, $f(2)$ το δεύτερο, κλπ. Με αυτή τη διαδικασία έχουμε ένα τρόπο να *απαριθμήσουμε* το B. Βεβαίως εάν απαριθμούμε τα στοιχεία χρησιμοποιώντας αυτή την αντιστοιχία, '$f(1)$, $f(2), \ldots$', δεν φτάνουμε ποτέ στο τέλος, αλλά γνωρίζουμε οτι για κάθε στοιχείο $b \in B$, $b = f(n)$ για κάποιο $n \in \mathbb{N}$, και συνεπώς θα φτάσουμε κάποια στιγμή αυτό το στοιχείο.

Υπενθυμίζουμε από το Κεφάλαιο 7 οτι ορίσαμε $\mathbb{N}(0) = \varnothing$ και για κάθε $n \in \mathbb{N}$, $\mathbb{N}(n) = \{m \in \mathbb{N} \,|\, 1 \leq m \leq n\}$. Λέμε οτι το σύνολο X είναι **πεπερασμένο** εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}(n) \to X$ για κάποιο $n \in \mathbb{N}_0$. Λέμε οτι X είναι **αριθμήσιμο** είτε εάν το X είναι πεπερασμένο είτε εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to X$. Εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}(n) \to X$, τότε λέμε οτι το X έχει n στοιχεία. Αυτή είναι η συνηθισμένη διαδικασία απαρίθμησης. Εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to X$, λέμε οτι το X έχει $\aleph_0$ στοιχεία. Το σύμβολο $\aleph$ είναι το πρώτο γράμμα του εβραϊκού αλφαβήτου, και ονομάζεται άλεφ. $\aleph_0$ είναι το πρώτο παράδειγμα που συναντάμε μίας νέας έννοιας αριθμού, που χρησιμοποιείται για να εκφράσουμε πόσο μεγάλο είναι ένα άπειρο σύνολο. Όταν λέμε οτι ένα σύνολο X έχει $\aleph_0$ στοιχεία, σημαίνει απλά οτι υπάρχει αμφιμονοσήμαντη συνάρτηση μεταξύ του $\mathbb{N}$ και του X, που σημαίνει ακριβώς οτι 'το X έχει τον ίδιο **πληθικό αριθμό** (ή το ίδιο πλήθος στοιχείων) με το $\mathbb{N}$'. Πριν εξετάσουμε πληθικούς αριθμούς γενικότερα, ας δούμε πιο προσεκτικά την έννοια της αριθμησιμότητας.

Παράδειγμα 8.1 $\mathbb{N}_0$ είναι αριθμήσιμο. Ορίζουμε $f : \mathbb{N} \to \mathbb{N}_0$ με $f(n) = n-1$. Η f είναι αμφιμονοσήμαντη συνάρτηση. Αυτή είναι η πρώτη εκπληκτική ιδιότητα αυτού του τρόπου 'απαρίθμησης απείρων συνόλων'. Το $\mathbb{N}$ είναι *γνήσιο υποσύνολο* του $\mathbb{N}_0$, άρα διαισθητικά θα έπρεπε να έχει λιγότερα στοιχεία, όμως με την έννοια της ύπαρξης αμφιμονοσήμαντης συνάρτησης, τα δύο σύνολα έχουν το ίδιο πλήθος στοιχείων.

Ιστορικά, ο Γαλιλαίος έδωσε ένα πιο εντυπωσιακό παράδειγμα το 1638, όταν επέδειξε μία αντιστοιχία μεταξύ των φυσικών αριθμών και των τετραγώνων φυσικών αριθμών:

Παράδειγμα 8.2 (Γαλιλαίος). Υπάρχει αντιστοιχία μεταξύ των φυσικών αριθμών και των τελείων τετραγώνων:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & \ldots & n & \ldots \\ \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \\ 1 & 4 & 9 & 16 & \ldots & n^2 & \ldots \end{array}$$

Στη σύγχρονη συνολοθεωρητική γλώσσα, εάν $S = \{n^2 \in \mathbb{N} \,|\, n \in \mathbb{N}\}$, η απεικόνιση $f : \mathbb{N} \to S$, όπου $f(n) = n^2$, είναι αμφιμονοσήμαντη.

Για περισσότερους από δύο αιώνες, αυτή η φαινομενική αντίφαση απέτρεψε κάθε προσπάθεια να θεωρηθεί το άπειρο με αυστηρότητα. Ο Leibniz έφτασε στο σημείο να προτείνει οτι πρέπει να εξετάζουμε μόνο πεπερασμένα σύνολα, διότι η αντίφαση προκύπτει από την απειρία των φυσικών αριθμών. Η απάντηση του στο πρόβλημα ήταν οτι εάν θεωρούσαμε μόνο πεπερασμένα σύνολα φυσικών αριθμών, ας πούμε τους αριθμούς μέχρι το εκατό, τότε δεν υπάρχει αντιστοιχία μεταξύ των φυσικών αριθμών μέχρι το εκατό και των τελείων τετραγώνων μέχρι το εκατό. Η επίλυση του παράδοξου από τον Cantor στην δεκαετία του 1870 ήταν πιο δραματική. Έδειξε οτι εάν ερμηνεύσουμε 'το ίδιο πλήθος στοιχείων' να σημαίνει 'υπάρχει αμφιμονοσήμαντη συνάρτηση μεταξύ δύο συνόλων', τότε κάθε άπειρο σύνολο έχει το ίδιο πλήθος στοιχείων με ένα γνήσιο υποσύνολό του! Εδώ **άπειρο** εννοείται ένα σύνολο B για το οποίο δεν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}(n) \to B$, για οποιοδήποτε $n \in \mathbb{N}_0$.

Πρόταση 8.1 (Cantor) *Εάν ένα σύνολο B είναι άπειρο, τότε υπάρχει ένα γνήσιο υποσύνολο $A \subseteq B$, $A \neq B$, και μία αμφιμονοσήμαντη συνάρτηση $f : B \to A$.*

Απόδειξη. Πρώτα επιλέγουμε ένα άπειρο υποσύνολο X του B, με τον ακόλουθο τρόπο. Αφού δεν υπάρχει αμφιμονοσήμαντη συνάρτηση μεταξύ $\mathbb{N}(0)$ και B, το B δεν είναι κενό, και υπάρχει κάποιο στοιχείο στο B, το οποίο ονομάζουμε x_1. Ορίζουμε μία συνάρτηση $g : \mathbb{N} \to B$ ως εξής: $g(1) = x_1$, και εάν έχουμε επιλέξει τα διαφορετικά στοιχεία $x_1, x_2, \ldots, x_n$, αφού δεν υπάρχει αμφιμονοσήμαντη συνάρτηση $g : \mathbb{N}(n) \to B$, πρέπει να υπάρχει κάποιο άλλο στοιχείο του B, το οποίο ονομάζουμε x_{n+1}, και το οποίο είναι διαφορετικό από τα $x_1, \ldots, x_n$. Ορίζουμε $g(n+1) = x_{n+1}$. Θεωρούμε το σύνολο

$$X = \{x_n \in B \,|\, n \in \mathbb{N}\}.$$

Τώρα θεωρούμε το σύνολο $A = B \setminus \{x_1\}$ και ορίζουμε $f : B \to A$ με

$$f(x_n) = x_{n+1} \text{ για } x_n \in X$$

και

$$f(b) = b \text{ για } b \notin X.$$

Η συνάρτηση f είναι αμφιμονοσήμαντη.

$\square$

Χρησιμοποιώντας το παράδειγμα του Γαλιλαίου, μπορούμε να επιλέξουμε και ένα υποσύνολο $C \subseteq B$, όπου $B \setminus C$ είναι άπειρο, και όμως υπάρχει αμφιμονοσήμαντη συνάρτηση $f : B \to C$. Αρκεί να επιλέξουμε ένα σύνολο X όπως στην απόδειξη, να θεωρήσουμε το σύνολο

$$C = B \setminus \{x_n \in X \,|\, n \text{ δεν είναι τέλειο τετράγωνο}\}$$

και να ορίσουμε τη συνάρτηση $f : B \to C$ με

$$f(x_n) = x_{n^2} \text{ για } x_n \in X$$

και

$$f : (b) = b \text{ για } b \notin X.$$

Ξεκινώντας με ένα άπειρο σύνολο B, μπορούμε να αφαιρέσουμε ένα (αριθμήσιμο) άπειρο υποσύνολο, και όμως να μας μείνει ένα υποσύνολο C το οποίο έχει 'το ίδιο πλήθος στοιχείων' με το B!

Ο Cantor έλυσε το πρόβλημα του απείρου εισάγοντας την έννοια του **πληθικού αριθμού**. Προς στιγμήν, θα υποθέσουμε οτι για κάθε σύνολο X υπάρχει μία έννοια, που ονομάζεται πληθικός αριθμός με την ιδιότητα οτι εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : X \to Y$, τότε το X και το Y έχουν τον ίδιο πληθικό αριθμό, και εάν δεν υπάρχει τέτοια συνάρτηση οι πληθικοί αριθμοί τους είναι διαφορετικοί. Για πεπερασμένα σύνολα έχουμε ένα κατάλληλο υποψήφιο για πληθικό αριθμό. Εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N}(n) \to X$, μπορούμε να πούμε οτι ο πληθικός αριθμός του X είναι n. Παρόμοια, εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to X$, λέμε οτι ο πληθικός αριθμός του X είναι $\aleph_0$. Για άλλα άπειρα σύνολα μπορεί να χρειαστούμε νέα σύμβολα για τους πληθικούς αριθμούς τους. Γενικά, θα συμβολίζουμε το πληθικό αριθμό (ή πληθάριθμο) του X με $|X|$ ή $\operatorname{card}(X)$, και εάν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : X \to Y$ θα θεωρούμε οτι $|X| = |Y|$. Σε αυτήν την περίπτωση $|X|$ και $|Y|$ είναι διαφορετικά σύμβολα για τον ίδιο πληθικό αριθμό. Εάν υπάρχει μία ενεικονική συνάρτηση $f : X \to Y$ τότε θα λέμε οτι $|X| \leq |Y|$. Εάν $|X| \leq |Y|$ και $|X| \neq |Y|$, λέμε οτι $|X| < |Y|$. Γενικά, εάν X είναι υποσύνολο του Y, ο εγκλεισμός $i : X \to Y$, $i(x) = x$, είναι ενεικόνιση, άρα ισχύει

$$X \subseteq Y \Rightarrow |X| \leq |Y|.$$

Η Πρόταση 8.1 λέει οτι, για κάθε άπειρο σύνολο B, υπάρχει γνήσιο υποσύνολο A τέτοιο ώστε $|A| = |B|$. Άρα, για άπειρα σύνολα, $X \subseteq Y$ και $X \neq Y$ δεν συνεπάγονται οτι $|X| < |Y|$.

Το δίλημμα που τέθηκε από το παράδειγμα του Γαλιλαίου είναι περισσότερο ψυχολογικό παρά μαθηματικό. Καθώς επεκτείνουμε το σύστημα των φυσικών αριθμών και την απαρίθμηση για να συμπεριλάβουμε άπειρους πληθικούς αριθμούς, το μεγαλύτερο σύστημα μπορεί να μην έχει όλες τις ιδιότητες του μικρότερου. Η οικειότητα με το μικρότερο σύστημα μας οδηγεί να αναμένουμε ορισμένες ιδιότητες, και συγχυζόμαστε όταν τα κομμάτια δεν ταιριάζουν όπως τα περιμέναμε. Παρόμοια ανασφάλεια προέκυψε όταν το τετράγωνο ενός μιγαδικού αριθμού παραβίασε τον κανόνα των πραγματικών αριθμών οτι το τετράγωνο κάθε αριθμού είναι θετικό. Αυτό ξεπεράστηκε όταν αντιληφθήκαμε οτι οι μιγαδικοί αριθμοί δεν επιδέχονται μία διάταξη, όπως γίνεται για το υποσύνολο των πραγματικών αριθμών. Ανάλογα, η φαινομενική αντίφαση του Γαλιλαίου επιλύεται όταν αντιληφθούμε οτι εάν εννοήσουμε ‘τον ίδιο πληθικό αριθμό’ ως μία αμφιμονοσήμαντη αντιστοιχία μεταξύ συνόλων, το γνήσιο υποσύνολο A του B δεν αποκλείεται να έχει τον ίδιο άπειρο πληθικό αριθμό με το B.

Ας εξετάσουμε τώρα την έννοια της αριθμησιμότητας. Αρχικά, για κάθε άπειρο σύνολο B μπορούμε, όπως στην απόδειξη της Πρότασης 8.1 να επιλέξουμε ένα άπειρο αριθμήσιμο σύνολο $X \subseteq B$. Αυτό σημαίνει οτι $\aleph_0 = |X| \leq |B|$, και συνεπώς $\aleph_0$ είναι ο μικρότερος άπειρος πληθικός αριθμός. Προκαλεί έκπληξη πόσα από τα γνωστά μας σύνολα, που φαίνεται να είναι πολύ μεγαλύτερα από το $\mathbb{N}$, έχουν τον ίδιο πληθικό αριθμό $\aleph_0$.

Παράδειγμα 8.3 Το σύνολο των ακεραίων είναι αριθμήσιμο.
Ορίζουμε $f : \mathbb{N} \to \mathbb{Z}$ με

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

και έχουμε την αντιστοιχία

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \dots \end{array}$$

Προσέξτε οτι αν και f είναι αμφιμονοσήμαντη συνάρτηση, δεν διατηρεί τη διάταξη: $m < n$ δεν συνεπάγεται οτι $f(m) < f(n)$, για παράδειγμα $f(2) > f(3)$. Όταν ορίζουμε αμφιμονοσήμαντες αντιστοιχίες μεταξύ συνόλων με διάταξη, μπορεί να χρειαστεί να ανακατέψουμε πολύ τα πράγματα, όπως δείχνει το επόμενο παράδειγμα.

Παράδειγμα 8.4 Το σύνολο των ρητών αριθμών είναι αριθμήσιμο. Θα το δείξουμε αυτό σε βήματα, αρχίζοντας από τους θετικούς ρητούς. Ένας τρόπος να απαριθμήσουμε τους ρητούς είναι να γράψουμε όλα τα κλάσματα σε ένα πίνακα

$$\begin{array}{ccccc} 1/1 & 1/2 & 1/3 & 1/4 & \dots \\ 2/1 & 2/2 & 2/3 & 2/4 & \dots \\ 3/1 & 3/2 & 3/3 & 3/4 & \dots \\ 4/1 & 4/2 & 4/3 & 4/4 & \dots \\ \vdots & \vdots & \vdots & \vdots & \end{array}$$

και να τα διαβάζουμε κατά μήκος ‘χιαστί διαγωνίων’, $1/1$, κατόπιν $1/2$, $2/1$, κατόπιν $1/3$, $2/2$, $3/1$, κ.ο.κ. Με αυτό τον τρόπο παίρνουμε μια ακολουθία $1/1$, $1/2$, $2/1$, $1/3$, $2/2$, $3/1, \dots$ στην οποία περιέχονται όλοι οι ρητοί, αλλά υπάρχουν επαναλήψεις, επειδή $1/1 = 2/2$, και πιο πέρα θα έχουμε $3/3$, $4/4$ κλπ. Παρόμοια $1/2 = 2/4 = 3/6$ κλπ. Θεωρούμε κάθε στοιχείο στην ακολουθία, και το διαγράφουμε εάν έχει ήδη εμφανιστεί. Το αρχικό κομμάτι της ακολουθίας που απομένει είναι

$$1/1,\ 1/2,\ 2/1,\ 1/3,\ 3/1,\ \dots$$

Ονομάζουμε το n-οστό αριθμό στην εναπομείνασα ακολουθία a_n, και ορίζουμε τη συνάρτηση f από τους φυσικούς στους θετικούς ρητούς με $f(n) = a_n$. Αλλά κάθε ρητός αριθμός είναι είτε θετικός ή μηδέν ή αρνητικός, και συνεπώς η ακολουθία

$$0,\ a_1,\ -a_1,\ a_2,\ -a_2, \dots,\ a_n,\ -a_n,\ \dots$$

περιέχει κάθε ρητό αριθμό ακριβώς μία φορά. Η συνάρτηση $g : \mathbb{N} \to \mathbb{Q}$ που ορίζεται ως

$$g(k) = \begin{cases} 0 & \text{εάν} \quad k = 1 \\ a_n & \text{εάν} \quad k = 2n \\ -a_n & \text{εάν} \quad k = 2n+1 \end{cases}$$

είναι η ζητούμενη αμφιμονοσήμαντη συνάρτηση. Αξίζει να επισημάνουμε οτι, αν και δεν έχουμε δώσει ένα τύπο για τη συνάρτηση $g(n)$, έχουμε μία συγκεκριμένη διαδικασία για τον υπολογισμό της. Οι πρώτοι όροι είναι:

$$\begin{array}{cccccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & 1 & -1 & \frac{1}{2} & -\frac{1}{2} & 2 & -2 & \frac{1}{3} & -\frac{1}{3} & 3 & -3 & \frac{1}{4} & \dots \end{array}$$

και θα μπορούσαμε να συνεχίσουμε όσο θέλουμε.

Σε πιο προχωρημένα μαθήματα Θεωρίας Συνόλων θα δούμε ένα πολύ ισχυρότερο αποτέλεσμα (το θεώρημα Schroeder–Bernstein) που μας επιτρέπει να δείξουμε οτι δύο σύνολα έχουν τον ίδιο πληθικό αριθμό χωρίς να χρειαστεί να κατασκευάσουμε μία συγκεκριμένη αμφιμονοσήμαντη απεικόνιση.

Ο λόγος για τον οποίο ορίσαμε τον όρο αριθμήσιμο να περιλαμβάνει τόσο τα πεπερασμένα όσο και τα αριθμήσιμα άπειρα σύνολα φαίνεται στο επόμενο αποτέλεσμα.

Πρόταση 8.2 *Ένα υποσύνολο αριθμήσιμου συνόλου είναι αριθμήσιμο.*

Απόδειξη. Εάν έχουμε μία αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to A$, και $B \subseteq A$, τότε είτε το B είναι πεπερασμένο, είτε μπορούμε να ορίσουμε μία συνάρτηση $g : \mathbb{N} \to B$ με

- $g(1) = f(m)$ όπου m είναι το ελάχιστο $m \in \mathbb{N}$ για το οποίο $f(m) \in B$.

- Εάν έχουμε ορίσει τα $g(1)$, $g(2)$, …, $g(n)$, τότε $g(n+1) = f(m)$ όπου m είναι το ελάχιστο $m \in \mathbb{N}$ για το οποίο $f(m) \in B \setminus \{g(1), \dots, g(n)\}$.

□

Μία αξιοσημείωτη ιδιότητα των αριθμήσιμων συνόλων είναι οτι μπορούμε να κατασκευάσουμε από αυτά σύνολα που φαίνεται να είναι πολύ μεγαλύτερα, τα οποία όμως είναι πάλι αριθμήσιμα.

Πρόταση 8.3 *Η ένωση μίας αριθμήσιμης οικογένειας αριθμήσιμων συνόλων είναι αριθμήσιμο σύνολο.*

Απόδειξη. Εάν έχουμε μια αριθμήσιμη συλλογή συνόλων, μπορούμε να θεωρήσουμε το $\mathbb{N}$ ως το σύνολο δεικτών, και να γράψουμε τα σύνολα A_n, $n \in \mathbb{N}$. (Εάν η συλλογή περιλαμβάνει μόνο πεπερασμένο πλήθος συνόλων $A_1, \dots, A_k$, θέτουμε $A_n = \varnothing$ για $n > k$.) Αφού κάθε A_n είναι αριθμήσιμο, μπορούμε να γράψουμε τα στοιχεία του A_n σε μία γραμμή,

$$a_{n1},\ a_{n2},\ \dots,\ a_{nm},\ \dots$$

η οποία θα τελειώνει εάν το A_n είναι πεπερασμένο, ενώ θα είναι μία άπειρη ακολουθία εάν το A_n είναι άπειρο αριθμήσιμο. Τώρα καταγράφουμε τα στοιχεία της ένωσης $\bigcup_{n\in\mathbb{N}} A_n$ σε ένα πίνακα,

$$\begin{array}{cccccc} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & \dots \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & \dots \\ a_{31} & a_{32} & a_{33} & & & \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

και τα διαβάζουμε κατα μήκος των χιαστί διαγωνίων, όπως κάναμε για να απαριθμήσουμε τους ρητούς αριθμούς: a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, ... Μπορεί να υπάρχουν κενά στον πίνακα, εάν κάποια από τα σύνολα είναι πεπερασμένα (όπως το A_3 στο παράδειγμα), ή εάν το πλήθος των συνόλων είναι πεπερασμένο. Μπορεί να υπάρχουν επαναλήψεις εάν κάποια σύνολα έχουν κοινά στοιχεία, έτσι ώστε ένα στοιχείο στη γραμμή n να επαναλαμβάνεται στη γραμμή m. Απλώς προσπερνάμε τα κενά, και τα στοιχεία που έχουν ήδη εμφανιστεί. Αυτή η διαδικασία δίδει είτε μία πεπερασμένη ακολουθία, είτε μία άπειρη ακολουθία χωρίς επαναλήψεις, και δείχνει οτι η ένωση $\bigcup_{n\in\mathbb{N}} A_n$ είναι αριθμήσιμο σύνολο.

□

Πρόταση 8.4 *Το καρτεσιανό γινόμενο δύο αριθμήσιμων συνόλων είναι αριθμήσιμο σύνολο.*

Απόδειξη. Εάν A και B είναι αριθμήσιμα, γράφουμε τα στοιχεία του A ως μία ακολουθία $a_1, a_2, \dots, a_n, \dots$ (η οποία θα τελειώνει εάν A είναι πεπερασμένο). Παρόμοια γράφουμε τα στοιχεία του B ως $b_1, b_2, \dots, b_m, \dots$ Τώρα γράφουμε τα στοιχεία του καρτεσιανού γινομένου $A \times B$ σε ένα ορθογώνιο πίνακα,

$$\begin{array}{cccc} (a_1, b_1) & (a_1, b_2) & (a_1, b_3) & \dots \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) & \dots \\ (a_3, b_1) & (a_3, b_2) & (a_3, b_3) & \dots \\ \vdots & \vdots & \vdots & \end{array}$$

και τα διαβάζουμε κατα μήκος των χιαστί διαγωνίων. Εάν ένα από τα A ή B είναι πεπερασμένο, θα υπάρχουν κενά, τα οποία παραλείπουμε. Εάν και τα δύο είναι πεπερασμένα, το γινόμενο $A \times B$ είναι πεπερασμένο. Εάν και τα δύο είναι άπειρα , μπορούμε να γράψουμε αναλυτικά τον τύπο της αμφιμονοσήμαντης συνάρτησης $f : \mathbb{N} \to A \times B$. Υπάρχει ένα στοιχείο στην πρώτη χιαστί διαγώνιο, δύο στη δεύτερη, και γενικά n στη n-οστή. Άρα υπάρχουν $1 + 2 + \ldots + n = \frac{1}{2}n(n+1)$ στοιχεία στις n πρώτες χιαστί διαγώνιους. Το r-οστό στοιχείο στην επόμενη χιαστί διαγώνιο είναι το (a_r, b_{n+2-r}), άρα η αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to A \times B$ είναι

$$f(m) = (a_r, b_{n+2-r}) \text{ όπου } m = \frac{1}{2}n(n+1) + r \text{ για } 1 \le r \le n+1 . \quad \square$$

Ως εφαρμογή της Πρότασης 8.4 έχουμε το ακόλουθο αποτέλεσμα.

Παράδειγμα 8.5 Το σύνολο των σημείων του επιπέδου με ρητές συντεταγμένες είναι αριθμήσιμο.

Σε αυτό το σημείο, δικαιολογημένα, θα μπορούσε κανείς να υποθέσει οτι κάθε άπειρο σύνολο είναι αριθμήσιμο, αλλά αυτό δεν ισχύει, όπως θα δούμε εξετάζοντας τους πραγματικούς αριθμούς.

Θεώρημα 8.5 *Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών δεν είναι αριθμήσιμο.*

Απόδειξη. Αυτό το αποδεικνύουμε με απαγωγή σε άτοπο, δείχνοντας οτι καμία συνάρτηση $f : \mathbb{N} \to \mathbb{R}$ δεν μπορεί να είναι επί, και άρα δεν υπάρχει αμφιμονοσήμαντη συνάρτηση $f : \mathbb{N} \to \mathbb{R}$. Εάν $f : \mathbb{N} \to \mathbb{R}$ είναι μία συνάρτηση, γράφουμε κάθε αριθμό $f(m) \in \mathbb{R}$ σε δεκαδική παράσταση

$$f(m) = a_m, \, a_{m1}\, a_{m2}\, a_{m3} \, \ldots \, a_{mn} \, \ldots$$

όπου a_m είναι ακέραιος, και για κάθε n, a_{mn} είναι το n-οστό δεκαδικό ψηφίο του $f(m)$, $0 \leq a_{mn} \leq 9$. Για παράδειγμα, εάν $f(m) = \sqrt{2} = 1,41421356...$ έχουμε $a_m = 1$, $a_{m1} = 4$, $a_{m2} = 1$, $a_{m3} = 4$, $a_{m4} = 2$, ...

Εάν $f(m)$ είναι δεκαδικό κλάσμα, όπως ο $\frac{125}{100} = 1,25$, συμπληρώνουμε την δεκαδική παράσταση με μηδενικά, 1,250000... Έτσι έχουμε μία ακολουθία

$$\begin{array}{rcl}
f(1) & = & a_1, \, a_{11}\, a_{12}\, a_{13} \ldots \\
f(2) & = & a_2, \, a_{21}\, a_{22}\, a_{23} \ldots \\
f(3) & = & a_3, \, a_{31}\, a_{32}\, a_{33} \ldots \\
\vdots & & \qquad \vdots \\
f(n) & = & a_n, \, a_{n1}\, a_{n2}\, a_{n3} \ldots \\
\vdots & & \qquad \vdots
\end{array}$$

Θα δείξουμε οτι η συνάρτηση f δεν είναι επί, γράφοντας τη δεκαδική παράσταση ενός αριθμού που είναι διαφορετικός από όλα τα $f(n)$. Έστω ο αριθμός $\beta = 0, \, b_1\, b_2 \, \ldots \, b_n \, \ldots$ όπου

$$b_n = \begin{cases} 1 & \text{εάν} \quad a_{nn} = 0 \\ 0 & \text{εάν} \quad a_{nn} \neq 0 \end{cases}$$

Τότε ο β είναι διαφορετικός από τον $f(n)$, γιατί διαφέρει στο n-οστό δεκαδικό ψηφίο, $b_n \neq a_{nn}$.

Αυτό το επιχείρημα ονομάζεται **διαγώνιο επιχείρημα του Cantor** και δείχνει οτι $|\mathbb{N}| \neq |\mathbb{R}|$. Αφού $\mathbb{N} \subseteq \mathbb{R}$, και άρα $|\mathbb{N}| \leq |\mathbb{R}|$, συμπεραίνουμε οτι ο πληθικός αριθμός του συνόλου των πραγματικών αριθμών είναι γνήσια μεγαλύτερος από τον πληθικό αριθμό των φυσικών αριθμών, $|\mathbb{R}| > |\mathbb{N}|$. Συμβολίζουμε τον πληθικό αριθμό του $\mathbb{R}$ με $\mathfrak{c}$. Έχουμε δείξει οτι

$$\mathfrak{c} > \aleph_0.$$

$\square$

Μία παραλλαγή του διαγωνίου επιχειρήματος μπορεί να χρησιμοποιηθεί για να δείξουμε οτι για κάθε πληθικό αριθμό μπορούμε να βρούμε έναν μεγαλύτερο. Απλά δείχνουμε οτι για κάθε σύνολο A το δυναμοσύνολο $\mathfrak{P}(A)$ έχει γνήσια μεγαλύτερο πληθικό αριθμό.

Πρόταση 8.6 *Για κάθε σύνολο A, $|\mathfrak{P}(A)| > |A|$.*

Απόδειξη. Προφανώς η συνάρτηση $g : A \to \mathfrak{P}(A)$ η οποία απεικονίζει το στοιχείο $a \in A$ στο μονοσύνολο $\{a\}$, $g(a) = \{a\}$, είναι ένα προς ένα, και συνεπώς $|A| \leq |\mathfrak{P}(A)|$. Πρέπει να δείξουμε οτι $|A| \neq |\mathfrak{P}(A)|$. Θα δείξουμε οτι καμία συνάρτηση $f : A \to \mathfrak{P}(A)$ δεν είναι επί. Εάν έχουμε μία τέτοια συνάρτηση, $f(a) \in \mathfrak{P}(A)$ για κάθε $a \in A$, άρα $f(a)$ είναι ένα υποσύνολο του A. Άρα για κάθε $a \in A$ μπορούμε να θέσουμε το ερώτημα 'ανήκει το a στο υποσύνολο $f(a)$;'. Η απάντηση είναι πάντα είτε 'ναι' είτε 'όχι'. Επιλέγουμε τα στοιχεία A για τα οποία η απάντηση είναι όχι, και ορίζουμε το σύνολο

$$B = \{a \in A \,|\, a \notin f(a)\}\,.$$

Τώρα ισχυριζόμαστε οτι το υποσύνολο $B \subseteq A$ δεν ανήκει στην εικόνα της f. Πράγματι, εάν B ανήκει στην εικόνα της f, δηλαδή εάν $B = f(b)$ για κάποιο $b \in A$, οδηγούμαστε σε αντίφαση:

$$\text{εάν } b \in B \text{ τότε, από τον ορισμό του } B,\ b \notin f(b) = B$$

$$\text{εάν } b \notin B \text{ τότε, από τον ορισμό του } B,\ b \in f(b) = B$$

Συμπεραίνουμε οτι το $B \in \mathfrak{P}(A)$ δεν ανήκει στην εικόνα της f, και άρα η $f : A \to \mathfrak{P}(A)$ δεν είναι επί. Συνεπώς η f δεν μπορεί να είναι αμφιμονοσήμαντη.

$\square$

Η Πρόταση 8.6 δείχνει οτι υπάρχει μία ιεραρχία από άπειρα. Ξεκινάμε με το $\aleph_0 = |\mathbb{N}|$. Το $|\mathfrak{P}(\mathbb{N})|$ είναι γνήσια μεγαλύτερο, το $|\mathfrak{P}(\mathfrak{P}(\mathbb{N}))|$ είναι πάλι μεγαλύτερο, κ.ο.κ.

Ασκήσεις

Άσκηση 8.1 Θεωρήστε το σύνολο X των σημείων $(x,\, y,\, z) \in \mathbb{R}^3$ για τα οποία $x,\, y,\, z \in \mathbb{Q}$. Είναι το X αριθμήσιμο;

Άσκηση 8.2 Θεωρήστε το σύνολο S των σφαιρών στο $\mathbb{R}^3$ των οποίων τα κέντρα έχουν ρητές συντεταγμένες, και των οποίων η ακτίνα είναι ρητός αριθμός. Δείξτε οτι το S είναι αριθμήσιμο.

Άσκηση 8.3 Ποιά από τα ακόλουθα σύνολα είναι αριθμήσιμα; (Δώστε απόδειξη σε κάθε περίπτωση).

α′. $\{n \in \mathbb{N} \,|\, n \text{ είναι πρώτος}\}$

β′. $\{r \in \mathbb{Q} \,|\, r > 0\}$

γ′. $\{x \in \mathbb{R} \,|\, 1 < x < 10^{-1000000}\}$

δ′. $\mathbb{C}$

ε′. $\{x \in \mathbb{R} \,|\, x^2 = 2^a 3^b \text{ για κάποια } a,\, b \in \mathbb{N}\}$

Άσκηση 8.4 Αποδείξτε οτι η $J : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ με

$$J(n,\, m) = 2^n(2m+1) - 1$$

είναι $1-1$ και επί του $\mathbb{N}_0$.

Άσκηση 8.5 Αποδείξτε οτι κάθε σύνολο ξένων διαστημάτων στο $\mathbb{R}$ είναι αριθμήσιμο. Χρησιμοποιήστε το παραπάνω για να αποδείξετε οτι το σύνολο σημείων ασυνέχειας μιας αύξουσας $f : \mathbb{R} \to \mathbb{R}$ είναι αριθμήσιμο.

Υπόδ. Αν $f : \mathbb{R} \to \mathbb{R}$ είναι αύξουσα, τότε για κάθε $a \in \mathbb{R}$ υπάρχουν τα πλευρικά όρια της f στο a και

$$\lim_{x\to a^-} f(x) \le \lim_{x\to a^+} f(x)$$

Άσκηση 8.6 Αποδείξτε οτι κάθε σύνολο διαστημάτων με ρητά άκρα στο $\mathbb{R}$ είναι αριθμήσιμο. Χρησιμοποιήστε το παραπάνω για να αποδείξετε οτι το σύνολο των τοπικών μεγίστων (ελαχίστων) μιας συνεχούς $f : \mathbb{R} \to \mathbb{R}$ είναι αριθμήσιμο.

Άσκηση 8.7 Έστω A σύνολο. Για κάθε $Y \subseteq A$ η **χαρακτηριστική συνάρτηση** του Y ορίζεται ως εξής

$$\chi_Y(t) = \begin{cases} 1 & \text{αν } t \in Y \\ 0 & \text{αν } t \notin Y \end{cases}$$

Αποδείξτε οτι η συνάρτηση $F : \mathfrak{P}(A) \longrightarrow \{0,\, 1\}^A$ με $F(Y) = \chi_Y$ είναι αμφιμονοσήμαντη.

Επίλογος

Θεμελίωση της θεωρίας συνόλων

Μέχρι αυτό το σημείο επικεντρώσαμε τις προσπάθειες μας να βρούμε μία τυπική δομή για την αριθμητική, στη βάση της θεωρίας συνόλων. Αλλά δεν έχουμε αναφερθεί στην αξιωματική θεμελίωση της ίδιας της θεωρίας συνόλων. Σε τελευταία ανάλυση, δεν αποτελεί μεγάλη πρόοδο να βασίσουμε μια τυπική θεωρία των αριθμών σε μία άτυπη, εποπτική και αφελή θεωρία συνόλων. Θα μπορούσαμε να κρατήσουμε την άτυπη, εποπτική και αφελή θεωρία των αριθμών!

Από την εποχή του Cantor και του Dedekind, που εισήγαγαν την εποπτική θεωρία συνόλων, έχουν δοθεί διάφορα αξιωματικά συστήματα για τη θεωρία συνόλων, που αποφεύγουν τα παράδοξα που συναντήσαμε, όπως αυτό του Russell. Τα πιο γνωστά είναι αυτά των Zermelo–Fraenkel και των von Neumann–Bernays–Goedel. Η βασική μέθοδος που χρησιμοποιούν για να αποφύγουν τα παράδοξα είναι να περιορίσουν την έννοια του συνόλου, ώστε να μην περιλάμβάνει οποιαδήποτε ‘συλλογή σε ένα όλον καθορισμένων αντικειμένων της σκέψης ή της εποπτείας μας που είναι εντελώς διακριτή μεταξύ τους’ όπως την είχε περιγράψει ο Cantor. Γίνεται η διάκριση μεταξύ τάξεων (classes) και συνόλων ή μπαίνουν περιορισμοί στα σύνολα. Αυτές οι αξιωματικές θεωρίες, μαζί με το αξίωμα ύπαρξης των φυσικών αριθμών, επαρκούν για να αναπτύξουν τη θεωρία των αριθμών, φυσικών, ρητών, πραγματικών, μιγαδικών.

Υπάρχουν όμως δύο αξιώματα που έχουν μία ιδιαίτερη θέση, και έχουν απασχολήσει αρκετά τους μαθηματικούς.

Το αξίωμα επιλογής

Στην Πρόταση 8.1, χρησιμοποιήσαμε ένα επιχείρημα στο οποίο επιλέγουμε ένα στοιχείο x_1 από ένα σύνολο B, κατόπιν ένα x_2 από το $B \setminus \{x_1\}, \ldots$, και γενικά ένα στοιχείο x_{n+1} από το σύνολο $B \setminus \{x_1, x_2, \ldots, x_n\}$. Παρ’ όλο που αυτό μοιάζει με την αναδρομική διαδικασία ορισμού, δεν καλύπτεται από το θεώρημα 6.3, γιατί το x_{n+1} επιλέγεται με αυθαίρετο τρόπο, και όχι μέσω μίας προκαθορισμένης συνάρτησης. Η μέθοδος μας απαιτεί να κάνουμε ‘άπειρο πλήθος αυθαίρετων επιλογών’. Μπορεί να αποδειχθεί (αν και δεν είναι εύκολο!) οτι τα υπόλοιπα αξιώματα της θεωρίας συνόλων δεν επαρκούν γι’ αυτό. Απαιτείται ένα επί πλέον αξίωμα, το Αξίωμα Επιλογής (Axiom of Choice).

Η θέση αυτού του αξιώματος είναι διαισθητικά δύσκολο να γίνει αντιληπτή, αλλά έχει πλέον γίνει καλά κατανοητή. Ούτε η υπόθεση της αλήθειας αυτού του αξιώματος, ούτε η άρνηση του, αντιφάσκουν με τα υπόλοιπα αξιώματα της θεωρίας συνόλων (όπως ούτε η αποδοχή του αιτήματος των παράλληλων του Ευκλείδη, ούτε η άρνηση του αντιφάσκει με τα υπόλοιπα αξιώματα της Γεωμετρίας). Εάν το αποδεχθούμε έχουμε μία πιο καλή θεωρία πληθικών αριθμών: για κάθε δύο σύνολα X, Y ισχύει (τουλάχιστον) ένα από τα $|X| \leq |Y|$, $|Y| \leq |X|$.

Παρόμοια θέση κατέχει ένα άλλο αξίωμα. Η Υπόθεση του Συνεχούς λέει οτι δεν υπάρχει άπειρος πληθικός αριθμός μεταξύ του $\aleph_0$ και του $\mathfrak{c}$, δηλαδή οτι δεν υπάρχει σύνολο X για το οποίο να ισχύει

$$|\mathbb{N}| < |X| < |\mathbb{R}|.$$

Ούτε η αποδοχή ούτε η άρνηση της Υπόθεσης του Συνεχούς αντιφάσκουν πρός τα υπόλοιπα αξιώματα, ή προς το Αξίωμα Επιλογής.

Συνέπεια

Παραμένει ακόμα το ερώτημα: έχοντας βρεί το σύνολο των αξιωμάτων της θεωρίας συνόλων, πώς *γνωρίζουμε* οτι δεν εμφανίζονται παράδοξα; Μέχρι τώρα τα έχουμε αποφύγει (αφού κανείς δεν έχει βρεί κάποιο) αλλά πως μπορούμε να είμαστε *σίγουροι* οτι δεν υπάρχουν κρυμμένες αντιφάσεις; Τώρα έχουμε μία σαφή, τελική απάντηση σε αυτό το ερώτημα. Δυστυχώς αυτή είναι η εξής: δεν μπορούμε *ποτέ* να είμαστε σίγουροι.

Για να εξηγήσουμε αυτό, πρέπει να πάμε πίσω στον Hilbert. Ας ονομάσουμε ένα σύστημα αξιωμάτων **συνεπές** (consistent) εάν δεν οδηγεί σε αντιφάσεις. Ο Hilbert ήθελε να αποδείξει οτι τα αξιώματα της θεωρίας συνόλων είναι συνεπή.

Για μερικά συστήματα αξιωμάτων αυτό είναι εύκολο. Εάν μπορούμε να βρούμε ένα *μοντέλο* για τα αξιώματα, δηλαδή μία δομή η οποία τα ικανοποιεί, τότε πρέπει να είναι συνεπή (αλλοιώς δεν θα υπήρχε το μοντέλο). Το πρόβλημα είναι τί υλικά μπορούμε να χρησιμοποιήσουμε για την κατασκευή του μοντέλου; Είναι γενικά αποδεκτό οτι ένα πεπερασμένο μοντέλο είναι ικανοποιητικό, αφού κάθε ισχυρισμός γι΄ αυτό μπορεί να ελεγχθεί, κατ΄ αρχήν, σε πεπερασμένο χρόνο. Αλλά ένα σύστημα που περιέχει τους φυσικούς αριθμούς δεν είναι πεπερασμένο.

Η ιδέα του Hilbert ήταν να χρησιμοποιήσει κάτι λιγότερο περιοριστικό, που ονόμασε *διαδικασία απόφασης*. Σε σύγχρονη γλώσσα, ένα πεπερασμένο πρόγραμμα υπολογιστή, στο οποίο όταν δοθεί οποιαδήποτε πρόταση στη θεωρία συνόλων, εκτελεί μία διαδικασία και αποφαίνεται εάν η πρόταση είναι αληθής ή όχι. Εάν μπορέσουμε να κατασκευάσουμε ένα τέτοιο πρόγραμμα και να αποδείξουμε οτι δουλεύει πάντα, τότε αρκεί να του δώσουμε την πρόταση

$$0 \neq 0.$$

Εάν απαντήσει 'αληθές' τότε τα αξιώματα της θεωρίας συνόλων δεν είναι συνεπή. Για κάποιο διάστημα φαινόταν οτι η ιδέα του Hilbert μπορούσε να δουλέψει. Αλλά τα θεωρήματα του Goedel απέδειξαν το αντίθετο. Ο Goedel απέδειξε οτι υπάρχουν στη θεωρία συνόλων προτάσεις οι οποίες είναι αληθείς, αλλά για τις οποίες δεν υπάρχει απόδειξη (Θεώρημα μη Πληρότητας) και οτι εάν η θεωρία συνόλων είναι συνεπής, τότε δεν υπάρχει διαδικασία απόφασης που να το εξακριβώνει (Θεώρημα μη Αποκρισιμότητας).

Τα αποτελέσματα του Goedel διέλυσαν τις ελπίδες του προγράμματος του Hilbert. Σημαίνουν οτι υπάρχουν κάποιοι έμφυτοι περιορισμοί στην ίδια την αξιωματική μέθοδο. Δεν δείχνουν οτι αυτή είναι περιττή. Αντιθέτως, αποτελεί ένα ικανοποιητικό πλαίσιο για όλα τα σύγχρονα μαθηματικά, και έμπνευση για την ανάπτυξη νέων ιδεών. Αλλά με τα αποτελέσματα του Goedel μπορούμε να αποφύγουμε την αυταπάτη οτι όλα είναι τέλεια, και να αντιληφθούμε τους περιορισμούς της αξιωματικής μεθόδου, μαζί με τις δυνατότητες που προσφέρει.