$$\dim V = \dim \ker(f) + \dim \mathrm{Im}(f)$$

Γραμμική Άλγεβρα

Αριστείδης Ι. Κοντογεώργης

ΑΡΙΣΤΕΙΔΗΣ Ι. ΚΟΝΤΟΓΕΩΡΓΗΣ

Γραμμική Άλγεβρα

Γραμμική Άλγεβρα

Συγγραφή
Αριστείδης Ι. Κοντογεώργης

ISBN:
Έκδοση 0.9 – 31 Μαρτίου 2024

Πνευματικά Δικαιώματα:

- Η φωτογραφία του εξωφύλλου είναι του Α. Ι. Κοντογεώργη από τα Κοντακαίικα της Σάμου, όπως και η φωτογραφία του κυκλάμινου στην παράγραφο V.3.1 από το δάσος της Καισαριανής.
- Τα σχεδιαγράμματα έχουν γίνει με το Sage, το Mathematica και την γλώσσα PGF/TikZ.
- Η γραμματοσειρά Kerkis είναι δημιουργία του Αντώνη Τσολομύτη από το Πανεπιστήμιο Αιγαίου.
- Το βιβλίο έχει στοιχειοθετηθεί με το LaTeX.
- Οι εικόνες των Μαθηματικών είναι κοινό κτήμα γιατί έχουν παρέλθει 100 χρόνια από θάνατο του δημιουργού, με εξαίρεση αυτή του von Neuman η οποία είναι κοινό κτήμα By LANL - http://www.lanl.gov/history/atomicbomb/images/NeumannL.GIF (archive copy), Attribution, https://commons.wikimedia.org/w/index.php?curid=3429594 και του Israel Gelfand η οποία προέρχεται από το MFO Prof. Konrad Jacobs CC BY-SA 2.0 DE DEED Attribution-Share Alike 2.0 Germany

Αφιερώνεται στους φοιτητές μου.

Γραμμική Άλγεβρα

Αριστείδης Ι. Κοντογεώργης

31 Μαρτίου 2024

Περιεχόμενα

Εισαγωγή

Η Γραμμική Άλγεβρα μαζί με τον Απειροστικό Λογισμό αποτελούν βασική γνώση για κάθε Μαθηματικό αλλά και για οποιονδήποτε θέλει να χρησιμοποιήσει τα Μαθηματικά. Αυτό είναι ένα βιβλίο Γραμμικής Άλγεβρας το οποίο έχει γραφεί έχοντας υπόψη πρωτίστως την διδασκαλία των μαθημάτων Γραμμική Άλγεβρα Ι και ΙΙ. Θέλουμε όμως να εισαγάγουμε τον αναγνώστη σε αυτά που θα ακολουθήσουν στην πορεία του για την κατάκτηση της Μαθηματικής επιστήμης.

Η γραμμική άλγεβρα έχει ένα πλήθος εφαρμογών πρώτα στα ίδια τα Μαθηματικά και μετά στις άλλες επιστήμες. Προσπαθήσαμε να δείξουμε αρκετές από αυτές, όπως για παράδειγμα ότι παράγωγος μιας συνάρτησης πολλών μεταβλητών είναι μια γραμμική συνάρτηση, ένα αντικείμενο που μελέτης της γραμμικής άλγεβρας.

Το πρώτο κεφάλαιο σκοπεύει στην ωρίμανση του Μαθηματικού αισθητηρίου των φοιτητών και στην ομαλή μετάβαση τους στο Πανεπιστήμιο. Είναι γεγονός ότι υπάρχει μια συστηματική έκπτωση των γνώσεων με τις οποίες έρχονται εφοδιασμένοι οι φοιτητές από τα Λυκειακά Μαθηματικά. Στο κεφάλαιο αυτό παρουσιάζονται και κατασκευάζονται τα σύνολα τα οποία πρωταγωνιστούν στα Μαθηματικά, και δίνονται κατασκευές των πραγματικών και μιγαδικών αριθμών. Επίσης δίνεται μια πρώτη εισαγωγή στις αλγεβρικές δομές, αυτή των διανυσματικών είναι μια από αυτές. Τέλος επιχειρείται να δοθεί μια εισαγωγή στην θεωρία της παραγώγου η οποία εισάγεται μέσω ενός ανορθόδοξου τρόπου, ακολουθώντας την ιδέα του Καραθεωδορή. Συνίσταται ο φοιτητής να επισκέπτεται τις παραγράφου αυτού κάθε φορά που έχει κενά στις γνώσεις του.

Στο δεύτερο κεφάλαιο ο αναγνώστης εισάγεται στους πίνακες και στις πράξεις μεταξύ τους. Στο τρίτο κεφάλαιο παρουσιάζονται τα γραμμικά συστήματα και η μέθοδος της απαλοιφής του Gauss. Επίσης γίνεται μια εισαγωγή στην ορίζουσα αλλά και σε εφαρμογές της στην απαλείφουσα την διακρίνουσα και τις λύσεις μη-γραμμικών συστημάτων και σε προβλήματα παρεμβολής.

Στο τέταρτο κεφάλαιο παρουσιάζεται η αφηρημένη έννοια του διανυσματικού χώρου και έννοιες γύρω από αυτή όπως η γραμμική εξάρτηση και ανεξαρτησία, αλλά και οι χώροι γραμμών και στηλών ενός πίνακα. Στο πέμπτο κεφάλαιο παρουσιάζονται οι φυσιολογικές συναρτήσεις μεταξύ γραμμικών χώρων, οι γραμμικές συναρτήσεις και δίνεται μια ποιοτική και θεωρητική αντιμετώπιση των λύσεων γραμμικών συστημάτων. Επίσης έχουμε αναπτύξει αρκετές γνώσεις σε αυτό το σημείο για να δώσουμε μια εφαρμογή στα γραφήματα και στα ηλεκτρικά κυκλώματα.

Στο έκτο κεφάλαιο εισάγονται οι έννοιες της ιδιοτιμής και του ιδιοδιανύσματος, το χαρακτηριστικό πολυώνυμο και αποδεικνύονται βασικά θεωρήματα όπως το Caley-Hamilton, παρουσιάζεται η διαγωνοποίηση και η κανονική μορφή Jordan. Το τελευταίο θεωρούνταν ένα αρκετά πολύπλοκο θέμα, όμως έχουν εμφανιστεί μερικές πολύ σύντομες αποδείξεις οι οποίες έχουν απλοποιήσει την περιγραφή και την απόδειξη και τις οποίες αξιοποιούμε στο βιβλίο αυτό.

Στο έβδομο κεφάλαιο δίνεται μια εισαγωγή στις απόλυτες τιμές και ιδιαίτερα σε αυτές που

παράγονται από εσωτερικά γινόμενα. Παρουσιάζεται ο εκθετικός πίνακας και δίνεται μια εισαγωγή στα συστήματα διαφορικών εξισώσεων, μία κλασική εφαρμογή της γραμμικής άλγεβρας. Παρουσιάζεται η μέθοδος ορθοκανονικοποίησης και δίνονται μερικές εφαρμογές την βελτιστοποίησης και την μέθοδο ελαχίστων τετραγώνων. Τέλος ορίζονται οι συζυγείς γραμμικές συναρτήσεις ως προς ένα εσωτερικό γινόμενο εισάγονται οι κανονικές, μοναδιαίες και αυτοσυζυγείς συναρτήσεις και εξετάζεται η θεωρία διαγωνοπίησης τους.

Το όγδοο κεφάλαιο είναι αφιερωμένο στις τετραγωνικές μορφές, δίνεται η κλασική εφαρμογή στην θεωρία των τετραγωνικών επιφανειών αλλά και στην θεωρία ακροτάτων συναρτήσεων πολλών μεταβλητών. Τέλος εξετάζονται γενικεύσεις του εσωτερικού γινομένου, όπως οι μιάμιση και διγραμμικές μορφές και αποδεικνύεται το θεώρημα του Sylvester.

Το ένατο και τελευταίο κεφάλαιο είναι αφιερωμένο σε μερικές από τις πάμπολλες εφαρμογές της γραμμικής άλγεβρας. Εξετάζεται η θεωρία αναπαραστάσεων, η οποία αποτελεί ένα κλάδο από μόνη της και αφορά την αλληλεπίδραση μιας ομάδας που δρα επί ενός διανυσματικού χώρου. Επίσης παρουσιάζεται ένα πεπερασμένης διάστασης μοντέλο της κβαντομηχανικής το οποίο δίνει μια φυσική ερμηνεία των αυτοσυζυγών γραμμικών συναρτήσεων και παρόλο που δεν μπορεί να περιγράψει την φυσική πραγματικότητα σε αυτό εμφανίζονται αρκετά αν όχι όλα τα φαινόμενα της φυσικής θεωρίας. Τέλος παρουσιάζεται το θεώρημα Perron-Frobenius στις αναδρομικές συναρτήσεις όπως και ο pagerank αλγόριθμος της google. Οι επινοητές του αλγορίθμου αυτού έδωσαν μια εφαρμογή της γραμμικής άλγεβρας η οποία όχι μόνο τους έκανε δισεκατομμυριούχους αλλά τους επέτρεψε να ελέγξουν την παγκόσμια πληροφορία και τον κόσμο.

I

Θεμέλια

I.1 Σύνολα

Η έννοια του συνόλου ως *πρωταρχική* έννοια της γλώσσας μας, δεν είναι δυνατόν να οριστεί με απόλυτη μαθηματική ακρίβεια. Λέμε απλά -διαισθητικά- ότι σύνολο είναι μία «συλλογή» αντικειμένων. Η συλλογή αυτή μπορεί να μην περιέχει κανένα αντικείμενο οπότε έχουμε την έννοια του *κενού* συνόλου. Για το κενό σύνολο χρησιμοποιούμε το σύμβολο $\varnothing$.

Όταν ένα σύνολο έχει πεπερασμένα το πλήθος στοιχεία θα λέγεται πεπερασμένο, και μπορεί να παρασταθεί περιγράφοντας τα στοιχεία του. Έτσι για παράδειγμα το

$$A := \{1, 2, 5, 7, 9, 74\} \tag{I.1}$$

είναι ένα σύνολο με 6 το πλήθος στοιχεία. Ακολουθώντας αυτό τον συμβολισμό πολλοί συγγραφείς συμβολίζουν το κενό σύμβολο με άδεια άγκιστρα δηλαδή με $\{\}$. Άλλες φορές ένα σύνολο περιγράφεται από μία ιδιότητα. Ο κύκλος για παράδειγμα μπορεί να περιγραφεί ως το σύνολο των σημείων του επιπέδου που ικανοποιούν

$$B := \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}. \tag{I.2}$$

I.1.1 Το παράδοξο του Russel

Το παρακάτω παράδοξο που οφείλεται στο Μαθηματικό και Φιλόσοφο B. Russel, έδειξε ότι πρέπει να είμαστε προσεκτικοί με την έννοια του συνόλου, όταν αυτό ορίζεται με βάση μία ιδιότητα.

Σε μία επαρχιακή πόλη ο κουρέας ξυρίζει μόνο όλους όσοι δεν ξυρίζονται μόνοι τους. Θέλουμε να μελετήσουμε την «συλλογή» A, των ανθρώπων που ξυρίζει ο κουρέας.

Το πρόβλημα είναι αν ο κουρέας ξυρίζεται ή όχι μόνος του. Αν ο κουρέας ξυρίζεται μόνος του τότε δεν πρέπει να ξυρίζει τον εαυτό του, άτοπο. Αν πάλι δεν ξυρίζεται μόνος του, τότε θα πρέπει να ξυρίζει τον εαυτό του, άτοπο.

Το παραπάνω παράδοξο έχει αρκετές διατυπώσεις με την «περισσότερο μαθηματική» την επόμενη: Θεωρούμε το «σύνολο»

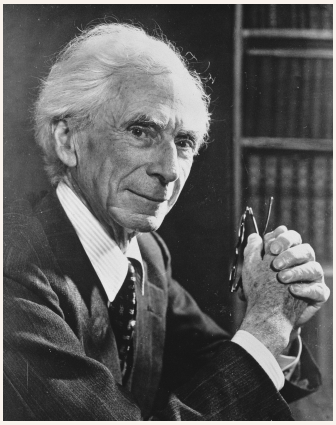
$$S := \{x : x \notin x\}.$$

Η προβληματική ερώτηση είναι αν $S \in S$. Πράγματι, αν $S \in S$, τότε εξ ορισμού $S \notin S$,άτοπο. Αν πάλι $S \notin S$, τότε εξ ορισμού του συνόλου S θα πρέπει να έχουμε $S \in S$, το οποίο είναι και πάλι άτοπο. Οι μαθηματικοί αντιμετωπίζουν τα προβλήματα αυτά με το να θεωρούν ένα συγκεκριμένο *σύμπαν* στοιχείων $\mathcal{A}$, δηλαδή μία ευρύτερη δυνατή συλλογή αντικειμένων μέσα στην οποία ορίζονται όλα τα σύνολα. Στην περίπτωση αυτή μπορούμε να ορίσουμε υποσύνολα του $\mathcal{A}$ περιγράφοντας τα με βάση τις ιδιότητες τους. Για παράδειγμα, στην (I.2) το σύμπαν μας είναι το $\mathbb{R} \times \mathbb{R}$. Μπορούμε

να παρατηρήσουμε ότι το παράδοξο του Russel θα εμφανιστεί και πάλι αν θεωρήσουμε ως σύμπαν την «συλλογή» όλων των δυνατών συνόλων. Παρόλα αυτά μπορεί να αποδειχτεί ότι δεν υπάρχει ένα σύνολο που να περιέχει όλα τα σύνολα ως στοιχεία. (Περιέχει τον εαυτό του;) Δεν θα επιμείνουμε περισσότερο στις παραπάνω έννοιες σε αυτή την φάση των μαθηματικών σπουδών σας.

Ο **Bertrand Arthur William Russell** (18 Μαΐου 1872 – 2 Φεβρουαρίου 1970) ήταν Βρετανός Μαθηματικός και Φιλόσοφος. Ασχολήθηκε με την Λογική, την θεωρία συνόλων, την γλωσσολογία την επιστημολογία και την Φιλοσοφία. Είχε σημαντική συνεισφορά στην λογική θεμελίωση των Μαθηματικών με γνωστότερο έργο του το Principia Mathematica, στο οποίο μεταξύ άλλων επιχειρηματολόγησε για την ταύτιση Μαθηματικών και Λογικής.

Το 1950 έλαβε το βραβείο Nobel στην λογοτεχνία, «ως αναγνώριση των ποικίλων και σημαντικών γραπτών του έργων, στα οποία υπερασπίζεται ανθρωπιστικές αξίες και την ελευθερία της σκέψης». Ήταν γνωστός ακτιβιστής με πολιτική δράση ενεργή συμμετοχή στον δημόσιο λόγο και φιλειρηνιστής.



Ι.1.2 Ιδιότητες συνόλων

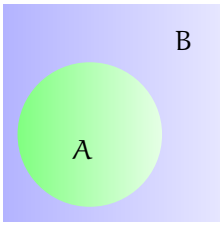
Θα πρέπει να σημειωθεί ότι για κάθε σύνολο απαιτούμε να μπορούμε να απαντήσουμε ή με άρνηση ή με κατάφαση, στο ερώτημα: Είναι το x στοιχείο του συνόλου A;

Έστω A σύνολο. Αν το x είναι στοιχείο του A, τότε θα λέμε ότι το x *ανήκει* στο σύνολο A, και θα το συμβολίζουμε με $x \in A$. Αν το x δεν είναι στοιχείο του A, τότε θα λέμε ότι το x *δεν ανήκει* στο σύνολο A, και θα το συμβολίζουμε με $x \notin A$.

Έτσι στο παράδειγμα (Ι.1) έχουμε $1 \in A$ και $55 \notin A$, ενώ στο παράδειγμα (Ι.2) έχουμε $(1,0) \in B$ ενώ $(34,56) \notin B$.

Ορισμός Ι.1.1. Θα λέμε ότι το είναι *υποσύνολο* του B και θα το συμβολίζουμε με $A \subset B$ αν και μόνο αν για κάθε $x \in A$ έχουμε ότι $x \in B$. Αν το $\subset B$ και υπάρχει $x \in B$ ώστε $x \notin A$, τότε θα λέμε ότι το A είναι γνήσιο υποσύνολο του και θα το συμβολίζουμε με $A \subsetneq B$

Σχήμα Ι.1: Υποσύνολο Συνόλου $A \subseteq B$



Ορισμός Ι.1.2. Θα λέμε ότι τα σύνολα A και B είναι ίσα αν και μόνο αν $A \subset B$ και $B \subset A$.

I.2 Συνολοθεωρητικές Πράξεις

Έστω $A, B \subset X$. Θα συμβολίζουμε με $A \cup B$, το σύνολο

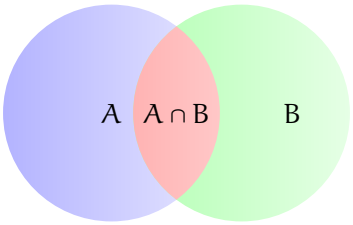
$$A \cup B := \{x \in X : x \in A \text{ ή } x \in B\},$$

και θα το ονομάζουμε *ένωση* των συνόλων A και B. Διαισθητικά η ένωση των συνόλων A, B περιέχει όλα τα στοιχεία και των δύο συνόλων.

Θα συμβολίζουμε με $A \cap B$, το σύνολο

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

και θα το ονομάζουμε *τομή* των συνόλων A και B. Διαισθητικά η τομή περιέχει τα στοιχεία που είναι κοινά και στα δύο σύνολα.



Σχήμα I.2: Τομή Συνόλων

Θα συμβολίζουμε με $A \backslash B$, το σύνολο

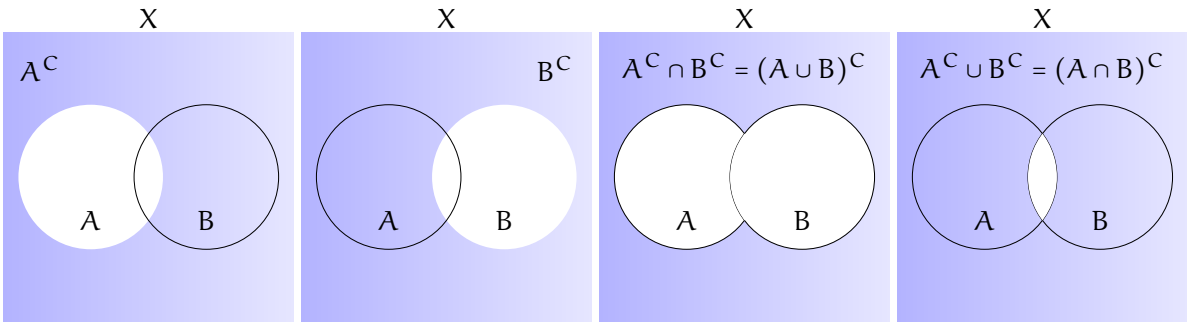
$$A \backslash B : \{x \in X : x \in A, x \notin B\},$$

και θα το ονομάζουμε *διαφορά* των συνόλων A, B. Διαισθητικά η διαφορά περιέχει τα στοιχεία του συνόλου A που δεν περιέχονται στο σύνολο B.

Το σύνολο $X \backslash A$ θα το ονομάζουμε συμπλήρωμα του A στο X, και αν είναι σαφές ποιό είναι το σύνολο X, τότε θα συμβολίζουμε $X \backslash A = A^C$.

Πρόταση I.2.1 (Τύποι De Morgan). *Ισχύουν τα παρακάτω:*

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



Σχήμα I.3: Νόμοι De Morgan. Τα σύνολα $A^C, B^C, A^C \cap B^C = (A \cup B)^C, A^C \cup B^C = (A \cap B)^C$ είναι χρωματισμένα γαλάζια.

Απόδειξη. Για να αποδείξουμε ότι δύο σύνολα είναι ίσα αρκεί να δείξουμε, σύμφωνα με τον ορισμό της ισότητας συνόλων, ότι το ένα είναι υποσύνολο του άλλου.

Θα δείξουμε ότι $(A \cap B)^C \subseteq A^C \cup B^C$. Πράγματι έστω $x \in (A \cap B)^C$. Αυτό σημαίνει ότι $x \in X$ και $x \notin (A \cap B)$, δηλαδή ισοδύναμα $x \in X$ και $x \notin A$ ή $x \notin B$. Άρα $x \in A^C$ ή $x \in B^C$, δηλαδή $x \in A^C \cup B^C$.

Αντιστρόφως θα δείξουμε ότι $A^C \cup B^C \subseteq (A \cap B)^C$. Πράγματι αν $x \in A^C \cup B^C$ τότε $x \in X$ και $x \notin A$ ή $x \in X$ και $x \notin B$. Άρα $x \notin (A \cap B)$ δηλαδή $x \in (A \cap B)^C$.

Συνδιάζοντας τα συμπεράσματα των δύο παραπάνω παραγράφων έχουμε ότι $(A \cap B)^C = A^C \cup B^C$.

Με όμοιο τρόπο θα δείξουμε ότι $(A \cup B)^C = A^C \cap B^C$. Πράγματι έστω $x \in (A \cup B)^C$. Αυτό σημαίνει ότι $x \in X$ ή $x \notin (A \cup B)$, δηλαδή ισοδύναμα $x \in X$ ή $x \notin A$ και $x \notin B$. Άρα $x \in A^C$ και $x \in B^C$, δηλαδή $x \in A^C \cap B^C$.

Αντιστρόφως θα δείξουμε ότι $A^C \cap B^C \subseteq (A \cup B)^C$. Πράγματι αν $x \in A^C \cap B^C$ τότε $x \in X$ ή $x \notin A$ και $x \in X$ ή $x \notin B$. Άρα $x \notin (A \cup B)$ δηλαδή $x \in (A \cup B)^C$.

Συνδιάζοντας τα συμπεράσματα των δύο παραπάνω παραγράφων έχουμε ότι $(A \cup B)^C = A^C \cap B^C$.

□

Ορισμός Ι.2.2. Έστω ένα σύνολο A. Θα συμβολίζουμε με $\mathcal{P}(A)$, το σύνολο όλων των υποσυνόλωνν του.

Παραδείγματα Έστω $A = \varnothing$, τότε $\mathcal{P}(\varnothing) = \{\varnothing\}$. Έστω $A = \{1, 2, 3\}$, τότε

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

Ι.3 Προτάσεις

Μία πρόταση στα μαθηματικά είναι κάθε φράση η οποία μπορεί να χαρακτηριστεί με απόλυτη ακρίβεια και αντικειμενικά ως αληθής ή ψευδής. Φράσεις οι οποίες περιέχουν υποκειμενικές κρίσεις ή εσωτερικές αντιφάσεις δεν είναι προτάσεις. Θα προσπαθήσουμε να κάνουμε τα παρακάτω σαφή με παραδείγματα. Η φράση:

«Η Αθήνα είναι μία όμορφη πόλη»

δεν είναι πρόταση γιατί η απάντηση είναι υποκειμενική. Διαφορετικοί άνθρωποι θα δώσουν διαφορετικές απαντήσεις, αλλά ακόμα και ο ίδιος άνθρωπος μπορεί να βρει θετικά και αρνητικά στοιχεία που να μην του επιτρέψουν να απαντήσει.

Οι προτάσεις μπορούν να συνδυαστούν και να δώσουν νέες προτάσεις. Έστω p, q προτάσεις. Η πρόταση $p \vee q$, που διαβάζεται «p ή q», είναι αληθής αν μία από τις p,q είναι αληθείς. Η πρόταση $p \wedge q$, που διαβάζεται «p και q», είναι αληθής αν και οι δύο προτάσεις p,q είναι αληθείς. Η πρόταση $\overline{p}$ που διαβάζεται «άρνηση p», είναι αληθής αν και μόνο αν η p είναι ψευδής.

Αν p, q προτάσεις μπορώ να σχηματίσω την πρόταση $p \Rightarrow q$, η οποία είναι αληθής αν

$$p \text{ αληθής, τότε και } q \text{ αληθής.}$$

Για τις σχέσεις μεταξύ προτάσεων ισχύει η παρακάτω

Πρόταση Ι.3.1.

1. $p \Leftrightarrow \overline{\overline{p}}$
2. $p \Leftrightarrow p \vee p$
3. $p \Leftrightarrow p \wedge p$

4. $p \vee q \Leftrightarrow q \vee p$
5. $p \wedge q \Leftrightarrow q \wedge p$
6. $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
7. $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
8. $\overline{p \wedge q} \Leftrightarrow \overline{p} \vee \overline{q}$ *Τύποι De Morgan*
9. $\overline{p \vee q} \Leftrightarrow \overline{p} \wedge \overline{q}$
10. $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
11. $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
12. $(p \Rightarrow q) \Leftrightarrow (\overline{q} \Rightarrow \overline{p})$ *Αντιθετοαντιστροφή*

Απόδειξη. 1. Αν η πρόταση p είναι αληθής τότε η πρόταση $\overline{p}$ είναι ψευδής, άρα η $\overline{\overline{p}}$ είναι αληθής. Αντιστρόφως, αν η πρόταση $\overline{\overline{p}}$ είναι αληθής τότε η $\overline{p}$ είναι ψευδής και η p αληθής.

2. Αν η πρόταση p είναι αληθής τότε μία τουλάχιστον από τις δύο προτάσεις εκατέρωθεν του $\vee$ είναι αληθής άρα $p \vee p$ είναι αληθής. Αντιστρόφως, αν το $p \vee p$ είναι αληθής τότε μία τουλάχιστον από τις δύο προτάσεις εκατέρωθεν του $\vee$ είναι αληθείς και επειδή και οι δύο είναι η p και η p είναι αληθής.

3. Αν η πρόταση p είναι αληθής τότε και οι δύο προτάσεις εκατέροθεν του $\wedge$ είναι αληθείς άρα και το $p \wedge p$ είναι αληθές. Αντιστρόφως αν το $p \wedge p$ είναι αληθής τότε και οι δύο προτάσεις εκατέρωθεν του $\wedge$ είναι αληθείς και αφού ταυτίζονται το p είναι αληθές.

4. Το $p \vee q$ είναι αληθές αν και μόνο αν μία τουλάχιστον από τις p, q είναι αληθής αν και μόνο αν το $q \vee p$ είναι αληθές, αφού η σειρά δεν παίζει ρόλο.

5. Ομοίως, το $p \wedge q$ είναι αληθές αν και μόνο αν και οι δύο p, q είναι αληθείς αν και μόνο αν το $q \wedge p$ είναι αληθές.

6. Το $p \wedge (q \wedge r)$ είναι αληθές αν και μόνο αν (και το p και το $q \wedge r$ είναι αληθή) το οποίο ισχύει αν και μόνο αν (και το p και το q και το r είναι αληθή) αν και μόνο αν ($(p \wedge q)$ αληθές και r αληθές) αν και μόνο αν $(p \wedge q) \wedge r)$ αληθές.

7. Το $p \vee (q \vee r)$ είναι αληθές αν και μόνο αν (ένα από τα p ή $q \wedge r$ είναι αληθή) το οποίο ισχύει αν και μόνο αν (ή το p ή το q ή το r είναι αληθή) αν και μόνο αν ($(p \vee q)$ αληθές ή r αληθές) αν και μόνο αν $(p \vee q) \vee r)$ αληθές.

8. Το $\overline{p \wedge q}$ είναι αληθές αν και μόνο αν το $p \wedge q$ είναι ψευδές αν και μόνο αν ένα τουλάχιστον από τα p, q είναι ψευδή, δηλαδή αν και μόνο αν $\overline{p} \vee \overline{q}$.

9. Το $\overline{p \vee q}$ είναι αληθές αν και μόνο αν το $p \vee q$ είναι ψευδές αν και μόνο αν και τα δύο p, q είναι ψευδή, δηλαδή αν και μόνο αν $\overline{p} \wedge \overline{q}$.

10. Έστω $p \vee (q \wedge r)$ είναι αληθές. Αυτό συμβαίνει αν και μόνο αν (p αληθές ή $(q \wedge r)$ αληθής. Αν p αληθής τότε $p \vee q$ και $p \vee r$ είναι και οι δύο αληθείς, ανεξάρτητα από την αλήθεια των q, r, άρα $(p \vee q) \wedge (p \vee r)$ είναι αληθής. Αν πάλι p ψευδής τότε θα πρέπει να είναι αληθής η $q \wedge r$ δηλαδή και το q και το r είναι αληθή, δηλαδή $p \vee q$ και $p \vee r$ οπότε και πάλι έχουμε ότι $(p \vee q) \wedge (p \vee r)$ είναι αληθής.

    Αντιστρόφως αν $(p \vee q) \wedge (p \vee r)$ είναι αληθής τότε $p \vee q$ και $q \vee r$ είναι αληθής. Αν p αληθής τότε $p \vee (q \wedge r)$ είναι αληθής ανεξάρτητα από την αλήθεια του $(q \wedge r)$. Αν p ψευδής, τότε q, p είναι και τα δύο αληθή, άρα και το $p \wedge q$ άρα και το $p \vee (q \wedge r)$.

11. Παρατηρούμε ότι το $p \wedge (q \vee r)$ είναι αληθές αν και μόνο αν p αληθές και (q αληθές ή r αληθές), αν και μόνο αν (p και q αληθές) ή (p και r αληθές) αν και μόνο αν $(p \wedge q) \vee (p \wedge r)$.

12. Αρκεί να αποδείξουμε ότι $p \Rightarrow q) \Rightarrow (\overline{q} \Rightarrow \overline{p})$ (γιατί;) Έστω λοιπόν ότι η αλήθεια της πρότασης p έχει σαν συνέπεια την αλήθεια της πρότασης q. Θα δείξουμε ότι η αλήθεια της πρότασης $\overline{q}$ έχει σαν συνέπεια την αλήθεια της πρότασης $\overline{p}$. Πράγματι αν η πρόταση $\overline{q}$ είναι αληθής τότε η q είναι ψευδής και συνεπώς η p είναι ψευδής (αφού αν ήταν αληθής η p θα ήταν και η q). Άρα η $\overline{p}$ είναι αληθής.

□

Ασκήσεις

Άσκηση Ι.1 Να γραφεί η άρνηση κάθε μιας από τις παρακάτω προτάσεις:

1. Η Αθήνα είναι η πρωτεύουσα της Ελλάδας
2. $3 + 5 = 8$
3. Για κάθε $\epsilon > 0$ υπάρχει $n_0(\epsilon)$ ώστε για $n > n_0(\epsilon)$ $-\epsilon < a_n < \epsilon$.
4. Τα μανταρίνια είναι κίτρινα και έχουν κουκούτσια
5. Υπάρχει φοιτητής που είναι ψηλότερος από 2 μέτρα.

Άσκηση Ι.2 Ας είναι p, q οι προτάσεις:

p: Το αυτοκίνητο σου δεν έχει βενζίνη

q: Δεν μπορείς να οδηγήσεις το αυτοκίνητό σου.

Να γραφούν οι παρακάτω προτάσεις σαν συναρτήσεις των p, q με τη βοήθεια λογικών συνδέσμων.

1. Το αυτοκίνητο σου έχει βενζίνη.
2. Δεν μπορείς να οδηγήσεις το αυτοκίνητο σου αν δεν έχει βενζίνη.
3. Το αυτοκίνητο σου έχει βενζίνη αν μπορείς να το οδηγήσεις
4. Αν δεν μπορείς να οδηγήσεις το αυτοκίνητο σου τότε δεν έχει βενζίνη.

Άσκηση Ι.3 Να διατυπωθεί αντιθετοαντίστροφη κάθε μίας από τις παρακάτω προτάσεις.

1. Αν βρέχει αύριο θα μείνω σπίτι.
2. Θα παίξουμε μπάλα αύριο αν έχει λιακάδα.
3. Αν ένας θετικός ακεραίος είναι πρώτος τότε δεν έχει άλλους διαιρέτες εκτός από το 1 και τον ευατό του.

Άσκηση Ι.4 Σε μία διασταύρωση είναι δύο αδέλφια. Ο ένας λέει πάντα αλήθεια και ο άλλος λέει πάντα ψέματα. Τι πρέπει να τους ρωτήσουμε για να καταλάβουμε ποιός είναι ο δρόμος μας;

Ι.4 Σχέσεις

Ορισμός I.4.1. Θεωρούμε δύο σύνολα A, B. Θα λέμε διατεταγμένο ζεύγος με στοιχεία από τα A, B κάθε στοιχείο της μορφής (a, b), $a \in A$, $b \in B$. Το σύνολο των διατεταγμένων ζευγών με στοιχεία από τα A, B θα το συμβολίζουμε με $A \times B$ και θα το ονομάζουμε καρτεσιανό γινόμενο των A, B.

Παρατήρηση: Στον ορισμό του διατεταγμένου ζεύγους έχει σημασία η σειρά που τα στοιχεία εμφανίζονται εντός των παρενθέσεων. Έτσι το διατεταγμένο ζεύγος (a, b) είναι διαφορετικό από το διατεταγμένο ζεύγος (b, a).
Παραδείγματα:

1. Θεωρούμε τα σύνολα $A = \{1, 2, 3\}$ και $B = \{2, 5\}$. Το γινόμενο $A \times B$ είναι το σύνολο
$$A \times B = \{(1, 2), (1, 5), (2, 2), (2, 5), (3, 2), (3, 5)\}$$
ενώ το $B \times A$ είναι το σύνολο
$$B \times A = \{(2, 1), (5, 1), (2, 2), (5, 2), (2, 3), (5, 3)\}.$$
Παρατηρήστε ότι $A \times B \neq B \times A$.
2. Αν $A = B = \mathbb{R}$ τότε το σύνολο $\mathbb{R} \times \mathbb{R}$ είναι σε ένα προς ένα και επί αντιστοιχία με τα σημεία του επιπέδου, αν θεωρήσουμε ότι το ζευγάρι $(x, y) \in \mathbb{R} \times \mathbb{R}$, περιγράφει τις συντεταγμένες ενός σημείου του επιπέδου.

Πρόταση I.4.2. *Για τα καρτεσιανά γινόμενα συνόλων ισχύουν οι σχέσεις*

1. $\varnothing \times A = A \times \varnothing = \varnothing$
2. $A \times B = B \times A$ *αν και μόνο αν* $A = \varnothing$ *ή* $B = \varnothing$ *ή* $A = B$.

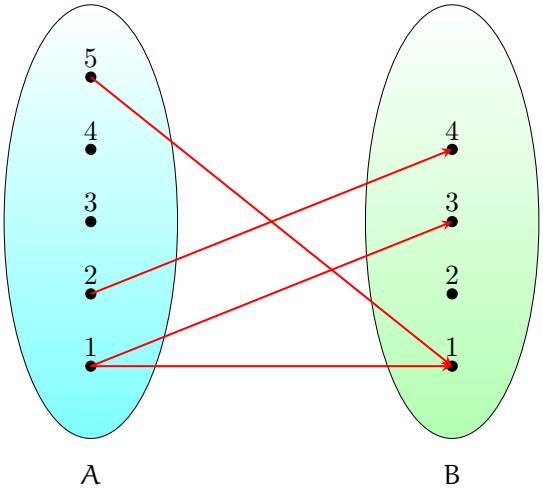
Απόδειξη. 1. Ας υποθέσουμε ότι το σύνολο $\varnothing \times A$ δεν ήταν διαφορετικό από το κενό σύνολο. Σε αυτή την περίπτωση θα υπήρχε ένα στοιχείο $(x, y) \in \varnothing \times A$ και άρα εξ ορισμού $x \in \varnothing$, άτοπο αφού το κενό σύνολο δεν περιλαμβάνει κανένα στοιχείο. Ομοίως δείχνουμε ότι $A \times \varnothing = \varnothing$.

2. Αν το A ή το B είναι κενά τότε προφανώς ισχύει το ζητούμενο. Ας υποθέσουμε λοιπόν ότι ούτε το A ούτε το B δεν είναι κενά. Έστω $x \in A$ και έστω $y \in B$. Εξ ορισμού $(x, y) \in A \times B = B \times A$, άρα $x \in B$ και $y \in A$, από όπου προκύπτει ότι $A \subset B$ και $B \subset A$, δηλαδή η ζητούμενη ισότητα. □

Ορισμός I.4.3. Μία διμελής σχέση από το σύνολο A στο σύνολο B είναι ένα υποσύνολο $\Sigma \subseteq A \times B$.

Παρατήρηση I.4.4. Ένα υποσύνολο του γινομένου $A \times B$, περιγράφεται από ένα σύνολο διατεταγμένων ζευγαριών. Ας υποθέσουμε για παράδειγμα ότι $A = \{1, 2, 3, 4, 5\}$ και ότι $B = \{1, 2, 3, 4\}$. Μία σχέση είναι το σύνολο
$$\Sigma = \{(1, 1), (2, 4), (5, 1), (1, 3)\} \subseteq A \times B.$$
Μία σχέση μπορεί να ερμηνευτεί σαν «συνδέσεις» μεταξύ στοιχείων του συνόλου A με αυτά του συνόλου B.

I.4.1 Σχέσεις ισοδυναμίας



Σχήμα Ι.4: Το σύνολο $\Sigma = \{(1,1),(2,4),(5,1),(1,3)\} \subseteq A \times B$ περιγράφει τις συνδέσεις μεταξύ των στοιχείων των A και B.

Ορισμός Ι.4.5. Μία σχέση $\Sigma \subseteq A \times A$ θα λέγεται *συμμετρική* αν $(a,b) \in \Sigma$ τότε $(b,a) \in \Sigma$.

Ορισμός Ι.4.6. Μία σχέση $\Sigma \subseteq A \times A$ θα λέγεται ανακλαστική αν και μόνο αν $(a,a) \in \Sigma$ για κάθε $a \in A$.

Ορισμός Ι.4.7. Μία σχέση $\Sigma \subseteq A \times A$ θα λέγεται μεταβατική αν και μόνο αν $(a,b) \in \Sigma$ και αν $(b,c) \in \Sigma$ τότε και $(a,c) \in \Sigma$.

Ορισμός Ι.4.8. Μία σχέση $\Sigma \subseteq A \times A$ θα λέγεται αντισυμμετρική αν και μόνο αν $(a,b) \in \Sigma$ και $(b,a) \in \Sigma$ τότε $a = b$.

Ορισμός Ι.4.9. Μία σχέση θα λέγεται σχέση ισοδυναμίας αν είναι συμμετρική, ανακλαστική και μεταβατική.

Παραδείγματα Ι.4.10.

1. Στο σύνολο των φοιτητών που είναι γραμμένοι στο μάθημα η σχέση ο/η φοιτητής/τρια x έχει το ίδιο φύλο με τον με τον/την φοιτητή/τρια y είναι μία σχέση ισοδυναμίας. Πράγματι, κάθε φοιτητής έχει το ίδιο φύλο με τον ευατό του άρα η σχέση είναι ανακλαστική. Αν ο x έχει το ίδιο φύλο με την y τότε και η y έχει το ίδιο φύλο με τον x, άρα η σχέση είναι συμμετρική. Τέλος αν ο x έχει το ίδιο φύλο με τον y και ο y το ίδιο φύλο με τον z, τότε και όλοι έχουν το ίδιο φύλο, άρα και ο x έχει το ίδιο φύλο με τον z, δηλαδή ισχύει και η μεταβατική ιδιότητα.

2. Στο σύνολο (x,y,z) των διατεταγμένων τριάδων στο $\mathbb{R}\times\mathbb{R}\times\mathbb{R}\setminus\{(0,0,0)\}$, θεωρούμε την σχέση $(x,y,z) \equiv (x',y',z')$ αν και μόνο αν υπάρχει $\lambda \in \mathbb{R}\setminus\{0\}$, ώστε
$$(x,y,z) = \lambda(x',y',z').$$

Σχήμα I.5: Διαμέριση συνόλου

Θα δείξουμε ότι η παραπάνω είναι μία σχέση ισοδυναμίας. Πράγματι, $(x,y,z) \equiv (x,y,z)$, αρκεί να πάρουμε για $\lambda = 1$. αν $(x,y,z) \equiv (x',y',z')$ τότε υπάρχει $\lambda \neq 0$, ώστε

$$(x,y,z) = \lambda(x',y',z') \Rightarrow (x',y',z') = \frac{1}{\lambda}(x,y,z) \ \ \frac{1}{\lambda} \in \mathbb{R}\backslash\{0\},$$

άρα η σχέση είναι συμμετρική. Τέλος αν $(x,y,z) \equiv (x_1,y_1,z_1)$ και $(x_1,y_1,z_1) \equiv (x_2,y_2,z_2)$ τότε

$$\big(x,y,z) = \lambda_1(x_1,y_1,z_1) \text{ και } (x_1,y_1,z_1) \equiv \lambda_2(x_2,y_2,z_2)\big) \Rightarrow$$
$$\Rightarrow (x,y,z) = \lambda_1\lambda_2(x_2,y_2,z_2),$$

δηλαδή $(x,y,z) \equiv (x_2,y_2,z_2)$ και η σχέση είναι και μεταβατική.

Ορισμός I.4.11. Ας θεωρήσουμε μία σχέση $\Sigma \subset A \times B$. Η αντίστροφη σχέση $\Sigma^{-1} \subset B \times A$ είναι η σχέση που ορίζεται από την ιδιότητα $(b,a) \in \Sigma^{-1}$ αν και μόνο αν $(a,b) \in \Sigma$.

Παράδειγμα Ας θεωρήσουμε την σχέση $\Sigma \subset \{a,b,c\}\times\{1,2\}$ που ορίζεται ως $\Sigma = \{(a,1),(b,2),(c,2)\}$. Η αντίστροφη σχέση $\Sigma^{-1} \subset \{1,2\} \times \{a,b,c\}$ είναι η $\Sigma^{-1} = \{(1,a),(2,b),(2,c)\}$.

Ορισμός I.4.12. Θα λέμε ότι τα σύνολα A_i, $i \in I$ αποτελούν μία διαμέριση του συνόλου X, αν και μόνο αν $\bigcup_{i\in I} A_i = X$ και $A_i \cap A_j = \varnothing$ ή $A_i = A_j$.

Πρόταση I.4.13. *Κάθε σχέση ισοδυναμίας $\Sigma \subseteq A \times A$ ορίζει διαμέριση του A σε ξένα σύνολα, τα οποία θα ονομάζουμε κλάσεις ισοδυναμίας. Αντιστρόφως κάθε διαμέριση $\{A_i\}_{i\in I}$ του συνόλου A ορίζει σχέση ισοδυναμίας όπου $(a,b) \in \Sigma$ αν και μόνο αν $x,y \in A_i$ για τον ίδιο δείκτη i.*

Απόδειξη. Ας υποθέσουμε ότι έχουμε την σχέση ισοδυναμίας $\Sigma \in A \times A$. Αν το σύνολο A είναι κενό δεν έχουμε τίποτα να δείξουμε. Ας υποθέσουμε ότι $x \in A$. Θέτουμε

$$A_x := \{y \in A, \text{ ώστε } (x,y) \in \Sigma\}.$$

Θα δείξουμε ότι τα σύνολα $\{A_x\}_{x\in} \subseteq A$ αποτελούν μία διαμέριση του συνόλου A.

Πράγματι είναι σαφές ότι $\bigcup_{x\in A} A_x = A$. Επιπλέον αν $A_x \cap A_y \neq \varnothing$, τότε υπάρχει $z \in A_x \cap A_y$, άρα $(x,z) \in \Sigma$ και $(y,z) \in \Sigma$ και λόγω της μεταβατικής ιδιότητας έχουμε ότι $(x,y) \in \Sigma$, άρα $A_x \subseteq A_y$ και $A_y \subseteq A_x$, δηλαδή $A_x = A_y$.

Αντιστρόφως αν $\{A_i\}_{i\in I}$ είναι μία διαμέριση του A, τότε ορίζουμε την σχέση ισοδυναμίας $\Sigma \subseteq A \times A$, ως εξής:

$$(x,y) \in \Sigma \text{ αν και μόνο αν υπάρχει } i \in I, \text{ ώστε } x,y \in A_i.$$

Θα δείξουμε τώρα ότι η Σ είναι πράγματι μία σχέση ισοδυναμίας. Έστω $x \in A$, υπάρχει $i \in I$ ώστε $x \in A_i$, αφού η ένωση των A_i δίνει το A. Άρα $(a,a) \in \Sigma$ και ισχύει η ανακλαστική ιδιότητα. Η συμμετρική ιδιότητα είναι προφανής, αφού αν $x,y \in A_i$ για κάποιο $i \in I$, τότε και $y,x \in A_i$. Τέλος για την μεταβατική ιδιότητα έχουμε ότι αν $(x,y) \in \Sigma$ και $(y,z) \in \Sigma$, τότε $x,y \in A_i$ και $y,z \in A_j$ για κάποια $i,j \in A$. Όμως $y \in A_i \cap A_j$ άρα $A_i \cap A_j \neq \varnothing$, άρα $A_i = A_j$, δηλαδή $x,z \in A_i$ και τελικά $(x,z) \in \Sigma$. □

Ορισμός Ι.4.14. Θεωρούμε μία σχέση ισοδυναμίας Σ σε ένα σύνολο A. Το σύνολο των κλάσεων ισοδυναμίας που ορίζει η Σ θα το λέμε το *σύνολο πηλίκο* της Σ.

Παράδειγμα Ι.4.15. Έστω A το σύνολο των φοιτητών του τμήματος. Ορίζουμε την σχέση ισοδυναμίας Σ με

$$(x, y) \in \Sigma \text{ αν και μόνο αν } x, y \text{ έχουν το ίδιο φύλο .}$$

Εύκολα βλέπουμε ότι η Σ είναι μία σχέση ισοδυναμίας (γιατι;), και διαμερίζει το σύνολο των φοιτητών σε δύο κλάσεις ισοδυναμίας το υποσύνολο A_1 των *αρσενικών φοιτητών* και το υποσύνολο A_2 των *θηλυκών φοιτητριών*. Το σύνολο πηλίκο είναι το $\{A_1, A_2\}$.

Παράδειγμα Ι.4.16. θεωρούμε το σύνολο X όλων των ανθρώπινων πλασμάτων. Ορίζουμε την σχέση $\sim$ ως εξής:

$$x \sim y \Leftrightarrow x \text{ είναι φίλος του } y.$$

Μπορούμε να θεωρήσουμε ότι ο καθένας είναι φίλος με τον εαυτό του, συνεπώς ισχύει ότι $x \sim x$. Αν ο x θεωρεί τον y φίλο του ας υποθέσουμε ότι και ο y θεωρεί τον x φίλο του, τουλάχιστον έτσι θα έπρεπε. Παρόλα αυτά μπορούμε να σκεφτούμε αρκετά παραδείγματα όπου ο x έχει ειλικρινή φιλία με τον y, ο y έχει ειλικρινή φιλία με τον z και παρόλα αυτά ο x με τον z είναι εχθροί! Παραφράζοντας λίγο τον Α. Γιαννόπουλο[1] θα λέγαμε ότι *«πολύπλοκοι είναι άνθρωποι και οι σχέσεις τους, όχι τα Μαθηματικά»*.

Θα μπορούσαμε να ορίσουμε μια νέα σχέση $\approx$ όπου ορίζουμε ότι

$$x \approx y \Leftrightarrow \text{ υπάρχουν } x_1, \dots, x_r \in X \text{ ώστε } x \sim x_1 \sim \cdots \sim x_r \sim y.$$

η οποία είναι πράγματι μια σχέση ισοδυναμίας.

Παρατήρηση Ι.4.17. Οι χώροι πηλίκο είναι δύσκολοι στην κατανόηση τους αλλά ιδιαίτερα σημαντικοί στα Μαθηματικά. Όπως θα δούμε τους χρησιμοποιούμε συνέχεια για να ορίσουμε νέα αντικείμενα στα οποία είτε θέλουμε να επιβάλουμε να ισχύει μια ιδιότητα, είτε να παραλείψουμε περιττές λεπτομέρειες ώστε να εστιάσουμε στο σημαντικό.

Οι συναρτήσεις με αφετηρία το σύνολο πηλίκο ορίζονται μέσω αντιπροσώπων της κλάσης. Χρειάζεται όμως προσοχή στο να είναι καλά ορισμένες δηλαδή ανεξάρτητες από την επιλογή του αντιπροσώπου. Θα επανέλθουμε στην έννοια αυτή ορισμού συναρτήσεων και πράξεων σε σύνολα πηλίκα πολύ συχνά.

Όπως παρατηρεί ο Masaaki Yoshida [14, παρ. 3 σελ. 6] στο παράδειγμα Ι.4.15 μπορούμε να έχουμε πολλές διαφορετικές ιστορίες αγάπης ανάμεσα σε αγόρια που αντιπροσωπεύουν την κλάση A_1 και σε κορίτσια που αντιπροσωπεύουν την κλάση A_2. Ορίζεται όμως και μια αφηρημένη έννοια αγάπης ανάμεσα στα στοιχεία του συνόλου πηλίκο, δηλαδή τα στοιχεία των κλάσεων ισοδυναμίας, όπως αυτή περιγράφηκε στο «Συμπόσιο» του Πλάτωνα[2].

Ι.4.2 Σχέσεις Διάταξης

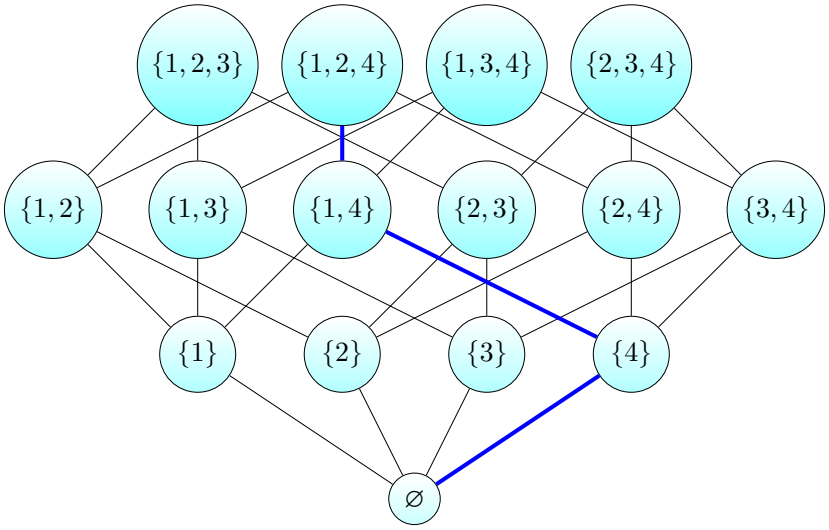
Ορισμός Ι.4.18. Μία σχέση $\Sigma \subset A \times A$ στο σύνολο A η οποία είναι ανακλαστική, μεταβατική και αντισυμμετρική θα λέγεται σχέση διάταξης ή σχέση μερικής διάταξης.

Αν επιπλέον για κάθε $a, b \in A$ ισχύει ότι είτε το $(a, b) \in \Sigma$ είτε το $(b, a) \in \Sigma$ θα λέγεται σχέση καθολικής διάταξης.

Παραδείγματα:

[1] Συνέντευξη στο LiFo 7.12.2022 | 08:13
https://www.lifo.gr/articles/apostolos-giannopoylos-polyplokos-einai-o-kosmos-ohi-ta-mathimatika

[2] 209e-212c https://www.greek-language.gr/digitalResources/ancient_greek/library/browse.html?text_id=110&page=26



Σχήμα I.6: Το σύνολο των γνησίων υποσυνόλων του $\{1,2,3,4\}$ μαζί με το ολικά διατεταγμένο υποσύνολο $\varnothing \subset \{4\} \subset \{1,4\} \subset \{1,2,4\}$.

1. Στο σύνολο των πραγματικών αριθμών ορίζουμε την σχέση $\Sigma_\leq \subset \mathbb{R}\times\mathbb{R}$, ως εξής: $(x,y) \in \Sigma$ αν και μόνο αν $x \leq y$. Η $\Sigma_\leq$ είναι σχέση διάταξης. Πράγματι, $x \leq x$ άρα $(x,x) \in \Sigma_\leq$ (ανακλαστική ιδιότητα). Επίσης αν $(x,y) \in \Sigma_\leq$ και $(y,z) \in \Sigma_\leq$ τότε εξ ορισμού $x \leq y$ και $y \leq z$, άρα $x \leq z$ δηλαδή $(x,z) \in \Sigma_\leq$ (μεταβατική ιδιότητα). Τέλος αν $(x,y) \in \Sigma_\leq$ και $(y,x) \in \Sigma_\leq$ τότε εξ ορισμού $x \leq y$ και $y \leq x$, άρα $x = y$ δηλαδή ισχύει η αντισυμμετρική ιδιότητα.

2. Θεωρούμε ένα σύνολο A, και το σύνολο των υποσυνόλων του A, $\mathcal{P}(A)$. Στο σύνολο $\mathcal{P}(A)\times\mathcal{P}(A)$ ορίζουμε την σχέση $\Sigma_\subset$ ως εξής: $(X,Y) \in \Sigma_\subset$ αν και μόνο αν $X \subset Y$. Η $\Sigma_\subset$ είναι μία σχέση διάταξης. Πράγματι, $X \subset X$ άρα $(X,X) \in \Sigma_\subset$ και συνεπώς ισχύει η ανακλαστική ιδιότητα. Αν $(X,Y) \in \Sigma_\subset$ και $(Y,Z) \in \Sigma_\subset$ τότε $X \subset Y$ και $Y \subset Z$ άρα $X \subset Z$ οπότε $(X,Z) \in \Sigma_\subset$ και συνεπώς ισχύει η μεταβατική ιδιότητα. Τέλος αν $(X,Y) \in \Sigma_\subset$ και $(Y,X) \in \Sigma_\subset$ τότε $X \subset Y$ και $Y \subset X$ άρα $X = Y$ και ισχύει και η αντισυμμετρική ιδιότητα.

3. Έστω a, b δύο φυσικοί αριθμοί. Θα λέμε ότι a διαιρεί τον b και θα το συμβολίζουμε με $a \mid b$ αν και μόνο αν υπάρχει $\lambda \in \mathbb{N}$ ώστε $b = \lambda a$. Στο σύνολο των φυσικών ορίζουμε την σχέση $\Sigma_| \subset \mathbb{N}\times\mathbb{N}$ ως εξής: $(a,b) \in \Sigma_|$ αν και μόνο αν $a \mid b$. Θα δείξουμε ότι είναι μία σχέση διάταξης. Πράγματι, $a \mid a$ αφού για $\lambda = 1$ έχουμε $a = \lambda a$. Άρα $(a,a) \in \Sigma_|$. Έστω $(a,b) \in \Sigma_|$ και $(b,c) \in \Sigma_|$. Άρα εξ ορισμού $a \mid b$ και $b \mid c$. Άρα υπάρχουν $\lambda_1, \lambda_2 \in \mathbb{N}$ ώστε $b = \lambda_1 a$ και $c = \lambda_2 b$. Συνεπώς $c = \lambda_2\lambda_1 a$ με $\lambda_2\lambda_1 \in \mathbb{N}$ και $a \mid c$ οπότε $(a,c) \in \Sigma_|$ και ισχύει η μεταβατική ιδιότητα. Τέλος, αν $(a,b) \in \Sigma_|$ και $(b,a) \in \Sigma_|$ τότε $a \mid b$ και $b \mid a$, άρα υπάρχουν $\lambda_1, \lambda_2 \in \mathbb{N}$ ώστε $a = \lambda_1 b$ και $b = \lambda_2 a$, οπότε $a = \lambda_1\lambda_2 a$, άρα $\lambda_1\lambda_2 = 1$ και αφού τα λ_1, λ_2 είναι φυσικοί έχουμε ότι $\lambda_1 = \lambda_2$ και συνεπώς $a = b$, άρα ισχύει και η αντισυμμετρική ιδιότητα.

I.4.3 Το λήμμα του Zorn

Ορισμός I.4.19. Το υποσύνολο B του μερικώς διατεταγμένου συνόλου A με την σχέση διάταξης $\leq$ θα λέμε ότι έχει άνω φράγμα το $c \in A$ αν $b \leq c$ για κάθε $b \in B$. Ένα maximal στοιχείο $m \in A$ είναι ένα στοιχείο το οποίο δεν έχει μεγαλύτερο στοιχείο στο $a \in A$, δηλαδή αν $m \leq a$ τότε $a = m$.

Ένα μερικά διατεταγμένο σύνολο A θα λέγεται επαγωγικό αν κάθε ολικά διατεταγμένο

υποσύνολο του έχει άνω φράγμα στο A.

Αν το m είναι maximal δεν σημαίνει κατανάγκη ότι το m είναι άνω φράγμα του A και επίσης μπορεί ένα σύνολο να έχει περισσότερα από ένα μέγιστα στοιχεία. Δείτε για παράδειγμα στο σχήμα I.6 στο οποίο περιγράφεται η σχέση διάταξη του εγκλεισμού στα γνήσια υποσύνολα του $\{1,2,3,4\}$.

Λήμμα I.4.20 (Το λήμμα του Zorn)**.** *Κάθε επαγωγικό μερικά διατεταγμένο σύνολο έχει maximal στοιχείο.*

Το λήμμα του Zorn είναι γνωστό ότι είναι ισοδύναμο με το αξίωμα της επιλογής το οποίο είναι ανεξάρτητο από τα συνήθη αξιώματα της θεωρίας συνόλων. Θα το χρησιμοποιήσουμε στο IV.3.10 για να δείξουμε ότι κάθε διανυσματικός χώρος έχει μία βάση.

Ασκήσεις

Άσκηση I.5 Θεωρήστε το σύνολο $A := \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$. Στο σύνολο αυτό ορίζουμε μία σχέση ως εξής:

$$(a,b) \equiv (a',b') \Leftrightarrow ab' - ba' = 0.$$

Αποδείξτε ότι η παραπάνω σχέση είναι σχέση ισοδυναμίας.

I.4.4 Συναρτήσεις

Οι συναρτήσεις αποτελούν μία ειδική κατηγορία σχέσεων οι οποίες ικανοποιούν τις παρακάτω ιδιότητες:

Ορισμός I.4.21. Μια διμελής σχέση $\Sigma \subset A \times B$, θα λέγεται συνάρτηση αν ισχύουν

1. Για κάθε $a \in A$ υπάρχει $b \in B$ ώστε $(a,b) \in \Sigma$
2. Αν $(a,b) \in \Sigma$ και $(a,b') \in \Sigma$, τότε $b = b'$.

Για κάθε $a \in A$ το μοναδικό $b \in B$ ώστε $(a,b) \in \Sigma$ θα το συμβολίζουμε με $f(a)$. Ένας συνηθισμένος τρόπος να συμβολίζουμε μία συνάρτηση είναι με $f : A \to B$. Το A λέγεται πεδίο ορισμού της συνάρτησης ενώ το B σύνολο τιμών.

Για παράδειγμα η σχέση $\Sigma \subset \{1,2,3\} \times \{1,2\}$, όπου $\Sigma = \{(1,2),(2,1)\}$ δεν ορίζει συνάρτηση γιατί το 3 δεν σχετίζεται με κανένα στοιχείο του $\{1,2\}$. Αν θεωρήσουμε την $\Sigma' \subset \{1,2,3\} \times \{1,2\}$ με $\Sigma' = \{(1,2),(2,1),(3,1)\}$ τότε η σχέση αυτή ορίζει συνάρτηση γιατί ικανοποιούνται όλες οι προϋποθέσεις του ορισμού. Αν μάλιστα θέλουμε μπορούμε να γράψουμε την συνάρτηση ως $f : \{1,2,3\} \to \{1,2\}$, με $f(1) = 2, f(2) = 1, f(3) = 1$.

Ορισμός I.4.22. Θεωρούμε μία συνάρτηση $f : A \to B$. Θα λέμε ότι η συνάρτηση είναι επί αν για κάθε $b \in B$ υπάρχει τουλάχιστον ένα $a \in A$, ώστε $f(a) = b$. Θα λέμε ότι η συνάρτηση είναι ένα προς ένα αν $f(a_1) = f(a_2)$ τότε $a_1 = a_2$.

Για παράδειγμα η συνάρτηση που ορίσαμε προηγουμενως είναι επί αλλά όχι ένα προς ένα αφού $f(3) = f(2) = 1$ αλλά $3 \neq 2$.

Κάθε συνάρτηση $f : A \to B$, ορίζεται και ορίζει μία σχέση $\Sigma_f \subset A \times B$, όπου το Σ_f αποτελείται από τα ζευγάρια $(a, f(a))$. Το Σ_f θα το λέμε και γράφημα της συνάρτησης f. Αν μάλιστα δούμε τα σύνολα A, B μπορούμε να τα «ζωγραφίσουμε» (για παράδειγμα στην περίπτωση $A = B = \mathbb{R}$, το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$, μπορούμε να το παραστήσουμε ως το σύνολο των σημείων του επιπέδου, ενώ το υποσύνολο που αντιστοιχεί στο Σ_f θα το ονομάζουμε γραφική παράσταση της f.

Στην συνάρτηση f αντιστοιχεί ένα γράφημα Σ_f. Το γράφημα αυτό έχει πάντα μία καλά ορισμένη αντίστροφη σχέση. Είναι αυτή η σχέση συνάρτηση;

Πρόταση I.4.23. *Η αντίστροφη σχέση του γραφήματος μίας συνάρτησης είναι συνάρτηση αν και μόνο αν η συνάρτηση f είναι ένα προς ένα και επί.*

Απόδειξη. Το γράφημα της συνάρτησης αποτελείται από τα ζευγάρια $(a, f(a))$ άρα η αντίστροφη σχέση θα αποτελείται από τα ζευγάρια

$$\Sigma_f^{-1} := \{(f(a), a) : a \in A\} \subset B \times A.$$

Οι πρώτη προϋπόθεση του ορισμού της συνάρτησης μεταφράζεται στο ότι για κάθε $b \in B$ υπάρχει $a \in A$ ώστε $(b, a) \in \Sigma^{-1}$ ή ισοδύναμα $b = f(a)$ για κάποιο a, δηλαδή η f πρέπει και αρκεί να είναι επί.

Από την άλλη η δεύτερη προϋπόθεση μεταφράζεται ότι αν $(b, a_1), (b, a_2) \in \Sigma_f^{-1}$ τότε $a_1 = a_2$, δηλαδή αν $f(a_1) = f(a_2)$ τότε $a_1 = a_2$. Δηλαδή για να ικανοποιεί η Σ_f^{-1} την δεύτερη προϋπόθεση του ορισμού της συνάρτησης πρέπει και αρκεί να είναι ένα προς ένα. □

Παράδειγμα I.4.24. Η συνάρτηση $f : \mathbb{R} \to \mathbb{R}$ η οποία στέλνει το x στο x^2, δηλαδή $f(x) = x^2$ δεν είναι ούτε ένα προς ένα ούτε επί. Πράγματι, δεν μπορεί να είναι ένα προς ένα αφού τα $1^2 = 1 = (-1)^2$ ενώ $1 \neq -1$. Για το επί παρατηρούμε ότι δεν υπάρχει πραγματικός αριθμός που το τετράγωνο του να είναι αρνητικός. Άρα η αντίστροφη σχέση του γραφήματος της x^2 δεν είναι συνάρτηση.

Ορισμός I.4.25. Μία συνάρτηση της οποίας το γράφημα S_f έχει αντίστροφη σχέση S_f^{-1} που αντιστοιχεί σε συνάρτηση θα λέγεται αντιστρέψιμη. Η δε συνάρτηση που αντιστοιχεί στην σχέση S_f^{-1} θα λέγεται αντίστροφη της f και θα την συμβολίζουμε με f^{-1}.

Ορισμός I.4.26. Αν $f : A \to B$ και $g : B \to C$ είναι δύο συναρτήσεις, θα συμβολίζουμε με $g \circ f$ και θα την ονομάζουμε σύνθεση των συναρτήσεων f, g, την συνάρτηση $g \circ f : A \to C$, η οποία στέλνει το x στο $g(f(x))$.

Ορισμός I.4.27. Η συνάρτηση $\mathbb{I}_A : A \to A$ η οποία στέλνει το $x \in A$ στο $\mathbb{I}_A(x) = x$ θα λέγεται η ταυτοτική συνάρτηση του A.

Πρόταση I.4.28. *Έστω $f : A \to B$ μία αντιστρέψιμη συνάρτηση. Η αντίστροφη συνάρτηση*

$f^{-1} : B \to A$ *ικανοποιεί:*

$$f \circ f^{-1} = \mathbb{I}_B, \quad f^{-1} \circ f = \mathbb{I}_A.$$

Απόδειξη. Πράγματι, παρατηρούμε ότι η η συνάρτηση f^{-1} είναι η συνάρτηση που προέρχεται από την σχέση Σ_f^{-1}, τα στοιχεία της οποίας είναι διατεταγμένα ζεύγη της μορφής $(f(a), a) = (b, f^{-1}(b)$. Έστω $b \in B$. Αφού η f είναι αντιστρέψιμη είναι επί, άρα υπάρχει $a \in A$, με $b = f(a)$. Άρα η παραπάνω σχέση γράφεται ως $(f(a), a) = (b, f^{-1}(f(a)))$, άρα $a = f^{-1}(f(a))$ και $f^{-1} \circ f = \mathbb{I}_A$. Για να αποδείξουμε την ισότητα $f \circ f^{-1} = \mathbb{I}_B$, εργαζόμαστε ομοίως, αντικαθιστόντας την f με την f^{-1} (παρατηρήστε ότι $(f^{-1})^{-1} = f$. □

Ορισμός Ι.4.29. Έστω $A, \leq$, $B, \leq$, σύνολα στα οποία έχουν οριστεί σχέσεις διάταξης και έστω $f : A \to B$. Θα λέμε ότι η f είναι:

1. *Αύξουσα* Αν $a \leq b \Rightarrow f(a) \leq f(b)$
2. *Γνήσια Αύξουσα* Αν $a < b \Rightarrow f(a) < f(b)$
3. *Φθίνουσα* Αν $a \leq b \Rightarrow f(b) \leq f(a)$
4. *Γνήσια Φθίνουσα* Αν $a < b \Rightarrow f(b) < f(a)$

Παράδειγμα Η συνάρτηση $f : \mathbb{N} \to \mathbb{N}$, με τύπο $f(x) = x^3$ είναι γνήσια αύξουσα αφού αν $x_1 < x_2$ τότε $x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) < 0$.

Ορισμός Ι.4.30. Θεωρούμε μία συνάρτηση $f : A \to B$ και έστω $A_1 \subset A$. Μπορούμε να ορίσουμε μία νέα συνάρτηση $f|_{A_1} : A_1 \to B$ την οποία θα ονομάζουμε περιορισμό της f και η οποία θα στέλνει το $x \in A_1 \subseteq A$ στο $f|_{A_1}(x) := f(x)$. Η συνάρτηση f θα λέγεται επέκταση της $f|_{A_1}$.

Παραδείγματα Θεωρούμε την συνάρτηση $\mathbb{R} \to \mathbb{R}$ με τύπο $f(x) = x^2$. Είναι σαφές ότι η f δεν είναι ένα προς ένα. Ο περιορισμός $f|_{x \in \mathbb{R}, x \geq 0}$ της f στο σύνολο των θετικών πραγματικών αριθμών είναι ένα προς ένα, αφού αν $x_1^2 = x_2^2$ τότε $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) = 0$. Άρα $x_1 = -x_2$ ή $x_1 = x_2$. Η πρώτη περίπτωση όμως πρέπει να αποκλειστεί αφού $x_1, x_2 \geq 0$.

Ορισμός Ι.4.31. Θα λέμε ότι δύο συναρτήσεις $f_i : A_i \to B_i$, $i = 1, 2$ είναι ίσες αν και μόνο αν τα αντίστοιχα γραφήματα είναι ίσα. Ο ορισμός αυτός είναι ισοδύναμος με το ότι $A_1 = A_2$, $B_1 = B_2$ και $f_1(x) = f_2(x)$ για όλα τα $x \in A_1 = A_2$.

Παρατήρηση Πολλοί συγγραφείς ορίζουν δύο συναρτήσεις f_1, f_2 να είναι ίσες αν έχουν το ίδιο πεδίο ορισμού A και $f_1(x) = f_2(x)$ για κάθε $x \in A$, χωρίς να ελέγξουν το σύνολο άφιξης. Ο ορισμός αυτός είναι προβληματικός γιατί αν μία συνάρτηση $f : A \to B$ είναι επί, και $f_1 : A \to B'$ είναι μία συνάρτηση με σύνολο άφιξης το $B \subset B'$ και $f(x) = f_1(x)$ για κάθε $x \in A$ τότε θα θεωρούσαμε τις f, f_1 ίσες αλλά η μία θα ήταν επί και η άλλη όχι. Δηλαδή η ιδιότητα του επί δεν θα ήταν καλά ορισμένη.

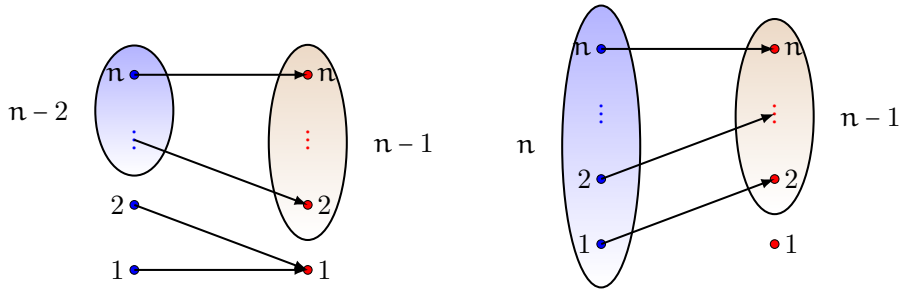
Ι.4.5 Μεταθέσεις

Ορισμός I.4.32. Έστω ένα πεπερασμένο σύνολο $\Sigma = \{1, 2, \dots, n\}$. Μία μετάθεση του Σ είναι μια συνάρτηση $\sigma \in \Sigma$ η οποία είναι 1-1 και επί.

Παρατήρηση I.4.33. Μία συνάρτηση $f : S \to S$, όπου S είναι ένα πεπερασμένο σύνολο με n-στοιχεία είναι 1-1 αν και μόνο αν είναι επί.

Πράγματι, αν μια συνάρτηση δεν είναι 1-1 τότε υπάρχουν δύο τουλάχιστον στοιχεία του πεδίου ορισμού, χωρίς περιορισμό της γενικότητας τα $\{1, 2\}$ ώστε $f(1) = f(2) = 1$. Σε αυτή την περίπτωση είναι αδύνατον να καλύψουμε με τα $n-2$ στοιχεία $\{3, 4, \dots, n\}$ τα $n-1$ στοιχεία $\{2, 3, \dots, n\}$. Άρα η f δεν μπορεί να είναι επί.

Αντιστρόφως, αν η f δεν είναι επί τότε υπάρχει ένα στοιχείο για παράδειγμα το 1 το οποίο δεν είναι εικόνα κάποιου $k \in \{1, 2, \dots, n\}$. Συνεπώς τα n στοιχεία $\{1, 2, \dots, n\}$ θα πρέπει να απεικονισθούν στα $n-1$ στοιχεία $2, 3, \dots, n$. Συνεπώς, θα υπάρχουν τουλάχιστον δύο βέλη που θα καταλήξουν στην ίδια εικόνα. Το τελευταίο είναι γνωστό και ως αρχή του περιστεριώνα.



Σχήμα I.7: Αριστερά βλέπουμε ότι αν δύο στοιχεία απεικονιστούν στην ίδια εικόνα, οπότε η συνάρτηση f δεν είναι 1-1 τότε θα πρέπει με $n-2$ στοιχεία να καλύψουμε $n-1$ θέσεις, άρα η η συνάρτηση δεν είναι ούτε επί. Δεξιά βλέπουμε ότι αν παραλείψουμε ένα στοιχείο από την εικόνα, δηλαδή αν η συνάρτηση f δεν είναι επί, τότε έχουμε n στοιχεία στο σύνολο αφετηρίας να τα στείλουμε σε $n-1$ δυνατές εικόνες άρα δύο θα πάνε σε ένα και η συνάρτηση δεν είναι ούτε 1-1.

Παρατήρηση I.4.34. Για άπειρα σύνολα δεν είναι σωστό ότι μια συνάρτηση είναι ένα προς ένα αν και μόνο αν είναι επί. Θα δούμε ότι ένας από τους κύριους προταγωνιστές του μαθήματος αυτού οι γραμμικές συναρτήσεις $L : V \to V$ από ένα πεπερασμένης διάστασης χώρο V στον εαυτό του είναι ένα προς ένα αν και μόνο αν είναι επί, δείτε το V.2.3.

Μια μετάθεση σ μπορεί να αναπαρασταθεί ως εξής

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

όπου με τον παραπάνω συμβολισμό εννοούμε ότι

$$\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 5, \sigma(5) = 3.$$

Θα συμβολίζουμε το σύνολο όλων των μεταθέσεων ενός συνόλου με n το πλήθος στοιχεία με S_n,

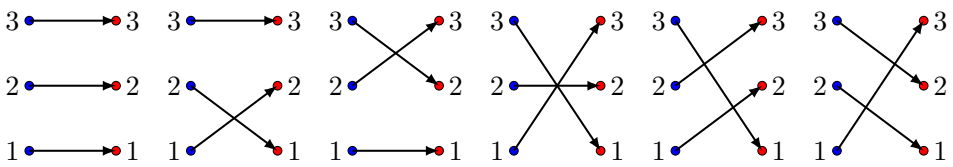
$$S_n = \{\sigma : \{1, 2, \dots, n\} \overset{\text{1-1,επί}}{\longrightarrow} \{1, 2, \dots, n\}\}.$$

Το σύνολο S_n έχει $n! := 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$ το πλήθος στοιχεία. Πράγματι, οι αντιστρέψιμες συναρτήσεις από το $\{1, 2, \dots, n\}$ στο $\{1, 2, \dots, n\}$ ταυτίζονται με τις 1-1 συναρτήσεις. Έτσι για το $\sigma(1)$ έχουμε n το πλήθος επιλογές, για το $\sigma(2)$, έχοντας ήδη επιλέξει το $\sigma(1)$ έχουμε $n-1$ επιλογές αφού δεν μπορούμε να επιλέξουμε $\sigma(1) = \sigma(2)$. Συνεχίζοντας με τον ίδιο τρόπο για το $\sigma(3)$

έχουμε $n-2$ επιλογές και τελικά για το $\sigma(n)$ έχουμε 1 επιλογή, το στοιχείο που δεν έχουμε ήδη διαλέξει. Συνολικά έχουμε $n!$ διαφορετικά στοιχεία. Έτσι το $S_1 = \mathrm{Id}$, $S_2 = \left\{\begin{pmatrix}1&2\\1&2\end{pmatrix}, \begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$ ενώ

$$S_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\},$$

δείτε και το σχήμα I.8.



Σχήμα Ι.8: Οι $6 = 3!$ διαφορετικές μεταθέσεις του συνόλου $\{1,2,3\}$

Η σύνθεση συναρτήσεων μας δίνει ένα τρόπο να «πολλαπλασιάσουμε μεταθέσεις», δηλαδή μπορούμε να ορίσουμε μια συνάρτηση

$$\begin{aligned} S_n \times S_n &\longrightarrow S_n \\ (f,g) &\longmapsto f \circ g. \end{aligned}$$

Για παράδειγμα στο σχήμα I.9 δείχνουμε σχηματικά ότι

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$$

Παρατηρούμε ότι η πράξη δεν είναι αντιμεταθετική, δηλαδή αν συνθέσουμε με διαφορετική σειρά παίρνουμε διαφορετικό αποτέλεσμα

$$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&3&1\end{pmatrix}$$

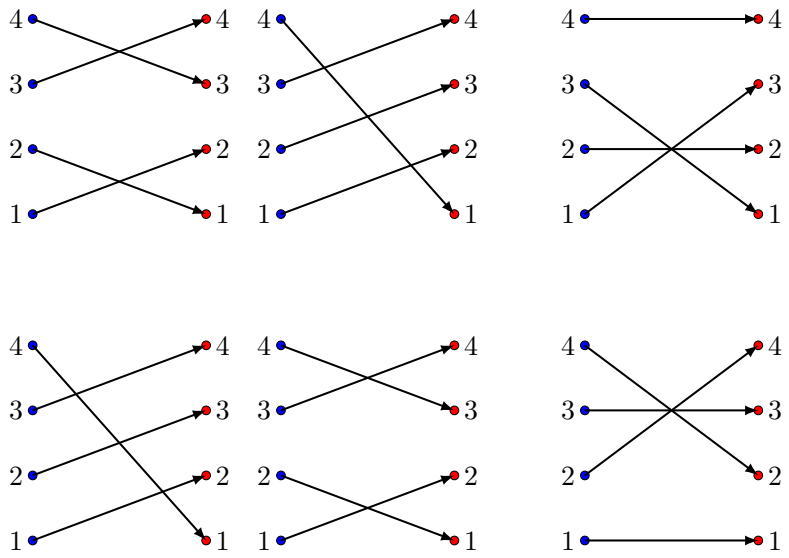
Ορισμός Ι.4.35. Μια αντιμετάθεση είναι μια μετάθεση του συνόλου $\{1,2,\ldots,n\}$ στην οποία αλλάζουν θέση μόνο δύο στοιχεία του συνόλου τα i,j. Την αντιμετάθεση αυτή την συμβολίζουμε με (i,j).

Παράδειγμα Ι.4.36. Στο παρακάτω παράδειγμα έχουμε την αντιμετάθεση $(2,4)$ όπου μόνο τα στοιχεία $2,4$ αλλάζουν θέση, ενώ τα $1,3,5$ παραμένουν σταθερά.

$$\begin{pmatrix}1&2&3&4&5\\1&4&3&2&5\end{pmatrix} = (2,4).$$

Πρόταση Ι.4.37. *Κάθε μετάθεση γράφεται ως γινόμενο αντιμεταθέσεων.*

Απόδειξη. Φανταζόμαστε μια μετάθεση ως ένα ανακάτωμα του συνόλου $\{1,2,\ldots,n\}$, για παράδειγμα ενός συνόλου από αριθμημένες σελίδες που έχουν ανακατωθεί. Μπορούμε να τις φέρουμε στην σειρά ακολουθώντας την παρακάτω διαδικασία: Ξεκινάμε από την αρχή των σελίδων και ψάχνουμε να βρούμε την θέση i_1 που είναι η σελίδα με τον αριθμό 1. Εναλλάσσουμε τις



Σχήμα Ι.9: Πολλαπλασιασμός μεταθέσεων. Ακολουθούμε τα βέλη από αριστερά στην σύνθεση και προκύπτει η μετάθεση στα δεξιά. Ο πολλαπλασιασμός με την αντίθετη σειρά δίνει διαφορετικό αποτέλεσμα.

πρώτη με την i σελίδα, δηλαδή κάνουμε την μετάθεση $(1, i_1)$. Η πρώτη σελίδα έχει έρθει στην κορυφή. Συνεχίζουμε με την δεύτερη σελίδα, ψάχνουμε να βρούμε την θέση i_2 στην οποία είναι η σελίδα με τον αριθμό 2 και εναλλάσσουμε την δεύτερη σελίδα με την i_2 δηλαδή εκτελούμε την μετάθεση $(2, i_2)$. Η πρώτη και η δεύτερη σελίδα είναι τώρα στην κορυφή. Συνεχίζουμε με τον ίδιο τρόπο μέχρι όλες οι σελίδες να είναι στην σειρά και έχουμε αναιρέσει το ανακάτωμα. □

Παράδειγμα Ι.4.38. θεωρούμε την μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix}$$

Δηλαδή μπορούμε να φανταστούμε ότι ένα άρθρο 6 σελίδων έχει ανακατωθεί και οι σελίδες είναι αριθμημένες με την σειρά $\{4,3,1,6,2,5\}$. Η σελίδα με τον αριθμό 1 είναι στην $i_1 = 3$ θέση. Οπότε εναλλάσσουμε την πρώτη με την τρίτη σελίδα, μετάθεση $(1,3)$. Καταλήγουμε στο σύνολο $\{1,3,4,6,2,5\}$. Στην συνέχεια η σελίδα με τον αριθμό 2 είναι στην πέμπτη $i_2 = 5$ θέση, οπότε εναλλάσσουμε την δεύτερη με την πέμπτη σελίδα, μετάθεση $(2,5)$ και το σύνολο γίνεται $\{1,2,4,6,3,5\}$. Συνεχίζουμε με τον ίδιο τρόπο εκτελώντας την μετάθεση $(3,5)$, οπότε το σύνολο γίνεται το $\{1,2,3,6,4,5\}$, την μετάθεση $(4,5)$ οπότε το σύνολο γίνεται $\{1,2,3,4,6,5\}$ και τέλος την $(5,6)$ οπότε οι σελίδες έχουν μπει στην σειρά $\{1,2,3,4,5,6\}$. Δηλαδή ως συνθέσεις έχουμε

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix} = (5,6)(4,5)(3,5)(2,5)(1,3),$$

δηλαδή την ζητούμενη γραφή της σ ως γινόμενο αντιμεταθέσεων.

Παρατήρηση Ι.4.39. Η γραφή μιας μετάθεσης ως γινόμενο αντιμεταθέσεων δεν είναι μοναδική. Για παράδειγμα η μετάθεση

$$(7,2)(3,8)(1,7)(2,8)(4,7) = (6,9)(6,4)(6,8)(1,2)(1,7)(1,5)(1,3)(5,6)(2,4)$$

Από το παραπάνω επίσης είναι σαφές ότι ούτε το πλήθος των αντιμεταθέσεων παραμένει σταθερό. Θα δώσουμε μια απόδειξη όταν εισάγουμε την έννοια της ορίζουσας ότι αυτό που παραμένει σταθερό είναι το αν το πλήθος είναι άρτιο ή περιττό, δείτε την εξίσωση (III.5).

Ι.5 Ισοπληθικά Σύνολα

Ορισμός Ι.5.1. Τα σύνολα A, B θα λέγονται ότι έχουν το ίδιο πλήθος, αν υπάρχει συνάρτηση $f : A \to B$ η οποία να είναι 1-1 και επί.

Παρατήρηση Ι.5.2. Παρατηρούμε ότι η σχέση $A \sim B$ αν και μόνο αν A, B είναι ισοπληθικά είναι μια σχέση ισοδυναμίας. Πράγματι το A είναι ισοπληθικό με τον ευατό του, αρκεί να χρησιμοποιήσουμε την ταυτοτική συνάρτηση. Αν το A είναι ισοπληθικό με το B μέσω της 1-1 και επί συνάρτησης f τότε και το B είναι ισοπληθικό με το A μέσω της 1-1 και επί συνάρτησης f^{-1}. Τέλος αν το A είναι ισοπληθικό με το B μέσω της 1-1 και επί συνάρτησης $f : A \to B$ και το B είναι ισοπληθικό με το C μέσω της 1-1 και επί συνάρτησης $g : A \to B$ τότε και το A γίνεται ισοπληθικό με το C μέσω της 1-1 και επί συνάρτησης $g \circ f$.

Παρατήρηση Ι.5.3. Δύο πεπερασμένα σύνολα είναι ισοπληθικά αν και μόνο αν έχουν τον ίδιο πληθάριθμο. Θα μπορούσαμε να ορίσουμε το σύνολο των φυσικών αριθμών $\mathbb{N} = \{0, 1, 2, \ldots\}$ ως το σύνολο πηλίκο των κλάσεων ισοδυναμίας των πεπερασμένων συνόλων ως προς την σχέση ισοδυναμίας της ισοπληθικότητας.

Στην περίπτωση των πεπερασμένων συνόλων η κατάσταση της ισοπληθικότητας ξεφεύγει από την διαίσθηση του ισοπληθικού που έχουμε από τα πεπερασμένα σύνολα.

Ορισμός Ι.5.4. Ένα σύνολο A θα λέγεται αριθμήσιμο αν και μόνο αν είναι ισοπληθικό με το σύνολο των φυσικών αριθμών, δηλαδή αν και μόνο αν υπάρχει μια συνάρτηση $f : \mathbb{N} \to A$. Ένα σύνολο θα λέγεται το πολύ αριθμήσιμο αν είναι είτε πεπερασμένο ή αριθμήσιμο.

Παρατήρηση Ι.5.5. Αν σε ένα αριθμήσιμο σύνολο A προσθέσουμε ένα ακόμα στοιχείο αυτό εξακολουθεί να είναι αριθμήσιμο δηλαδή ισοπληθικό με το A. Πράγματι, έχουμε ότι η συνάρτηση

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n + 1 \end{aligned}$$

είναι 1-1 και επί του συνόλου $\{1, 2, 3, \ldots\}$, συνεπώς υπάρχει η αντίστροφη συνάρτηση

$$f^{-1} : \{1, 2, 3, \ldots\} \longrightarrow \mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

Συνεπώς αν $\phi : \mathbb{N} \to A$ είναι μια 1-1 και επί συνάρτηση, μπορούμε να ορίσουμε μια 1-1 και επί συνάρτηση $\Phi : \mathbb{N} \to A \cup \{x\}$ ως εξής:

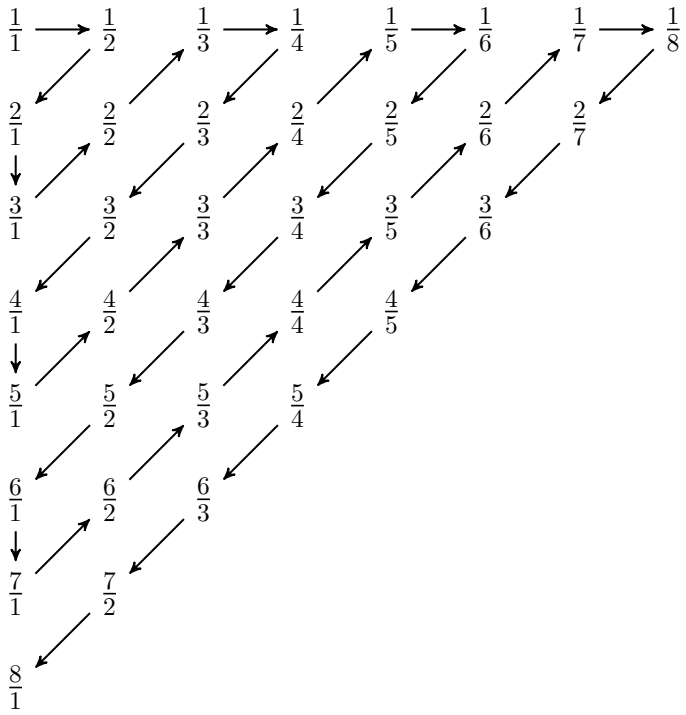
$$\Phi(0) = x, \Phi(n) = \phi(f^{-1}(n)) \text{ για } n \geq 1.$$

Το παράδειγμα αυτό είναι γνωστό ως «Ξενοδοχείο του Hilbert». Σε ένα ξενοδοχείο με άπειρα αριθμημένα δωμάτια το οποίο είναι πλήρες καταφθάνει ένας νέος επισκέπτης. Ο ξενοδόχος δεν έχει να ζητήσει από όλους τους ενοίκους να μετακινηθούν στο επόμενο δωμάτιο οπότε το πρώτο δωμάτιο είναι τώρα ελεύθερο.

Παράδειγμα Ι.5.6. Τα σύνολα των ακεραίων και ρητών είναι αριθμήσιμα. Πράγματι για το σύνολο των ακεραίων έχουμε ότι η συνάρτηση

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto f(n) = \begin{cases} \frac{n+1}{2} \text{ αν } n \text{ περιττός} \\ -\frac{n}{2} \text{ αν } n \text{ άρτιος} \end{cases} \end{aligned}$$

είναι 1-1 και επί.



Σχήμα I.10: Μία αρίθμηση των ρητών θετικών αριθμών, συνεχίζουμε με παρόμοιο τρόπο την διαδικασία

Παράδειγμα I.5.7. Το σύνολο των ρητών είναι αριθμήσιμο. Αντί να γράψουμε μία πολύπλοκη 1-1 και επί συνάρτηση θα δείξουμε πρώτα σχηματικά, στο σχήμα I.10 πως μπορούμε να έχουμε μία 1-1 και επί συνάρτηση από τους φυσικούς $\mathbb{N}$ στο σύνολο των ρητών θετικών αριθμών. Για να αριθμήσουμε το σύνολο των ρητών $\mathbb{Q}$ ξεκινάμε από το 0 και προσθέτουμε τον $-p/q$ αμέσως μετά τον p/q.

Το ερώτημα είναι αν υπάρχουν σύνολα τα οποία δεν είναι αριθμήσιμα.

Θεώρημα I.5.8. *Το σύνολο των πραγματικών αριθμών $\mathbb{R}$ δεν είναι αριθμήσιμο.*

Απόδειξη. Θα δείξουμε ότι το σύνολο των πραγματικών αριθμών $A = \{x \in \mathbb{R} : 0 < x \leq 1\}$ δεν είναι αριθμήσιμο. Το δεκαδικό ανάπτυγμα ενός πραγματικού αριθμού $x \in A$ είναι ένας αριθμός της μορφής

$$0, x_1x_2x_3x_4 \ldots = 0.113512280\ldots$$

όπου $x_1 = 1$, $x_2 = 1$, $x_3 = 3$, $x_4 = 3$ κτλ. Δηλαδή, $x_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Αν μάλιστα αποκλήσουμε την περίπτωση της άπειρης ακολουθίας που καταλήγει σε 9, όπως $0.2 = 0,1999999\ldots$ έχουμε ότι το δεδαδικό ανάπτυγμα του x είναι μοναδικό και μπορεί να οριστεί ως

$$x_i = [10^i x] - 10[10^{i-1}x].$$

Υποθέτουμε για να καταλλήξουμε σε άτοπο, ότι υπάρχει μια απαρίθμηση των πραγματικών

αριθμών στο A οπότε γράφουμε στην σειρά:

$$\begin{aligned} x_1 &= 0, x_{11}x_{12}x_{13}x_{14}\dots \\ x_2 &= 0, x_{21}x_{22}x_{23}x_{24}\dots \\ x_3 &= 0, x_{31}x_{32}x_{33}x_{34}\dots \\ &\vdots \quad \vdots \\ x_n &= 0, x_{n1}x_{n2}x_{n3}x_{n4}\dots \\ &\vdots \quad \vdots \end{aligned}$$

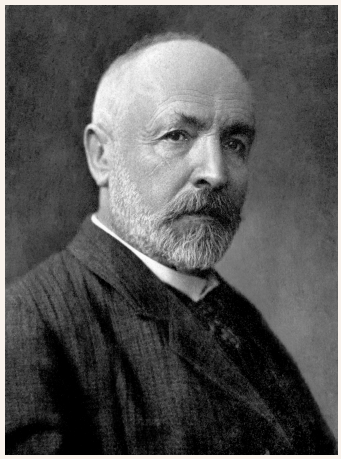
Για κάθε n διαλέγουμε $b_n \leq 2$ ώστε $b_n \neq x_{nn}$. Με αυτό τον τρόπο κατασκευάζουμε το δεκαδικό ανάπτυγμα του αριθμού

$$b = 0, b_1b_2b_3b_4\dots$$

ο οποίος διαφέρει στην n θέση από όλους τους αριθμούς $x_1, \dots, x_n, \dots$ άρα είναι ένας αριθμός στο A διαφορετικός από όλους τους αριθμούς $x_1, \dots, x_n, \dots$ που έχουμε καταγράψει. Συνεπώς δεν είναι δυνατόν να αριθμήσουμε τα στοιχεία του A και κατά συνέπεια ούτε τα στοιχεία του $\mathbb{R}$. □

Για περισσότερες πληροφορίες παραπέμπουμε στα [15, 1.3] και [2, κεφ. 19].

Ο **Georg Ferdinand Ludwig Philipp Cantor** (3 Μαρτίου 1845 – 6 Ιανουαρίου 1918) ήταν πρωτοπόρος της θεωρίας συνόλων. Εργάστηκε πάνω στην θεωρία των πληθαρίθμων μη-πεπερασμένων συνόλων και απέδειξε ότι το οι πραγματικοί αριθμοί έχουν «περισσότερα» στοιχεία από τους φυσικούς αριθμούς. Εισήγαγε την έννοια του αριθμήσιμου και μη-αριθμήσιμου συνόλου και διατύπωσε την εικασία του συνεχούς, η οποία ήταν και το πρώτο από τα ανοιχτά ερωτήματα που ξεχώρισε ο D. Hilbert στην περίφημη ομιλία του το 1900 στο διεθνές συνέδριο Μαθηματικών στο Παρίσι. Εισήγαγε την έννοια του δυναμοσυνόλου και απόδειξε ότι έχει «περισσότερα» στοιχεία από το ίδιο το σύνολο, αποτέλεσμα γνωστό και ως θεώρημα του Cantor. Μελέτησε προβλήματα σχετικά με συνολοθεωρητική τοπολογία σχετικά με το σύνολο Cantor και ήταν πρωτοπόρος στην θεωρία που σήμερα είναι γνωστή ως θεωρία των fractals.



Ι.6 Μια σειρά από σύνολα που πρωταγωνιστούν στα Μαθηματικά

Στα Μαθηματικά κατασκευάζουμε μια σειρά από σύνολα τα οποία προκύπτουν από βασικές ανάγκες τους, τα οποία τα θεωρούμε να περιέχεται το ένα μέσα στο άλλο

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Στην παράγραφο αυτή θα περιγράψουμε το κάθε ένα από αυτά εξηγώντας και την ανάγκη που μας οδήγησε στον ορισμό και στην χρήση τους και μερικές από τις βασικές τους ιδιότητες. Θα μπορούσε να πει κανείς ότι οι φυσικοί αριθμοί είναι δημιούργημα της ανάγκης για αρίθμηση διαφόρων αντικειμένων της καθημερινής ζωής. Όπως είπε ο R. Dedekind

> «Ο Θεός έφτιαξε τους φυσικούς αριθμούς, όλα τα υπόλοιπα είναι δημιούργημα του ανθρώπου»

Στην συνέχεια ορίσαμε τους ακέραιους αριθμούς ως αποτέλεσμα της ανάγκης να αφαιρέσουμε από μικρότερο φυσικό έναν μεγαλύτερο. Οι ρητοί αριθμοί εισάγονται για να μπορέσουμε να χειριστούμε κλάσματα στην περίπτωση που ο παρονομαστής δεν διαιρεί τον αριθμητή. θα δώσουμε μια κατασκευή και των ακεραίων αλλά και των ρητών με βάση την έννοια του χώρου πηλίκου μιας ισοδυναμίας.

Οι πραγματικοί αριθμοί κατασκευάστηκαν για λόγους που έχουν την βάση τους στην ανάλυση, συγκεκριμένα για να ισχύει το αξίωμα της πληρότητας. Θα συζητήσουμε δύο διαφορετικούς τρόπους κατασκευής των πραγματικών.

Τέλος οι μιγαδικοί αριθμοί κατασκευάστηκαν για να έχει λύση η εξίσωση $x^2 + 1 = 0$. Αυτή η απαίτηση είναι αρκετή για να έχει κάθε πολυώνυμο όλες του τις ρίζες στους μιγαδικούς αριθμούς.

I.6.1 Στοιχειώδης θεωρία Αριθμών

Το πρώτο σύνολο το οποίο θεωρούμε είναι το σύνολο των φυσικών αριθμών $\mathbb{N}$. Γενικά έχει απασχολήσει αρκετά τους μαθηματικούς αλλά και τους φιλόσοφους τι ακριβώς είναι οι φυσικοί αριθμοί και πως μπορεί το σύνολο των φυσικών αριθμών να θεμελιωθεί αξιωματικά. Οι προβληματισμοί αυτοί δεν θα μας απασχολήσουν σε αυτό το πρώτο μάθημα.

Για δύο τυχαίους φυσικούς αριθμούς, n, m η διαφορά τους $n - m$ είναι φυσικός αριθμός μόνο αν $n > m$. Προκειμένου η αφαίρεση να είναι καλά ορισμένη, ορίζουμε το σύνολο των $\mathbb{Z}$ των ακεραίων αριθμών, δηλαδή το σύνολο

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$$

Στην πραγματικότητα προκειμένου να ορίσουμε τους ακεραίους για κάθε $n \in \mathbb{N}$ «επισυνάπτουμε)) στο σύνολο των φυσικών αριθμών ένα στοιχείο $-n$ ώστε $n + (-n) = 0$.

Στην πραγματικότητα το σύνολο των ακεραίων ορίζεται ως το σύνολο των κλάσεων ισοδυναμίας στο σύνολο

$$(\mathbb{N} \times \mathbb{N}) : (a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Παρατηρούμε ότι αυτή είναι πράγματι μια σχέση ισοδυναμίας αφού

- Το $(a, b) \sim (a, b)$ αφού $a + b = a + b$.
- Αν το $(a, b) \sim (c, d)$ τότε $a + d = b + c \Rightarrow c + b = d + a$ άρα $(c, d) \sim (a, b)$.
- Αν $(a, b) \sim (c, d)$ και $(c, d) \sim (e, f)$ τότε $a + d = b + c$ $c + f = d + e$ συνεπώς $a + d + c + f = b + c + d + e$ άρα $a + f = b + e$, δηλαδή $(a, b) \sim (e, f)$.

Παρατήρηση I.6.1. Στην απόδειξη χρησιμοποιήσαμε ότι η πρόσθεση στους φυσικούς είναι αντιμεταθετική αλλά και το ότι αν $a + e = b + e$ τότε $a = b$ για φυσικούς αριθμούς a, b, e.

Ορισμός I.6.2. Θεωρούμε το σύνολο πηλίκο $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$, στο οποίο ορίζουμε πρόσθεση:

$$[(a, b) + (c, d)] = [a + c, b + d].$$

Παρατηρούμε ότι η πράξη είναι καλά ορισμένη δηλαδή αν $(a, b) \sim (a', b')$ και $(c, d) \sim (c', d')$, δηλαδή $[a, b] = [a', b']$ και $[(c, d)] = [(c', d')]$ τότε $[(a, b)] + [(c, d)] = [(a', b')] + [(c', d')]$.

Επίσης παρατηρούμε ότι οι φυσικοί μπορούν να θεωρηθούν ως υποσύνολο των ακεραίων θεωρώντας την 1-1 συνάρτηση

$$\begin{aligned} \mathbb{N} &\longrightarrow (\mathbb{N} \times \mathbb{N})/\sim = \mathbb{Z} \\ n &\longmapsto [(n, 0)]. \end{aligned}$$

Με βάση το παραπάνω ένας φυσικός είναι μια κλάση $[(a,b)]$ με $a > b$ αφού τότε $[(a,b)] = [(a-b,0)]$.

Παρατηρούμε ότι το 0 στο σύνολο των ακεραίων είναι η κλάση $[(0,0)]$,ενώ το $-n$ λοιπόν για $n \in \mathbb{N}$ είναι η κλάση $[(0,n)]$. Πράγματι, παρατηρούμε ότι $[(n,0)] + [(0,n)] = [(n,n)] = [(0,0)]$. Ομοίως το $-[(a,b)] = [(b,a)]$. Οπότε οι αρνητικοί αριθμοί είναι οι κλάσεις $[(a,b)]$ με $a < b$ αφού τότε $[(a,b)] = [(0,b-a)]$. Ορίζουμε $-[(a,b)] = [(b,a)]$.

Μπορούμε να ορίσουμε τώρα πολλαπλασιασμό στο $\mathbb{Z}$ με βάση τον πολλαπλασιασμό των φυσικών ως εξής

$$a \cdot b = \begin{cases} a.b & \text{αν } a,b \geq 0 \text{ ή } a,b < 0 \\ -a.b & \text{διαφορετικά .} \end{cases}$$

Το σύνολο $\mathbb{Z}$ με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού ικανοποιεί τις παρακάτω ιδιότητες

- Για κάθε $x,y,z \in \mathbb{Z}$ ισχύει $x + (y+z) = (x+y) + z$,
- Για κάθε $x,y \in \mathbb{Z}$, ισχύει $x + y = y + z$,
- Το $0 \in \mathbb{Z}$, ικανοποιεί $x + 0 = x$.
- Για κάθε $x \in \mathbb{Z}$, υπάρχει μοναδικά ορισμένο $-x$ ώστε $x + (-x) = 0$.
- Για κάθε $x,y,z \in \mathbb{Z}$, ισχύει $x(yz) = (xy)z$.
- Για κάθε $x,y \in \mathbb{Z}$, ισχύει $xy = yx$.
- Το $1 \in \mathbb{Z}$ ικανοποιεί $1x = x$.

Θα δούμε αργότερα ότι ένα σύνολο εφοδιασμένο με δύο πράξεις πρόσθεσης και πολλαπλασιασμού που ικανοποιεί τις παραπάνω σχέσεις λέγεται αντιμεταθετικός δακτύλιος με μονάδα.

Επιπλέον στο σύνολο $\mathbb{Z}$ ισχύει ότι

$$xy = 0 \Leftrightarrow x = 0 \text{ ή } y = 0.$$

Στο σύνολο $\mathbb{Z}$, αναζητούμε μία λύση της εξίσωσης

$$ax = b, \quad a,b \in \mathbb{Z}. \tag{I.3}$$

Στην περίπτωση που η παραπάνω εξίσωση έχει μία λύση $x \in \mathbb{Z}$, θα λέμε ότι το b διαιρεί το a και θα γράφουμε $b|a$.

Είναι σαφές ότι η εξίσωση (I.3) δεν έχει πάντα λύση, για παράδειγμα για $a = 2, b = 1$, δεν υπαρχεί $x \in \mathbb{Z}$ ώστε $2x = 1$. Πράγματι, ένα τέτοιο x θα έπρεπε να είναι θετικό και τότε $2x > 2 > 1$.

Ορισμός Ι.6.3. Θα συμβολίζουμε με $n!$ το γινόμενο των φυσικών αριθμών που είναι μικρότεροι ή ίσοι με το n, δηλαδή

$$n! := 1 \cdot 2 \cdot 3 \cdots n.$$

Ι.6.2 Επαγωγή

Για κάθε φυσικό αριθμό $n \in \mathbb{N}$ ορίζεται ο «επόμενος» φυσικός $n+1$. Όταν κατασκευάσουμε το σύνολο των ρητών αριθμών θα δούμε ότι κάτι τέτοιο δεν είναι σωστό για τους ρητούς, δεν υπάρχει δηλαδή ένα ελάχιστο «βήμα» που να το προσθέσουμε σε ένα ρητό και να πάρουμε τον «επόμενο» ρητό.

Η ιδιότητα αυτή μας επιτρέπει να αποδεικνύουμε προτάσεις για το σύνολο των φυσικών αριθμών. Έχουμε μία ιδιότητα η οποία εξαρτάται από ένα φυσικό αριθμό n. Δηλαδή έχουμε μια ακολουθία προτάσεων μία για κάθε φυσικό αριθμό $n \in \mathbb{N}$.

Για παράδειγμα έχουμε την πρόταση

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ για κάθε } n \in \mathbb{N}. \tag{I.4}$$

Αυτό που εννοούμε στην παραπάνω πρόταση είναι ότι για οποιοδήποτε φυσικό $n \in \mathbb{N}$ το άθροισμα των n πρώτων φυσικών δίνεται από τον τύπο $\frac{n(n+1}{2}$. Δηλαδή έχουμε

$$\begin{array}{lll} n = 1, & 1 & \frac{1(1+1)}{2} = 1 \\ n = 2, & 1 + 2 = 3 & \frac{2\cdot 3}{2} = 3 \\ n = 3, & 1 + 2 + 3 = 6 & \frac{3\cdot 4}{2} = 6 \\ n = 4, & 1 + 2 + 3 + 4 = 10 & \frac{4\cdot 5}{2} = 10 \\ \vdots & \vdots & \vdots \end{array}$$

Μπορούμε να πιστοποιήσουμε την αλήθεια της εξίσωσης (I.4) για όσους φυσικούς αριθμούς θέλουμε αλλά για όσους φυσικούς αντέξουμε να δοκιμάσουμε πάντα θα έχουμε αφήσει έξω τους υπόλοιπους φυσικούς που είναι άπειροι.

Για να δώσουμε μία απόδειξη για όλους τους φυσικούς η ιδέα είναι να αποδείξουμε την αλήθεια της ιδιότητας $p(n+1)$ κάνοντας χρήση της προηγούμενης $p(n)$. Δηλαδή αν δείξουμε ότι η αλήθεια της πρότασης $p(n)$ έχει σαν συνέπεια την αλήθεια της πρότασης $p(n+1)$ και πιστοποιήσουμε την αλήθεια της $p(1)$ τότε έχουμε ότι: Η πρόταση $p(1)$ είναι αληθής άρα και η πρόταση $p(2)$ είναι αληθής άρα και η πρόταση $p(3)$ είναι αληθής άρα και η πρόταση $p(3)$ είναι αληθής και με αυτό τον τρόπο εξαντλούμε το σύνολο των φυσικών αριθμών.

Ας δούμε πως μπορούμε να χρησημοποιήσουμε αυτή την κατασκευή για να αποδείξουμε την ιδιότητα (I.4) για όλους τους φυσικούς. Η $p(1)$ είναι αληθής αφού $1 = 1 \cdot 2/2$. Υποθέτουμε ότι για ένα $k \in \mathbb{N}$ η πρόταση $p(k)$ είναι αληθής, δηλαδή ότι

$$1 + 2 + 3 + \cdot + k = \frac{k(k+1)}{2}.$$

Θα δείξουμε ότι είναι αληθής η πρόταση και για $k+1$, χρησημοποιώντας τον τύπο του αθροίσματος για τους πρώτους k φυσικούς. Έχουμε

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

δηλαδή η πρόταση που θέλαμε να αποδείξουμε.

Η ακριβής διατύπωση του αξιώματος της επαγωγής είναι η παρακάτω

Αξίωμα I.6.4. *Έστω ένα σύνολο $S \subset \mathbb{N}$ το οποίο ικανοποιεί:*

1. $1 \in S$
2. $n \in S \Rightarrow n + 1 \in S$.

Τότε $S = \mathbb{N}$

Τέλος παραθέτουμε την επόμενη πρόταση η οποία μπορούμε να αποδείξουμε ότι είναι ισοδύναμη με το αξίωμα της επαγωγής

Αξίωμα I.6.5. *Κάθε μη κενό υποσύνολο φυσικών έχει ελάχιστο στοιχείο.*

Πρόταση Ι.6.6. *Το αξίωμα της επαγωγής είναι ισοδύναμο με το αξίωμα Ι.6.5.*

Απόδειξη. Θα αποδείξουμε την ιδιότητα του ελαχίστου στοιχείου με βάση το αξίωμα της επαγωγής. Θεωρούμε ένα μη κενό σύνολο φυσικών αριθμών S. Υποθέτουμε ότι το σύνολο S δεν έχει ελάχιστο στοιχείο. Θεωρούμε το σύνολο A που αποτελείται από τους φυσικούς που είναι μικρότεροι από όλα τα στοιχεία του S δηλαδή

$$k \in A \Leftrightarrow \text{ για κάθε } s \in S\, k < s.$$

Παρατηρούμε ότι $1 \in A$, διαφορετικά θα ήταν ελάχιστο στοιχείο του S. Έστω ότι $n \in A$, τότε για κάθε $s \in S$ έχουμε $n < s$. Από την υπόθεση ότι το S δεν έχει ελάχιστο στοιχείο έχουμε ότι $n+1 \notin S$. Γιατί διαφορετικά το $n+1$ θα ήταν το ελάχιστο του S (γιατί?) Σε αυτή την περίπτωση όμως βλέπουμε ότι $n+1 \in A$ και από το αξίωμα της επαγωγής έχουμε ότι $A = \mathbb{N}$ οπότε $S = \varnothing$, άτοπο.

Αντιστρόφως θα δείξουμε ότι το αξίωμα του ελαχίστου στοιχείου έχει ως συνέπεια το αξίωμα της επαγωγής. Ας υποθέσουμε ότι έχουμε ένα σύνολο S το οποίο ικανοποιεί τις δύο προϋποθέσεις του αξιώματος Ι.6.4. Ας υποθέσουμε ότι $\mathbb{N} \neq S$ άρα το σύνολο $\mathbb{N}\backslash S$ δεν είναι κενό. Από το αξίωμα του ελαχίστου έχουμε ότι το σύνολο $\mathbb{N}\backslash S$ έχει ελάχιστο στοιχείο έστω m_0. Αφού $1 \in S$ έχουμε ότι $m_0 > 1$, άρα υπάρχει $m > 0$ ώστε $m_0 = 1 + m$, με $m \in \mathbb{N}$. Το στοιχείο $m \in S$, γιατί διαφορετικά θα ήταν το ελάχιστο στοιχείο του $\mathbb{N}\backslash S$. Όμως η δεύτερη συνθήκη του αξιώματος της επιλογής δίνει ότι $m+1 = m_0 \in S$, άτοπο. □

Πολύ συχνά είναι χρήσιμη και η εξής μορφή της επαγωγής η οποία μοιάζει ισχυρότερη:

Πρόταση Ι.6.7. *Θεωρούμε ένα σύνολο $S \subset \mathbb{N}$ το οποίο ικανοποιεί:*

1. $1 \in S$
2. *Για κάθε* $n \in \mathbb{N}$
$$(\{1,2,3,\ldots,n\} \subset S) \Rightarrow n+1 \in S.$$

Τότε $S = \mathbb{N}$.

Απόδειξη. Για να δείξουμε ότι η δεύτερη μορφή της επαγωγής είναι ισοδύναμη με την πρώτη θα δείξουμε ότι είναι και αυτή ισοδύναμη με το αξίωμα του ελαχίστου στοιχείου.

Ας υποθέσουμε ότι ισχύει η δεύτερη μορφή της επαγωγής και βάσει αυτής θα δείξουμε ότι ισχύει το αξίωμα του ελαχίστου στοιχείου. Πράγματι, έστω $S \subset \mathbb{N}$ και ας υποθέσουμε ότι δεν έχει ελάχιστο στοιχείο. Θέτουμε $A = \mathbb{N}\backslash S$ και έχουμε $1 \in A$ γιατί διαφορετικά θα ήταν ελάχιστο στοιχείο του S.

$$\{1,2,\ldots,n\} \subset A \Rightarrow n+1 \subset ,$$

γιατί διαφορετικά το $n+1$ θα ήταν ελάχιστο στοιχείο. Άρα η δεύτερη μορφή της επαγωγής δίνει ότι $A = \mathbb{N}$, συνεπώς $S = \varnothing$. Αντιστρόφως, έστω ότι ισχύει το αξίωμα του ελαχίστου στοιχείου θα δείξουμε ότι ισχύει η δεύτερη αρχή της επαγωγής. Έστω $S \subset \mathbb{N}$ και ικανοποιεί της δύο ιδιότητες της δεύτερης μορφής της επαγωγής. Αν $S \neq \mathbb{N}$ τότε το $\mathbb{N}\backslash S \neq \varnothing$ και συνεπώς έχει ελάχιστο στοιχείο m_0. Αφού $1 \in S$ έχουμε ότι $m_0 > 1$. Αφού όμως το m_0 είναι ελάχιστο έχουμε ότι $\{1,2,\ldots,m_0-1\} \subset S$ άρα $m_0 \in S$, άτοπο. □

Ασκήσεις

Άσκηση I.6 Να αποδείξετε ότι για κάθε $n \in \mathbb{N}$ ισχύει

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Άσκηση I.7 Αποδείξτε ότι για κάθε $n \in \mathbb{N}$

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n! = (n+1)! - 1.$$

Άσκηση I.8 Για δύο φυσικούς αριθμούς n, m, $n \geq m$ ορίζουμε το σύμβολο $\binom{n}{m} := \frac{n!}{m!(n-m)!}$. Αποδείξτε ότι $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. Στην συνέχεια δείξτε ότι οι δυονιμικοί συντελεστές μπορούν να υπολογιστούν με την βοήθεια του τριγώνου του Pascal:

$$\begin{array}{ccccc} 1 & & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{array} .$$

Ο τρόπος με τον οποίο σχηματίσαμε το τρίγωνο του Pascal είναι να υπολογίζουμε τους συντελεστές της κάθε γραμμής ως το άθροισμα των δύο προηγουμένων.

Ο πρώτος τύπος μπορεί να υπολογιστεί κάνοντας πράξεις. Η κατασκευή του τριγώνου του Pascal προκύπτει από τον προηγούμενο τύπο.

Άσκηση I.9 Αποδείξτε ότι για κάθε φυσικό αριθμό n

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}.$$

Στην συνέχεια δικαιολογείστε γιατί το $\binom{n}{m}$ είναι φυσικός.

Χρησιμοποιήστε επαγωγή. Θα χρειαστεί να χρησημοποιήσετε το $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ της προηγούμενης άσκησης.

Άσκηση I.10 Αποδείξτε ότι για όλους τους φυσικούς ισχύει:

$$1^2 - 2^2 + 3^2 - 4^2 + \ldots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1}{2}.$$

Άσκηση I.11 Θεωρήστε μία συνάρτηση $f : \mathbb{N} \to \mathbb{N}$. Δείξτε ότι αν η f είναι αύξουσα τότε $f(n) \geq n$

I.6.3 Κατασκευή των ρητών

Στην παράγραφο αυτή θα κατασκευάσουμε το σύνολο $\mathbb{Q}$, των ρητών αριθμών.

Ορίζουμε το σύνολο

$$A = \mathbb{Z} \times \mathbb{Z} \backslash \{0\},$$

δηλαδή το σύνολο των διατεταγμένων ζευγαριών (a, b) με $a \in \mathbb{Z}, b \in \mathbb{Z}\backslash\{0\}$.

Στο σύνολο αυτό ορίζουμε μια σχέση ισοδυναμίας

$$(a, b) \equiv (a', b') \Leftrightarrow ab' - ba' = 0.$$

Το ότι η παραπάνω σχέση αποτελεί σχέση ισοδυναμίας το είδαμε στην άσκηση I.5 του πρώτου κεφαλαίου.

Ορισμός Ι.6.8. Το σύνολο $\mathbb{Q}$ είναι το σύνολο πηλίκο $(\mathbb{Z}\times\mathbb{Z}\backslash\{0\})/\sim$.

Το σύνολο $\mathbb{Q}$ θα το ορίσουμε να είναι το σύνολο πηλίκο της παραπάνω σχέσης ισοδυναμίας, δηλαδή το σύνολο των κλάσεων ισοδυναμίας.

Θα πρέπει να δείξουμε ότι το σύνολο $\mathbb{Q}$ περιέχει το σύνολο $\mathbb{Z}$ και ότι κάθε στοιχείο $x\in\mathbb{Q}$, $x\neq 0$ έχει αντίστροφο.

Καταρχάς ας ορίσουμε πρόσθεση και πολλαπλασιασμό στο σύνολο $\mathbb{Q}$.

$$(a,b)+(a',b')=(ab'+a'b,bb'),(a,b)(a',b')=(aa',bb').$$

Προκειμένου να δείξουμε ότι οι πράξεις είναι καλά ορισμένες θα πρέπει να δείξουμε ότι είναι ανεξάρτητες του αντιπροσώπου. Δηλαδή αν $(a,b)\cong(a_1,b_1)$ και $(a',b')\cong(a'_1,b'_1)$, θα πρέπει να δείξουμε ότι

$$(a,b)+(a',b')\cong(a_1,b_1)+(a'_1,b'_1),$$

και

$$(a,b)(a',b')\cong(a_1,b_1)(a'_1,b'_1).$$

Θα αφήσουμε την απόδειξη του καλά ορισμένου των πράξεων ως άσκηση.

Παρατηρούμε ότι το σύνολο $\mathbb{Z}$ μπορεί να θεωρηθεί σαν υποσύνολο του $\mathbb{Q}$, ταυτίζοντας το $n\in\mathbb{Z}$ με την κλάση ισοδυναμίας του $(n,1)$ στο $\mathbb{Q}$. Επιπλέον παρατηρούμε ότι οι πράξεις στο $\mathbb{Q}$ περιοριζόμενες στο $\mathbb{Z}$, δίνουν τις συνηθισμένες πράξεις στους ακαίρεους.

Ο συνηθισμένος συμβολισμός για την κλάση ισοδυναμίας του (a,b) στο $\mathbb{Q}$ είναι a/b.

Ι.6.4 Το σύνολο των πραγματικών αριθμών

Η ανάγκη κατασκευής των πραγματικών αριθμών δεν ήταν αλγεβρική. Οι πραγματικοί αριθμοί κατασκευάστηκαν προκειμένου να ικανοποιηθεί το λεγόμενο *αξίωμα της πληρότητας* δηλαδή

Αξίωμα Ι.6.9. *Κάθε άνω φραγμένο σύνολο έχει supremum.*

Η έννοια του supremum ή ελάχιστου άνω φράγματος ορίζεται ως εξής:

Ορισμός Ι.6.10. Για ένα υποσύνολο S ενός διατεταγμένου συνόλου $(P,\leq)$ ένα άνω φράγμα είναι ένα στοιχείο b ώστε $s\leq b$ για κάθε $s\in S$. Το ελάχιστο άνω φράγμα ή supremum του S είναι ένα άνω φράγμα s το οποίο να ικανοποιεί $s\leq b$ για κάθε άλλο άνω φράγμα b του S.

Με παρόμοιο τρόπο ορίζεται το κάτω φράγμα και το μέγιστο κάτω φράγμα ή infimum.

Παρατηρούμε ότι το υποσύνολο

$$A=\{x\in\mathbb{Q}:x^2<2\},$$

των ρητών αριθμών είναι άνω φραγμένο από το 2. Το supremum του παραπάνω συνόλου θα είναι η τετραγωνική ρίζα του 2. Πράγματι αν $a\in\mathbb{R}$, ώστε a άνω φράγμα του A τότε $x\leq a$ για κάθε $x\in A$ και συνεπώς $x^2\leq a^2$, το μικρότερο τετράγωνο που φράσει από πάνω το x^2 είναι το $\sqrt{2}$.

Αριθμοί που δεν είναι ρητοί

Θα συμβολίζουμε με $\sqrt{2}$ τον θετικό πραγματικό αριθμό ο οποίος όταν υψωθεί στο τετράγωνο δίνει 2. Σε ένα σώμα που ισχύει το αξίωμα της πληρότητας υπάρχει και είναι ίσος με το supremum του παραπάνω συνόλου. Γεωμετρικά ένας τέτοιος αριθμός αντιστοιχεί στην υποτείνουσα ορθογωνίου τριγώνου με κάθετες πλευρές ίσες με την μονάδα.

Πρόταση I.6.11. *Ο αριθμός $\sqrt{2}$ δεν είναι ρητός.*

Απόδειξη. Ας υποθέσουμε ότι ο αριθμός $\sqrt{2}$ μπορεί να γραφεί σαν κλάσμα m/n, όπου $m, n \in \mathbb{N}$, $n \neq 0$. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι το κλάσμα m/n είναι ανάγωγο, δηλαδή ότι τα m, n δεν έχουν κοινό διαιρέτη. Θα καταλήξουμε σε άτοπο. Παρατηρούμε ότι

$$\sqrt{2} = \frac{m}{n} \Rightarrow 2n^2 = m^2, \tag{I.6}$$

δηλαδή το τετράγωνο του m είναι άρτιος. Αυτό έχει σαν άμεση συνέπεια ότι και ο m είναι άρτιος, διότι διαφορετικά, αν δηλαδή ο m ήταν περιττός, αν δηλαδή $m = 2k+1$ για κάποιο φυσικό αριθμό k, τότε $m^2 = 4k^2 + 4k + 1$ θα ήταν επίσης περιττός. Άρα $m = 2k$ για κάποιο k και συνεπώς $m^2 = 4k^2$. Αντικαθιστούμε στην (I.6) οπότε έχουμε ότι $2n^2 = 4k^2 \Rightarrow n^2 = 2k^2$, άρα και ο n^2 είναι άρτιος και συνεπώς και ο n είναι άρτιος. Σε αυτή την περίπτωση όμως το κλάσμα m/n δεν μπορεί να είναι ανάγωγο και άρα έχουμε καταλήξει σε άτοπο, δηλαδή ο αριθμός $\sqrt{2}$ είναι άρρητος. □

I.6.5 Κατασκευή των Πραγματικών Αριθμών

Στην ενότητα αυτή θα προσπαθήσουμε να σκιαγραφήσουμε την κατασκευή του συνόλου των πραγματικών αριθμών ακολουθώντας τις ιδέες του Dedekind. Αργότερα θα δώσουμε και άλλη μία εναλλακτική κατασκευή βασισμένη στις ακολουθίες Cauchy.

Ορισμός I.6.12. Ένα υποσύνολο $A \subset \mathbb{Q}$ θα λέγεται αρχικό τμήμα του $\mathbb{Q}$ αν ικανοποιεί:

$$\text{Αν } p \in A \text{ και } q < p \text{ τότε } q \in A.$$

Δηλαδή αν το αρχικό τμήμα περιέχει ένα ρητό αριθμό τότε περιέχει και όλους τους μικρότερούς του. Το A θα λέγεται ανοιχτό αρχικό τμήμα του $\mathbb{Q}$ αν δεν έχει μέγιστο στοιχείο.

Επιπλέον ορίζουμε το (αντ. ανοιχτό) τελικό τμήμα του $\mathbb{Q}$ να είναι το συμπλήρωμα ενός (αντ. ανοιχτού) αρχικού τμήματος του $\mathbb{Q}$.

Ορισμός I.6.13. Το σύνολο όλων των αρχικών ανοιχτών τμημάτων του $\mathbb{Q}$ είναι το σύνολο των πραγματικών αριθμών.

Ο παραπάνω ορισμός αφήνει πολλά ερωτήματα. Καταρχάς θα πρέπει να καταλάβουμε πως μπορούμε να θεωρήσουμε τους ρητούς αριθμούς ως υποσύνολο των πραγματικών αριθμών. Αυτό δεν είναι ιδιαίτερα δύσκολο: Οι ρητοί αποτελούνται από τα αρχικά τμήματα της μορφής:

$$A_q := \{x \in \mathbb{Q} : x < q\},$$

με $q \in \mathbb{Q}$. Παρατηρούμε ότι η συνάρτηση

$$\mathbb{Q} \to \mathbb{R}$$

$$q \mapsto A_q$$

είναι μία συνάρτηση ένα προς ένα (γιατί?)

Το επόμενο θέμα είναι πως θα ορίσουμε πράξεις στους πραγματικούς αριθμούς. Αν έχουμε δύο πραγματικούς αριθμούς, δηλαδή δύο αρχικά τμήματα A, B του $\mathbb{Q}$ τότε ορίζουμε σαν άθροισμα τους το σύνολο

$$+ := \{a + b : a \in A, b \in B\}$$

και σα γινόμενό τους το σύνολο

$$A \cdot B := \{ab : a \in A, b \in B\}.$$

Θα πρέπει να δείξουμε ότι οι παραπάνω πράξεις είναι καλά ορισμένες, δηλαδή ότι τα $A+B, A \cdot B$ είναι όντως ανοιχτά αρχικά τμήματα του $\mathbb{Q}$.

Για παράδειγμα αν $x \in A+B$ τότε εξ ορισμού $x = a+b$, με $a \in A$ και $b \in B$. Αν λοιπόν $\mathbb{Q} \ni y < x$ τότε $y - a < b$, άρα $y - a \in B$ οπότε εξ ορισμού του $A+B$, έχουμε ότι $y = a + (y-a) \in A+B$. Με παρόμοιο τρόοπο δείχνουμε ότι και το $A \cdot B$ είναι αρχικό τμήμα του $\mathbb{Q}$.

Θα πρέπει να δείξουμε ότι οι παραπάνω ορισμένες πράξεις έχουν όλες τις αναμενόμενες ιδιότητες των πράξεων όπως προσεταιριστική, ύπαρξη αντίστροφου, ουδετέρου κτλ. Δεν θα επεκταθούμε περισσότερο στον έλεγχο αυτό, θα αρκεστούμε στο να παρατηρήσουμε ότι όλες οι αναμενόμενες πράξεις, ανάγονται στις αντίστοιχες ιδιότητες πράξεων των ρητών.

Τέλος θα λέμε ότι $A \leq B$ αν και μόνο αν $A \subset B$. Γνωρίζουμε ότι ο εγκλεισμός συνόλων δίνει μία σχέση διάταξης. Ο προσεκτικός αναγνώστης θα πρέπει να δείξει ότι η σχέση αυτή διάταξης είναι συμβατή με τις πράξεις.

Παράδειγμα Ι.6.14. Ο $\sqrt{2}$ που δείξαμε ότι δεν είναι ρητός, είναι το σύνολο

$$A := \{x \in \mathbb{Q} : x < 0\} \cup \{x \in \mathbb{Q} : x^2 < 2\}.$$

Πράγματι, το σύνολο A είναι ένα αρχικό τμήμα αφού αν $x \in A$ και $y < x$ τότε αν $x < 0$ τότε προφανώς $y \in A$ αφού $y < x < 0$. Αν πάλι $0 \leq y < x$ τότε αν $y < x$ έχουμε και $y^2 < x^2 < 2$ οπότε $y \in A$ ενώ αν $y < 0$ πάλι εξ ορισμού $y \in A$. Τέλος παρατηρούμε ότι

$$A \cdot A = \{x \in \mathbb{Q} : x < 2\},$$

δηλαδή το τετράγωνο του A είναι το αρχικό τμήμα που έχουμε ταυτίσει με τον ρητό αριθμό 2. Θα αποδείξουμε πρώτα ότι $A \cdot A \subset \{x \in \mathbb{Q} : x < 2\}$. Πράγματι, αν $0 < x \in A \cdot A$, τότε υπάρχουν $a, b \in A$ ώστε $x = ab$ και $a^2 < 2$, $b^2 < 2$ συνεπώς $x^2 = aabb < 4$ άρα $x < 2$. Η περίπτωση $x < 0$ είναι προφανής.

Αντιστρόφως θα πρέπει να δείξουμε ότι $\{x \in \mathbb{Q} : x < 2\} \subset A \cdot A$. Έστω $y \in \{y \in \mathbb{Q} : y < 2\}$, θεωρούμε το ανοιχτό τμήμα $A_{y/2} := \{c \in \mathbb{Q} : c^2 < y/2\}$. Παρατηρούμε ότι $y/2 < 2$ συνεπώς $A_{y/2} < A$ (γιατί?) άρα $A^C_{y/2} \cap A \neq \varnothing$. Συνεπώς υπάρχει $a \in \mathbb{Q}$ ώστε $y^2/2 < a^2 < 2$, και $y/a := b \in A$. Άρα καταφέραμε να γράψουμε το y ως γινόμενο στοιχείων του A.

Θεώρημα Ι.6.15. *Κάθε άνω φραγμένο υποσύνολο του $\mathbb{R}$ έχει supremum.*

Απόδειξη. Θεωρούμε ένα σύνολο πραγματικών αριθμών A, το οποίο είναι άνω φραγμένο. Εξ ορισμού των πραγματικών αριθμών κατά Dedekind, το σύνολο A, έχει σαν στοιχεία του αρχικά ανοιχτά τμήματα του $\mathbb{Q}$, το ότι είναι άνω φραγμένο σημαίνει ότι υπάρχει ένα αρχικό ανοιχτό τμήμα του $\mathbb{Q}$, M, το οποίο περιέχει κάθε ανοιχτό αρχικό τμήμα $x \in A$. Παρατηρούμε ότι το σύνολο $\cup_{x \in A} x \subset M$ δεν ταυτίζεται με το $\mathbb{Q}$ και είναι ένα ανοιχτό αρχικό τμήμα του $\mathbb{Q}$ το οποίο περιέχει κάθε άνω φράγμα του A, είναι δηλαδή το supremum του συνόλου A. □

Για τους πραγματικούς αριθμούς ισχύει η αρχή του *Αρχιμήδη*

Πρόταση Ι.6.16. *Από κάθε πραγματικό αριθμό x υπάρχει φυσικός αριθμός $n \in \mathbb{N}$ ώστε $x \leq n$.*

Απόδειξη. Ας υποθέσουμε ότι ο πραγματικός αριθμός $x \in \mathbb{R}$ παρίσταται με το αρχικό τμήμα A. Η αρχή του Αρχιμήδη είναι ισοδύναμη με το ότι υπάρχει φυσικός αριθμός $n \in \mathbb{N}$ ώστε το σύνολο $A_n = \{a \in \mathbb{Q} : a < n\}$ περιέχει το A. Αν το τελευταίο δεν ήταν αληθές τότε το $A = \mathbb{Q}$ από τις ιδιότητες διάταξης στους ρητούς. □

Ορισμός I.6.17. Μια ακολουθία είναι μία συνάρτηση από το σύνολο των φυσικών αριθμών $\mathbb{N}$ στο σύνολο των πραγματικών αριθμών $\mathbb{R}$. Θα συμβολίζουμε με a_n την τιμή της συνάρτησης (ακολουθίας) στο $n \in \mathbb{N}$.

Θα λέμε ότι η ακολουθία (a_n) συγκλίνει στον πραγματικό αριθμό ℓ αν και μόνο αν

$$\text{Για κάθε } \epsilon > 0, \text{ υπάρχει φυσικός αριθμός } n_0(\epsilon) \text{ ώστε αν } n > n_0 \text{ τότε } |a_n - \ell| < \epsilon.$$

Στην περίπτωση που η ακολουθία συγκλίνει στον πραγματικό ℓ, θα γράφουμε $\lim a_n = \ell$ ή $a_n \to \ell$.

Ορίσαμε σε προηγούμενο κεφάλαιο τους πραγματικούς αριθμούς με τέτοιο τρόπο ώστε να ικανοποιούν το αξίωμα της πληρότητας, δηλαδή κάθε φραγμένο υποσύνολο να έχει supremum.

Ορισμός I.6.18. Μία ακολουθία (a_n) είναι Cauchy αν και μόνο αν

$$\text{Για κάθε } \epsilon > 0, \text{ υπάρχει φυσικός αριθμός } n_0(\epsilon) \text{ ώστε } n, m > n_0 \Rightarrow |a_n - a_m| < \epsilon.$$

Ο **Augustin-Louis Cauchy** (21 Αυγούστου 1789 – 23 Μαΐου 1857) ήταν Γάλλος Μαθηματικός, Φυσικός και μηχανικός. Ήταν πρωτοπόρος στην αυστηρή απόδειξη θεωρημάτων του απειροστικού λογισμού και επίσης είχε σημαντική συνεισφορά στην μελέτη των ομάδων μεταθέσεων στην κυματική θεωρία, στην θεωρία της ελαστικότητας αλλά και στις μιγαδικές συναρτήσεις. Περισσότερο συγκεκριμένα πέρα από τις ακολουθίες που έχουν το όνομα του και περιγράφουμε σε αυτό το κεφάλαιο, οι εξισώσεις Cauchy-Riemann αλλά και ο ολοκληρωτικός τύπος του στις μιγαδικές συναρτήσεις είναι στον πυρήνα της θεωρίας όπως διδάσκεται σήμερα και άνοιξε νέους δρόμους στην τοπολογία και στην αλγεβρική Γεωμετρία. Στην θεωρία ομάδων είναι γνωστό το θεώρημα του Cauchy για ύπαρξη υποομάδων τάξης p για κάθε διαιρέτη της τάξης της ομάδας το οποίο είναι ένας πρόδρομος των θεωρημάτων Sylow.

Το συνολικό του έργο αριθμεί 789 εργασίες και τα άπαντα του συνολικά καταλαμβάνουν 27 τόμους. Το όνομα του είναι μεταξύ των 72 ονομάτων που έχουν εγγραφεί στον πύργο του Eiffel [a]

[a] https://en.wikipedia.org/wiki/List_of_the_72_names_on_the_Eiffel_Tower.

Είναι σαφές ότι αν μία ακολουθία συγκλίνει στον πραγματικό αριθμό ℓ αφού οι όροι πλησιάζουν στο ℓ θα πλησιάζουν και μεταξύ τους. Δηλαδή

Πρόταση I.6.19. *Κάθε συγκλίνουσα ακολουθία με όριο τον πραγματικό αριθμό ℓ είναι Cauchy.*

Απόδειξη. Ξεκινάμε από τον ορισμό της συγκίνουσας ακολουθίας στον πραγματικό αριθμό ℓ, όπου αντί για $\epsilon > 0$ έχουμε πάρει $\epsilon/2 > 0$.

$$\text{Για κάθε } \epsilon/2 > 0, \text{ υπάρχει φυσικός αριθμός } n_0(\epsilon) \text{ ώστε } n > n_0 \Rightarrow |a_n - \ell| < \epsilon.$$

Η τριγωνική ανισότητα μας εξασφαλίζει ότι για $n, m > n_0$

$$|a_n - a_m| = |a_n - \ell + \ell - a_m| \leq |a_n - \ell| + |a_m - \ell| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

δηλαδή το ζητούμενο. □

Είναι οι ακολουθίες Cauchy συγκλίνουσες; Ας δούμε πρώτα ένα παράδειγμα, θεωρούμε τον αριθμό $\sqrt{2}$. Αποδείξαμε σε προηγούμενο κεφάλαιο ότι είναι άρρητος. Η ακολουθία των δεκαδικών προσεγγίσεων του που ορίζεται ως:

$$a_n = \frac{[10^n\sqrt{2}]}{10^n},$$

δηλαδή

a_1	a_2	a_3	a_4	a_5	$\cdots$
1.4	1.41	1.414	1.4142	1.41421	$\cdots$

είναι μία ακολουθία (a_n) με όρους στο $\mathbb{Q}$, η οποία συγκλίνει στον $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$. Βλέπουμε λοιπόν ότι μία ακολουθία Cauchy από το $\mathbb{Q}$ δεν έχει όριο κατ' ανάγκη στο $\mathbb{Q}$. Μπορούμε να κατασκευάσουμε όπως θα δούμε στην συνέχεια τους πραγματικούς αριθμους από το $\mathbb{Q}$, επισυνάπτοντας στους ρητούς όλα τα όρια ακολουθιών από το $\mathbb{Q}$.

Λήμμα Ι.6.20. *Οι ακολουθίες Cauchy είναι φραγμένες.*

Απόδειξη. Για να αποδείξουμε ότι κάθε ακολουθία Cauchy είναι φραγμένη. θέτουμε $\epsilon = 1$ στον ορισμό της ακολουθίας Cauchy, οπότε έχουμε ότι υπάρχει n_0 ώστε για κάθε $n, m > n_0$ $|a_n - a_m| < 1$. Σταθεροποιούμε το $m = n_0 + 1$, και έχουμε ότι

$$|a_n - a_{n_0+1}| < 1 \Leftrightarrow a_{n_0+1} - 1 < a_n < a_{n_0+1} + 1,$$

για κάθε $n > n_0$. Αρκεί λοιπόν να πάρουμε

$$m = \min\{a_1, \ldots, a_{n_0}, a_{n_0+1} - 1\}$$

$$M = \max\{a_1, \ldots, a_{n_0}, a_{n_0+1} + 1\},$$

για να έχουμε

$$m < a_n < M \quad \text{για κάθε } n \in \mathbb{N}.$$

□

Λήμμα Ι.6.21. *Αν ισχύει το αξίωμα της πληρότητας τότε κάθε αύξουσα και άνω φραγμένη ακολουθία (a_k) συγκλίνει στο $\sup_{k\in\mathbb{N}} a_k$. Επίσης κάθε φθίνουσα και κάτω φραγμένη ακολουθία συγκλίνει στο $\inf_{k\in\mathbb{N}} a_k$.*

Απόδειξη. Θεωρούμε την ακολουθία (a_n) η οποία είναι άνω φραγμένη και συνεπώς έχει supremum $c = \sup_{k\in\mathbb{N}}$. Συνεπώς για κάθε $\epsilon > 0$ το $c - \epsilon < c$ δεν μπορεί να είναι άνω φράγμα, άρα υπάρχει $n_0(\epsilon)$ ώστε $c - \epsilon < a_{n_0(\epsilon)}$. Λόγω της μονοτονίας της a_n, για κάθε $n \geq n_0(\epsilon)$ έχουμε ότι

$$c - \epsilon < a_n < c,$$

όπου η τελευταία ανισότητα προκύπτει από το ότι το c είναι άνω φράγμα της (a_n). Συνεπώς $a_n \to c$.

Παρατηρούμε ότι αν η (a_k) είναι φθίνουσα και κάτω φραγμένη η $(-a_n)$ είναι αύξουσα και άνω φραγμένη από όπου προκύπτει και το ζητούμενο. □

Θεώρημα I.6.22. *Στο σύνολο των πραγματικών αριθμών το αξίωμα της πληρότητας I.6.9, ότι κάθε άνω φραγμένο σύνολο έχει supremum είναι ισοδύναμο με το ότι κάθε ακολουθία Cauchy συγκλίνει.*

Απόδειξη. Είναι σαφές ότι αν κάθε άνω φραγμένο σύνολο S έχει supremum τότε και κάθε κάτω φραγμένο σύνολο έχει infimum, αρκεί να θεωρήσουμε το σύνολο $-S = \{-s : s \in S\}$. Με την βοήθεια αυτών για μια ακολουθία Cauchy που είναι φραγμένη σύμφωνα με το λήμμα I.6.20 μπορούμε να ορίσουμε τα

$$\limsup a_n = \lim_{k\to\infty} \sup_{n\geq k} a_n = \inf_{k\in\mathbb{N}} \sup_{n\geq k} a_n$$
$$\liminf a_n = \lim_{k\to\infty} \inf_{n\geq k} a_n = \sup_{k\in\mathbb{N}} \inf_{n\geq k} a_n$$

τα οποία υπάρχουν και τα δύο αφού η ακολουθία $\sup_{n\geq k} a_n$ είναι φθίνουσα και η $\inf_{n\geq k} a_n$ είναι αύξουσα. Αν τα δύο παραπάνω όρια είναι ίσα τότε η ακολουθία συγκλίνει. Σε μια ακολουθία Cauchy τα δύο παραπάνω όρια πρέπει να είναι ίσα. Αυτό σημαίνει ότι για κάθε $\epsilon > 0$ υπάρχει n_0, n_1 ώστε αν $k \geq n_0$ τότε $|\sup_{n\geq k} a_n - \ell| \leq \epsilon$ και αν $k \geq n_1$ τότε $|\inf_{n\geq k} a_n - \ell| \leq \epsilon$ από όπου έχουμε ότι για $k > n_0, n_1$

$$\ell - \epsilon < \inf a_k \leq a_k \leq \sup a_k \leq \ell + \epsilon$$

συνεπώς υπάρχει το όριο της (a_k).

Αντιστρόφως αν κάθε ακολουθία Cauchy συγκλίνει θα δείξουμε ότι κάθε άνω φραγμένο σύνολο έχει supremum. Θεωρούμε ένα $\varnothing \neq S \subset \mathbb{R}$ το οποίο είναι άνω φραγμένο. Έστω b_0 ένα άνω φράγμα του S και έστω $a_0 \in S$. Αν το $(a_0 + b_0)/2$ είναι άνω φράγμα ορίζουμε $a_{n+1} := a_n$ και $b_{n+1} = (a_n + b_n)/2$ ενώ διαφορετικά ορίζουμε $a_{n+1} = (a_n + b_n)/2$, $b_{n+1} = b_n$. Με βάση τον παραπάνω ορισμό οι a_n, b_n είναι και οι δύο ακολουθίες Cauchy αφού

$$|a_m - a_n| \leq \frac{1}{2^{|m-n|}}|b_0 - a_0|, \quad |b_m - b_n| \leq \frac{1}{2^{|m-n|}}|b_0 - a_0|.$$

Συνεπώς και οι δύο ακολουθίες συγκλίνουν και μάλιστα στο ίδιο όριο ℓ αφού

$$|b_n - a_n| = \frac{1}{2^n}|b_0 - a_0| \to 0.$$

Το όριο ℓ είναι ένα άνω φράγμα του S αφού όλα τα b_n είναι άνω φράγματα. Επίσης, δεν υπάρχει γνήσια μικρότερο άνω φράγμα btou S από το ℓ αφού κανένα από τα a_n δεν είναι άνω φράγμα, παρατηρήστε ότι αν το b είναι άνω φράγμα τότε όλα τα $c > b$ είναι και αυτά άνω φράγματα. Συνεπώς το όριο ℓ είναι το μικρότερο άνω φράγμα, δηλαδή το supremum. □

Θα δούμε τώρα πώς μπορούμε κάνοντας χρήση ακολουθιών Cauchy $a_n : \mathbb{N} \to \mathbb{Q}$ να ορίσουμε τους πραγματικούς αριθμούς.

Θεωρούμε το σύνολο των ακολουθίων Cauchy $a_n : \mathbb{N} \to \mathbb{Q}$ στο οποίο θεωρούμε την σχέση ισοδυναμίας

$$(a_n) \sim (b_n) \Leftrightarrow a_n - b_n \to 0.$$

Λήμμα I.6.23. *Θεωρούμε το σύνολο A το οποίο περιέχει όλες τις ακολουθίες Cauchy. Η σχέση*

$$(a_n) \sim (b_n) \Leftrightarrow a_n - b_n \to 0,$$

είναι μία σχέση ισοδυναμίας.

Απόδειξη. Για να δείξουμε ότι η σχέση είναι ανακλαστική παρατηρούμε ότι για κάθε ακολουθία (a_n), ισχύει $(a_n) - (a_n) = 0$ οπότε έχουμε ότι $(a_n) \sim (a_n)$.

Για να δείξουμε ότι η σχέση είναι συμμετρική παρατηρούμε ότι

$$(a_n) \sim (b_n) \Rightarrow a_n - b_n \to 0 \Rightarrow b_n - a_n \to 0 \Rightarrow (b_n) \sim (a_n)$$

Τέλος για να δείξουμε ότι η σχέση είναι μεταβατική θεωρούμε τρείς ακολουθίες Cauchy $(a_n), (b_n), (c_n)$ με $(a_n) \sim (b_n)$ και $(b_n) \sim (c_n)$. Εξ'ορισμού $a_n - b_n \to 0$ και $b_n - c_n \to 0$. Άρα

$$a_n - c_n = (a_n - b_n) - (b_n - c_n) \to 0,$$

και τελικά $(a_n) \sim (c_n)$.

Θα πρέπει να ορίσουμε πράξεις ανάμεσα στις παραπάνω κλάσεις ισοδυναμίας. Έστω A το σύνολο πηλίκο της παραπάνω σχέσης ισοδυναμίας, δηλαδή το σύνολο που σαν στοιχεία του έχει τις κλάσεις ισοδυναμίας $[(a_n)]$. θεωρούμε δύο στοιχεία στο σύνολο πηλίκο $[(a_n)]$ και $[(b_n)]$. Ορίζουμε ως άθροισμα των κλάσεων την κλάση του αθροίσματος των αντιπροσώπων. Δηλαδή $[(a_n)] + [(b_n)] = [(a_n) + (b_n)]$. Ομοίως ορίζουμε ως γινόμενο των κλάσεων την κλάση του γινομένου των αντιπροσώπων, δηλαδή $[(a_n)] \cdot [(b_n)] = [(a_n) \cdot (b_n)]$. Θα πρέπει να δείξουμε ότι οι παραπάνω πράξεις είναι καλά ορισμένες, δηλαδή ανεξάρτητες των αντιπροσώπων. Δηλαδή θα πρέπει να αποδειχτεί Θα πρέπει να αποδειχτεί ότι αν $(a_n), (a'_n)$ είναι διαφορετικοί αντιπρόσωποι της κλάσης ισοδυναμίας του $[(a_n)]$ και $(b_n), (b'_n)$ διαφορετικοί αντιπρόσωποι της κλάσης ισοδυναμίας του $[(b_n)]$, τότε τότε η ακολουθία $(a_n + b_n)$ είναι ισοδύναμη με την $(a'_n + b'_n)$ και επίσης η ακολουθία $(a_n \cdot b_n)$ είναι ισοδύναμη με την $(a'_n \cdot b'_n)$.

Αφού $(a_n) \sim (a'_n)$ εξ' ορισμού $a_n - a'_n \to 0$ και ομοίως $b_n - b'_n \to 0$. Άρα

$$((a_n) + (b_n)) - (a'_n + b'_n) = (a_n - a'_n) - (b_n - b'_n) \to 0.$$

Επίσης

$$\begin{aligned} &\lim\big((a_n) \cdot (b_n) - (a'_n) \cdot (b'_n)\big) = \\ &= \lim\big((a_n) \cdot (b_n) - (a'_n) \cdot (b'_n)\big) + \lim(a_n - a'_n) \cdot (b_n) = \\ &= \lim(a_n)\big((b_n) - (b'_n)\big) - \lim(b_n)\big((a'_n) - (a_n)\big) = 0. \end{aligned}$$

□

Το σύνολο των κλάσεων ισοδυναμίας με την παραπάνω σχέση «ταυτίζεται» με τους πραγματικούς αριθμούς!

Η απόδειξη γιατί το παραπάνω σύνολο «ταυτίζεται» με το σύνολο των πραγματικών αριθμών, αν και δεν είναι πολύ δύσκολη προϋποθέτει γνώσεις μερικών βασικών στοιχείων αφηρημένης *άλγεβρας*, κυρίως για να εξηγήσουμε τι εννοούμε ακριβώς γράφοντας «ταυτίζεται» στις παραπάνω προτάσεις.

Ασκήσεις

Άσκηση Ι.12 Ποιά από τα παρακάτω είναι σωστά;

1. Το άθροισμα ρητών αριθμών είναι πάντα ρητός αριθμός.
2. Το άθροισμα ρητού και άρρητου είναι άρρητος.
3. Το άθροισμα δύο άρρητων είναι άρρητος.
4. Το άθροισμα δύο άρρητων είναι πάντα ρητός.
5. Για κάθε $x \in \mathbb{R}$ υπάρχει ακολουθία άρρητων που να συγκλίνει στο x.

6. Για κάθε $x \in \mathbb{R}$ υπάρχει ακολουθία άρρητων που να συγκλίνει στο x.

7. Ανάμεσα σε δύο πραγματικούς υπάρχει άρρητος.

Άσκηση I.13 Αποδείξτε ότι ανάμεσα σε δύο ρητούς υπάρχει ρητός

Άσκηση I.14 Αποδείξτε ότι ανάμεσα σε δύο πραγματικούς υπάρχει ρητός.

Κάνοντας χρήση της αρχής του Αρχιμήδη δείξτε ότι μπορούμε να πολλαπλασιάσουμε τους αριθμούς a, b με κατάλληλο φυσικό n ώστε η απόσταση τους να γίνει μεγαλύτερη της μονάδας.

Άσκηση I.15 Αποδείξτε ότι το γινόμενο δύο θετικών αριθμών είναι θετικός αριθμός.

I.6.6 Το σύνολο των μιγαδικών αριθμών

Στο σύνολο των πραγματικών αριθμών η εξίσωση $x^2 = -1$ δεν έχει λύση, αφού το γινόμενο δύο θετικών αριθμών έχει σαν αποτέλεσμα θετικό αριθμό (Βλέπε άσκηση I.15). Θα προσπαθήσουμε να «διευρύνουμε» το σύνολο των πραγματικών αριθμών και να κατασκευάσουμε ένα νέο σύνολο όπου η εξίσωση $x^2 = -1$ να έχει λύση.

Ορισμός I.6.24. Ορίζουμε το σύνολο των μιγαδικών αριθμών $\mathbb{C}$ να είναι το σύνολο των διατεταγμένων ζευγών (a, b), όπου προσθέτουμε δύο ζεύγη με τον παρακάτω τρόπο:

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

και πολλαπλασιάζουμε δύο ζεύγη ως εξής:

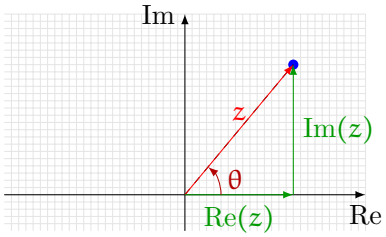
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).$$

Θα πρέπει κανείς τώρα να ελέγξει ότι το παραπάνω σύνολο με τις δύο πράξεις έχει παρόμοιες ιδιότητες με αυτές των πραγματικών αριθμών δηλαδή ότι

- Για κάθε $a, b, c \in \mathbb{C}$, ισχύει $(a + b) + c = a + (b + c)$.
- Για κάθε $a, b \in \mathbb{C}$, ισχύει $a + b = b + a$.
- Υπάρχει στοιχείο $\mathbb{C} \ni \mathbf{0} := (0, 0)$, ώστε για κάθε $a \in \mathbb{C}$, $\mathbf{0} + a = a$.
- Για κάθε $a \in \mathbb{C}$, υπάρχει $-a \in \mathbb{C}$, ώστε $a + (-a) = 0$.
- Για κάθε $a, b \in \mathbb{C}$, ισχύει $ab = ba$.
- Για κάθε $a, b, c \in \mathbb{C}$, ισχύει $a(b + c) = ab + ac$.
- Υπάρχει ένα στοιχείο $\mathbb{C} \ni \mathbf{1} := (1, 0)$, ώστε για κάθε $a \in \mathbb{C}$, $\mathbf{1}a = a$.
- Για κάθε $a \in \mathbb{C}\backslash\{0\}$, υπάρχει ένα στοιχείο $a^{-1} \in \mathbb{C}$ ώστε $a \cdot a^{-1} = \mathbf{1}$.

Σύνολα που ικανοποιούν τις παραπάνω ιδιότητες θα τα ονομάζουμε «σώματα», δείτε τον ορισμό I.7.34. Παρατηρούμε ότι η συνάρτηση

$$\phi : \begin{cases} \mathbb{R} \to \mathbb{C} \\ x \mapsto (x, 0) \end{cases},$$



Σχήμα Ι.11: Γεωμετρική αναπαράσταση μιγαδικού αριθμού

είναι ένα προς ένα και επιπλέον «σέβεται» τις πράξεις του $\mathbb{R}$ και $\mathbb{C}$, δηλαδή $\phi(a+b) = \phi(a)+\phi(b)$, $\phi(ab) = \phi(a)\phi(b)$, για κάθε $a, b \in \mathbb{R}$. Δηλαδή οι πραγματικοί αριθμοί είναι υποσύνολο των μιγαδικών αριθμών και ο περιορισμός των πράξεων των μιγαδικών αριθμών στους πραγματικούς αριθμούς δίνουν τις συνηθισμένες πράξεις των πραγματικών. Τα στοιχεία της μορφής $(x, 0)$, $x \in \mathbb{R}$ θα τα συμβολίζουμε χάρην συντομίας απλά με x.

Θέτουμε $i := (0, 1) \in \mathbb{C}$ και τον αριθμό αυτό θα τον ονομάζουμε μιγαδική μονάδα. Με βάση τον ορισμό του πολλαπλασιασμού μιγαδικών αριθμών μπορούμε να αποδείξουμε ότι $i^2 = -1$. Πράγματι,

$$i^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0).$$

Παρατηρούμε ότι κάθε μιγαδικός αριθμός μπορεί να γραφτεί στη μορφή

$$(a, b) = a(1, 0) + b(0, 1) = a + bi.$$

Ι.6.7 Γεωμετρική Αναπαράσταση Μιγαδικών αριθμών.

Ορίσαμε τους μιγαδικούς αριθμούς ως το σύνολο των διατεταγμένων ζευγών $(a, b) \in \mathbb{R} \times \mathbb{R}$. Γεωμετρικά ένα τέτοιο ζευγάρι αντιστοιχεί στις συντεταγμένες ενός σημείου στο επίπεδο.

Στο παραπάνω σχήμα βλέπουμε τον μιγαδικό αριθμό $z = a + ib$ να παρίσταται ως σημείο του μιγαδικού επιπέδου. Ορίζουμε ως μέτρο του μιγαδικού αριθμού το μήκος του ευθύγραμμου τμήματος που συνδέει την αρχή $(0, 0)$ του συστήματος συντεταγμένων με το μιγαδικό αριθμό (a, b). Το μέτρο του μιγαδικού z θα το συμβολίζουμε με $|z|$ και προκύπτει ότι

$$|z| = \sqrt{a^2 + b^2}.$$

Επίσης ορίζουμε σαν όρισμα του μιγαδικού αριθμού z την γωνία θ που σχηματίζει ο άξονας των πραγματικών αριθμών με το ευθύγραμμο τμήμα που συνδέει την αρχή $(0, 0)$ του συστήματος συντεταγμένων με τον μιγαδικό αριθμό (a, b) μετρημένη αντίστροφα με την φορά των δεικτών του ρολογίου. Τη γωνία θ θα την ονομάζουμε όρισμα του μιγαδικού αριθμού. Παρατηρούμε ότι αν θ είναι ένα όρισμα του μιγαδικού αριθμού τότε για κάθε $k \in \mathbb{Z}$ και το $\theta + 2k\pi$ είναι ένα όρισμα. Το μοναδικά ορισμένο όρισμα θ του z το οποίο ικανοποιεί $0 \le \theta < 2\pi$ θα λέγεται πρωτεύον.

Έτσι ο μιγαδικός αριθμός $z = a + bi$ μπορεί να γραφεί σε τριγωνομετρική μορφή ως:

$$z = a + bi = |z|\big(\cos(\theta) + i\sin(\theta)\big).$$

Ορισμός Ι.6.25. Έστω $z = a + ib \in \mathbb{C}$. Θα συμβολίζουμε με $\bar{z}$, τον μιγαδικό αριθμό $a - ib$ και θα τον καλούμε συζυγή του z.

Πρόταση I.6.26. *Ισχύουν τα παρακάτω:*

1. $\overline{z_1 z_2} = \overline{z}_1 \overline{z}_2$.
2. $\overline{\overline{z}} = z$.
3. $z\overline{z} = |z|^2$.
4. $\overline{z} = z \Leftrightarrow z \in \mathbb{R}$.

Απόδειξη. 1. Έστω $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2$. Έχουμε ότι

$$\begin{aligned} \overline{z_1 z_2} &= \overline{a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1)} = \\ &= a_1 a_2 - b_1 b_2 - i(a_1 b_2 + a_2 b_1) = \\ &= (a_1 - ib_1)(a_2 - ib_2) = \\ &= \overline{(a_1 + ib_1)}\,\overline{(a_2 + ib_2)} = \\ &= \overline{z}_1 \overline{z}_2. \end{aligned}$$

2. $\overline{\overline{a + ib}} = \overline{a - ib} = a + ib$.
3. $z\overline{z} = (a + ib)(a - ib) = a^2 + b^2 = |z|^2$.
4. Αν $a + ib \in \mathbb{R}$ τότε $b = 0$ και είναι σαφές ότι $a = a + ib = a - ib = b$. Αντιστρόφως αν $z = \overline{z}$ τότε $b = -b \Rightarrow 2b = 0 \Rightarrow b = 0 \Rightarrow z \in \mathbb{R}$.

□

Πρόταση I.6.27. *Για το μέτρο μιγαδικού αριθμού ισχύουν τα παρακάτω:*

1. *Για κάθε $z \in \mathbb{C}$ ισχύει $|z| \geq 0$ και $|z| = 0$ αν και μόνο αν $z = 0$.*
2. *$|z_1 z_2| = |z_1| \cdot |z_2|$, για κάθε $z_1, z_2 \in \mathbb{C}$.*
3. *$|z_1 + z_2| \leq |z_1| + |z_2|$, για κάθε $z_1, z_2 \in \mathbb{C}$.*

Απόδειξη. 1. Έστω $z = a + ib$, έχουμε $|z| = \sqrt{a^2 + b^2} > 0$. Επιπλέον αν $|z| = 0$, τότε $a^2 + b^2 = 0$ δηλαδή το άθροισμα δυο μη αρνητικών πραγματικών αριθμών είναι 0, άρα $a^2 = b^2 = 0 \Rightarrow a = b = 0$.

2. Προκειμένου να αποδείξουμε ότι δύο θετικοί αριθμοί είναι ίσοι αρκεί να αποδείξουμε ότι τα τετράγωνα τους είναι ίσα. Αρκεί δηλαδή να αποδείξουμε ότι $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$. Όμως

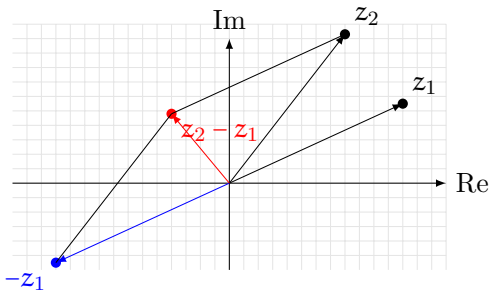
$$|z_1 z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z}_1 z_2 \overline{z}_2 = |z_1|^2 |z_2|^2.$$

3. Η ιδιότητα αυτή είναι γνωστή ως *τριγωνική ανισότητα* και εκφράζει την γνωστή από την ευκλείδεια γεωμετρία πρόταση: *η ευθεία συνδέει με τον συντομότερο τρόπο δύο σημεία στο επίπεδο*. Πράγματι όπως βλέπουμε και στο σχήμα I.12, ας είναι z_1 ο μιγαδικός που ορίζεται από το διάνυσμα OA, z_2 ο μιγαδικός που ορίζεται από το διανυσμα OB. Ο μιγαδικός $-z_2$ ορίζεται από το διάνυσμα OC. Παρατηρούμε ότι το μέτρο του μιγαδικού $z_1 - z_2$ ταυτίζεται με το μήκος $|OD|$ ενώ από το σχήμα έχουμε

$$|OD| + |DB| \leq |OB| \Leftrightarrow |OD| \leq |OB| - |DB| \Leftrightarrow |z_1 - z_2| \leq |z_1| - |z_2|,$$

δηλαδή το ζητούμενο.

□



Σχήμα Ι.12: Απόδειξη της τριγωνικής ανισότητας

Πρόταση Ι.6.28 (De' Moivre). *Ας υποθέσουμε ότι* $z = |z|(\cos(\phi) + \mathrm{i}\sin(\phi)$, *και* $w = |w|(\cos(\theta) + \mathrm{i}\sin(\theta)$, *είναι δύο μιγαδικοί αριθμοί γραμμένοι σε τριγωνομετρική μορφή. Ισχύει:*

$$zw = |z||w|\big(\cos(\phi+\theta) + \mathrm{i}\sin(\phi+\theta)\big).$$

Απόδειξη. Στην στοιχειώδη τριγωνομετρία αποδεικνύουμε τους τύπους

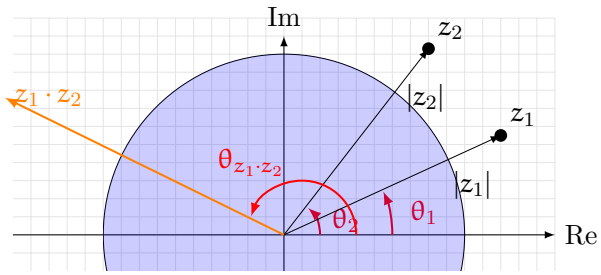
$$\begin{aligned}\cos(\theta+\phi) &= \cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi)\\ \sin(\theta+\phi) &= \cos(\theta)\sin(\phi) + \sin(\theta)\cos(\phi).\end{aligned} \tag{I.7}$$

Άρα το γινόμενο υπολογίζεται ως

$$zw = |z|\big(\cos(\phi) + \mathrm{i}\sin(\phi)\big)|w|\big(\cos(\theta) + \mathrm{i}\sin(\theta)\big) =$$

$$= |z||w|\big(\cos(\theta)\cos(\phi) - \sin(\theta)\sin(\phi) + \mathrm{i}\big(\cos(\theta)\sin(\phi) + \sin(\theta)\cos(\phi)\big)\big) =$$

$$= |zw|\big(\cos(\theta+\phi) + \mathrm{i}\sin(\theta+\phi)\big)\big)$$



Σχήμα Ι.13: Απόδειξη του τύπου του De' Moivre, το σύνολο $|z| \le 1$ δείχνεται με μπλε χρώμα.

Θα δώσουμε μία ακόμα απόδειξη τόσο των τύπων (I.7) όσο και της πρότασης De' Moivre χρησιμοποιώντας της μιγαδική εκθετική συνάρτηση στην παρατήρηση I.8.59. □

Θεώρημα I.6.29. *Κάθε πολυωνυμική εξίσωση*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{C},$$

έχει τουλάχιστον μία ρίζα στο $\mathbb{C}$.

Παρόλο που το παραπάνω θεώρημα έχει την ονομασία «το θεμελιώδες θεώρημα της άλγεβρας», η απόδειξη του βασίζεται σε καθαρά αναλυτικά εργαλεία αφού το αξίωμα της πληρότητας που χαρακτηρίζει τους πραγματικούς αριθμούς θα πρέπει να παίξει ρόλο στην απόδειξη.

Πιθανότατα θα δείτε μια απόδειξη σε ένα πρώτο μάθημα μιγαδικής ανάλυσης, διαφορισίμων πολλαπλοτήτων ή αλγεβρικής τοπολογίας. Θα δώσουμε και εμείς μια απόδειξη βασισμένοι στην γραμμική Άλγεβρα στην εφαρμογή 2 στην σελίδα 204.

Θα πρέπει να παρατηρήσουμε ότι αν το $n \leq 4$, τότε οι ρίζες του πολυωνύμου μπορούν να εκφραστούν σε κλειστή μορφή, σαν συναρτήσεις των συντελεστών a_i, με την βοήθεια ριζικών. Η περίπτωση $n = 2$ σας είναι γνωστή από τα λυκειακά μαθηματικά. Πράγματι οι ρίζες $\rho_{1,2}$ του

$$a_2 x^2 + a_1 x + a_0 = 0,$$

δίνονται από τους τύπους

$$\rho_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}$$

Παρόμοιοι αλλά πιο πολύπλοκοι τύποι είναι γνωστοί για τις περιπτώσεις $n = 3, 4$. Η περίπτωση $n \geq 5$, ήταν ένα από τα μεγάλα άλυτα πρόβλημα των μαθηματικών του 19 αιώνα. Πρώτος ο N. Abel απόδειξε ότι οι ρίζες της εξίσωσης πέμπτου βαθμού δεν εκφράζονται κατ' ανάγκην με την βοήθεια ριζικών, ενώ ο E. Galois έδωσε κριτήρια για το πότε οι ρίζες μίας πολυωνυμικής εξίσωσης n βαθμού μπορούν να εκφραστούν με τη βοήθεια ριζικών.

Ο **Évariste Galois** (25 Οκτωβρίου 1811 – 31 Μαΐου 1832) ήταν Γάλλος Μαθηματικός ο οποίος στην σύντομη ζωή του, σκοτώθηκε σε μονομαχία σε ηλικία 21 ετών, ανέπτυξε εργαλεία τα οποία επηρέασαν και άλλαξαν την εξέλιξη της Θεωρίας ομάδων, της Άλγεβρας και γενικότερα των Μαθηματικών μέχρι σήμερα.

Εισήγαγε την έννοια του πεπερασμένου σώματος αλλά και της ομάδας όπως την αντιλαμβανόμαστε σήμερα. Κατασκεύασε την γενική γραμμική ομάδα πάνω από ένα πεπερασμένο σώμα στην μελέτη του της γενικής πολυωνυμικής εξίσωσης βαθμού p^n. Κατασκεύασε τις προβολικές γενικές γραμμικές ομάδες $\mathrm{PSL}(2, p)$ και έδειξε ότι είναι απλές εκτός αν $p = 2, 3$.

Όμως η σημαντικότερη συμβολή του Galois στα Μαθηματικά είναι η θεωρία Galois στην οποία ανήγαγε το πρόβλημα της επιλυσιμότητας μιας πολυωνυμικής εξίσωσης με ριζικά στην δομή της ομάδας συμμετριών των ριζών της εξίσωσης. Η θεωρία αυτή έδωσε την βάση και την γλώσσα στην οποία εκφράζονται μια σειρά από έννοιες της αλγεβρικής θεωρίας Αριθμών αλλά και των διαφορικών εξισώσεων και της Φυσικής.

Θεώρημα Ι.6.30. *Κάθε πολυωνυμική εξίσωση*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in \mathbb{C},$$

έχει ακριβώς n*-ρίζες στο* $\mathbb{C}$.

Απόδειξη. Θα κάνουμε χρήση του θεωρήματος Ι.6.29. Πράγματι η πολυωνυμική εξίσωση έχει μία τουλάχιστον ρίζα ρ_1, άρα μπορούμε να γράψουμε

$$f(x) = (x - \rho_1)g(x),$$

όπου το $g(x)$ είναι ένα πολυώνυμο βαθμού $n-1$. Εφαρμόζουμε το θεώρημα Ι.6.29 στο πολυώνυμο $g(x)$, η απόδειξη του θεωρήματος αποδεικνύεται επαγωγικά. □

Ι.6.8 Ν-ρίζες μιγαδικών αριθμών.

Στην ενότητα αυτή θα μάθουμε πως να υπολογίζουμε τις λύσεις της εξίσωσης $x^n = a$, όπου $a \in \mathbb{C}$. Η εξίσωση αυτή έχει ακριβώς n το πλήθος ρίζες σύμφωνα με το θεώρημα Ι.6.30. Μπορούμε να τις υπολογίσουμε ακριβώς.

Πρόταση Ι.6.31. *Οι* n *το πλήθος λύσεις της εξίσωσης*

$$x^n = 1,$$

δίνονται από τον τύπο

$$x_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right).$$

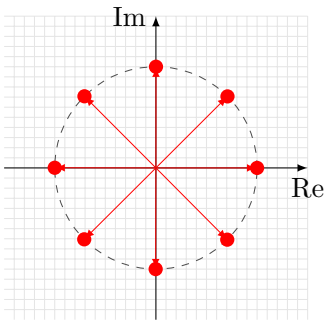
Απόδειξη. Έστω $x \in \mathbb{C}$, ώστε $x^n = 1$. Γράφουμε $x = |x|\big(\cos(\theta) + i\sin(\theta)\big)$. Κάνουμε χρήση της πρότασης Ι.6.28 για να υπολογίσουμε

$$1 = x^n = |x|^n\big(\cos(n\theta) + i\sin(n\theta)\big).$$

Συνεπώς $|x| = 1$ και επιπλέον

$$\cos(n\theta) = 1, \quad \sin(n\theta) = 0,$$

από όπου έχουμε ότι $n\theta = 2\pi k \Rightarrow \theta = 2\pi k/n$. Από τα παραπάνω θ μόνο τα $0 \le k < n$ δίνουν διαφορετικές ανά δύο ρίζες. □



Σχήμα Ι.14: Οι 8-ες ρίζες της μονάδας στο μιγαδικό επίπεδο.

Λήμμα I.6.32. *Αν z_0 είναι μία ρίζα της $x^n = a$, τότε οι υπόλοιπες ρίζες δίνονται από του τύπο $z_i = \zeta_i z_0$, όπου το ζ_i διατρέχει τις n-ρίζες της μονάδας.*

Απόδειξη. Αφού το z_0 είναι μία ρίζα έχουμε $z_0^n = a$. Αν z είναι μία τυχαία άλλη ρίζα τότε $z_0^n = z^n$, συνεπώς $(z/z_0)^n = 1$, δηλαδή το z/z_0 είναι μία n-ρίζα της μονάδας. □

Πρόταση I.6.33. *Έστω $a = |a|\big(\cos(\theta) + i\sin(\theta)\big)$. Οι n-ρίζες του a δίνονται από του τύπο*

$$z_i = \sqrt[n]{|a|}\Big(\cos\Big(\frac{2\pi k + \theta}{n}\Big) + i\sin\Big(\frac{2\pi k + \theta}{n}\Big)\Big),$$

$k = 0, \dots n-1$.

Απόδειξη. Μία ρίζα z_0 της εξίσωσης είναι η

$$z_0 = \sqrt[n]{|a|}\Big(\cos\Big(\frac{\theta}{n}\Big) + i\sin\Big(\frac{\theta}{n}\Big)\Big),$$

όπως παρατηρούμε κάνοντας χρήση του DeMoivre. Για να πάρουμε όλες τις ρίζες πολλαπλασιάζουμε την ρίζα αυτή με τις n-ρίζες της μονάδας σύμφωνα με το λήμμα I.6.32 οι οποίες έχουν υπολογιστεί στην πρόταση I.6.31. Το ζητούμενο προκύπτει και πάλι με χρήση του τύπου του DeMoivre. □

Ασκήσεις

Άσκηση I.16 Αποδείξτε ότι αν $a + ib \in \mathbb{C} \neq 0$, τότε $(a+ib)^{-1} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$.

Άσκηση I.17 Να υπολογιστούν οι ρίζες της εξίσωσης $x^2 + x + 3$.

Άσκηση I.18 Να υπολογιστούν οι 10 ρίζες του $1 + i$.

Άσκηση I.19 Θεωρήστε το σύνολο $\mu(n)$ των n-ριζών της μονάδας. Αποδείξτε ότι αν $x, y \in \mu(n)$ τότε $xy \in \mu(n)$. Δείξτε ότι υπάρχει ένα στοιχείο $e \in \mu(n)$ ώστε $ex = x$ για κάθε $x \in \mu(n)$ και ότι αν $x \in \mu(n)$, τότε υπάρχει $x^{-1} \in \mu(n)$ ώστε $x \cdot x^{-1} = 1$.

Άσκηση I.20 Θεωρήστε τον μοναδίαιο δίσκο D κέντρου 0 και ακτίνας 1, δηλαδή $D := \{z \in \mathbb{C} : |z| < 1\}$. Θεωρήστε την συνάρτηση $z^n : D \to \mathbb{C}$. Αποδείξτε, ότι η εικόνα της z^n είναι το D. Είναι η z^n ένα προς ένα; Περιγράψτε την z^n γεωμετρικά.

Άσκηση I.21 Αποδείξτε ότι το άθροισμα των n-οστών ριζών του 1 είναι 0.

I.7 Αφηρημένη Άλγεβρα

Ο άνθρωπος σκέφτεται αφαιρετικά. Μία από τις πρώτες αφαιρέσεις που μαθαίνει κανείς είναι αυτή των φυσικών αριθμών. Η έννοια του αριθμού 3 εκφράζει τον πληθικό αριθμό ενός συνόλου και είναι *ανεξάρτητη από τη φύση των στοιχείων* που περιέχει το σύνολο με 3 το πλήθος στοιχεία. Το επόμενο βήμα είναι να *απομονώσουμε τις πράξεις από τη φύση των συνόλων στα οποία αναφέρονται* και να μελετήσουμε τις ιδιότητες των πράξεων από μόνες τους. Καλώς ήρθατε στον κόσμο της μοντέρνας Άλγεβρας!

Ι.7.1 Ομάδες

Ορισμός Ι.7.1. Μια ομάδα είναι ένα σύνολο G εφοδιασμένο με μια πράξη +, δηλαδή μία συνάρτηση

$$+ : G \times G \longrightarrow G$$
$$(a, b) \longmapsto a + b$$

για την οποία ισχύουν οι παρακάτω ιδιότητες:

1. $(a + b) + c = a + (b + c)$ για κάθε $a, b, c \in G$ (προσεταριστική ιδιότητα).
2. Υπάρχει ένα στοιχείο $\mathbf{0}_G$, ώστε $a + \mathbf{0}_G = \mathbf{0}_G + a = a$, για κάθε $a \in G$ (Ύπαρξη ουδέτερου στοιχείου της G)
3. Για κάθε $a \in G$ υπάρχει ένα μοναδικό στοιχείο $-a \in G$ ώστε $a + (-a) = (-a) + a = \mathbf{0}_G$ για κάθε $a \in G$ (ύπαρξη αντιθέτου).

Επιπλέον μια ομάδα θα λέγεται αβελιανή (προς τιμή του Νορβηγού Μαθηματικού Niels Henrik Abel) αν για κάθε $a, b \in G$ ισχύει $a + b = b + a$.

Σε μια ομάδα το ουδέτερο στοιχείο είναι μοναδικό αφού υπήρχει και ένα δεύτερο ουδέτερο στοιχείο $\mathbf{0}'_G$, τότε

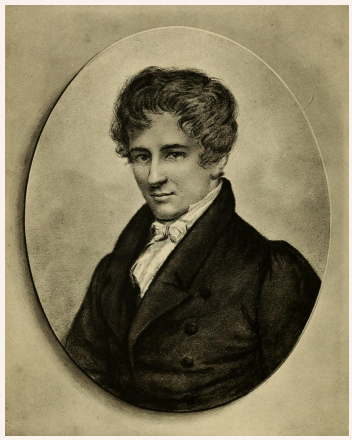
$$\mathbf{0}_G = \mathbf{0}_G + \mathbf{0}'_G = \mathbf{0}'_G$$

Επίσης το αντίθετο ενός στοιχείου a είναι μοναδικό. Πράγματι αν $-a, -a'$ είναι τα αντίθετα του a, τότε

$$-a = \mathbf{0}_G + (-a) = ((-a') + a) + (-a) = (-a') + (a + (-a)) = (-a') + \mathbf{0}_G = (-a').$$

Επίσης, υπάρχουν ομάδες στις οποίες το σύμβολο της πράξης γράφεται προσθετικά όπως παραπάνω και ομάδες στις οποίες το σύμβολο της πράξης γράφεται πολλαπλασιαστικά. Δηλαδή γράφουμε $a(bc)$ αντί $a + (b + c)$, ή το αντίθετο $-a$, γράφεται πολλαπλασιαστικά με a^{-1}, και η σχέση $a + b = \mathbf{0}_G$, γράφεται ως $aa^{-1} = \mathbf{1}_G$.

Ο **Niels Henrik Abel** (5 Αυγούστου 1802 – 6 Απριλίου 1829) ήταν Νορβηγός Μαθηματικός με πρωτοποριακή συνεισφορά σε πολλά Μαθηματικά αντικείμενα. Έδωσε την πρώτη πλήρη απόδειξη για την αδυναμία επίλυσης της πεμπτοβάθμιας εξίσωσης με ριζικά, ένα από τα ανοιχτά προβλήματα της εποχής του. Ασχολήθηκε με τις ελλειπτικές και αβελιανές συναρτήσεις και βοήθησε στην ανάπτυξη της θεωρίας των αβελιανών πολλαπλοτήτων (που φέρουν και το όνομα του). Ήταν ένας από τους πρωτοπόρους της θεωρίας ομάδων την οποία ανέπτυξε με ανεξάρτητο και πρωτότυπο τρόπο. Μπόρεσε να ασχοληθεί ενεργά με τα Μαθηματικά μόνο για επτά χρόνια. Τις ανακαλύψεις του τις έκανε ζώντας μέσα στην φτώχεια και πέθανε από φυματίωση σε ηλικία 27 ετών, δύο μέρες πριν μάθει ότι του έχει προσφερθεί θέση καθηγητή στο πανεπιστήμιο του Βερολίνου. Ο Charles Hermite είπε χαρακτηριστικά για το έργο του: «Ο Abel έχει αφήσει αρκετό υλικό για να κρατήσει απασχολημένους τους Μαθηματικούς τα επόμενα πεντακόσια χρόνια». Το βραβείο Abel στα Μαθηματικά, το οποίο συμπληρώνει το βραβείο Nobel και απονεμήθηκε το 2003 για πρώτη φορά ονομάσθηκε έτσι προς τιμήν του.



Παραδείγματα I.7.2. 1. Το σύνολο των ακέραιων αριθμών $\mathbb{Z}$ με πράξη τη (συνήθη) πρόσθεση αποτελεί *άπειρη αβελιανή ομάδα*. Το ίδιο ισχύει και για τα σύνολα $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$.

2. Το σύνολο των κλάσεων υπολοίπων modulo n, $n \in \mathbb{N}$, $n > 1$:

$$\mathbb{Z}_n = \{\overline{a} := a \mod n | a \in \mathbb{Z}\}$$

με (καλά ορισμένη) πράξη την πρόσθεση κλάσεων

$$\oplus \left\{ \begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ (\overline{a}, \overline{b}) \mapsto \overline{a} \oplus \overline{b} \end{array} \right\}$$

αποτελεί *πεπερασμένη, αβελιανή, ομάδα*.

3. Το σύνολο $M_n(\mathbb{R})$ των τετραγωνικών $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξη την πρόσθεση πινάκων αποτελεί άπειρη *αβελιανή ομάδα*.

4. Έστω $\omega := e^{\frac{2\pi i}{n}}$. Το σύνολο

$$\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$$

με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών, αποτελεί πεπερασμένη αβελιανή ομάδα. Η ομάδα αυτή λέγεται ομάδα των n-ριζών της μονάδας.

5. Το σύνολο των πρώτων κλάσεων υπολοίπων $\mod n$, $n \in \mathbb{N}$, $n > 1$

$$\mathbb{Z}_n^* = \{\overline{a} := a \mod n | a \in \mathbb{Z}, (a, n) = 1\}$$

με πράξη τον (καλά ορισμένο) πολλαπλασιασμό κλάσεων

$$\odot \left\{ \begin{array}{c} \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^* \\ (\overline{a}, \overline{b}) \mapsto \overline{a} \odot \overline{b} \end{array} \right\}$$

αποτελεί *πεπερασμένη, αβελιανή ομάδα*.

6. Τα σύνολα $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ των μη-μηδενικών στοιχείων των $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ με πράξη τον συνήθη πολλαπλασιασμό αποτελούν *άπειρη, αβελιανή* ομάδα.

7. Το σύνολο $M_n(\mathbb{R})$ των $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξη τον πολλαπλασιασμό πινάκων *δεν* αποτελεί ομάδα, αφού υπάρχουν $n \times n$ πίνακες με στοιχεία πραγματικούς οι οποίοι δεν έχουν αντίστροφο. Αν θεωρήσουμε το υποσύνολο του $M_n(\mathbb{R})$

$$GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) | \det(A) \neq 0\},$$

τότε αυτό με πράξη τον πολλαπλασιασμό πινάκων αποτελεί *άπειρη ομάδα*. Η ομάδα αυτή, αν $n > 1$, *δεν* είναι αβελιανή επειδή δεν ισχύει εν γένει $A \cdot B = B \cdot A$.

Κυκλικές ομάδες

Ορισμός I.7.3. Μια ομάδα $(G, \circ)$ λέγεται *κυκλική ομάδα* όταν υπάρχει κάποιο στοιχείο αυτής $x \in G$, τέτοιο ώστε όλα τα στοιχεία της G να γράφονται ως δυνάμεις του x.

Κάθε τέτοιο στοιχείο σε μια κυκλική ομάδα λέγεται *γεννήτορας* αυτής.

Σημείωση: Αν $g \in G$ και $n \in \mathbb{Z}$, τότε η δύναμη g^n ορίζεται ως εξής:

$$g^n = \begin{cases} \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ φορές}} & \text{όταν } n \geq 1 \\ e & \text{όταν } n = 0 \\ \underbrace{g^{-1} \circ g^{-n} \circ \cdots \circ g^{-1}}_{-n \text{ φορές}} & \text{όταν } n < 0 \end{cases}$$

Συμβολισμός Αν G είναι κυκλική με γεννήτορα g, τότε γράφουμε $G = \langle g \rangle$.

Παραδείγματα: Οι ομάδες των παραδειγμάτων 4 και 5 είναι κυκλικές.

Ορισμός Ι.7.4. Το πλήθος των στοιχείων μιας πεπερασμένης ομάδας, λέγεται *τάξη αυτής*.

Πρόταση Ι.7.5. *Αν η ομάδα* G *είναι πεπερασμένη και κυκλική τάξης* n, $G = \langle g \rangle$, *τότε οι γεννήτορες αυτής είναι τα στοιχεία της μορφής* g^d *με* $(d, n) = 1$.

Το θεώρημα του Lagrange

Υποθέτουμε ότι $(G, \circ)$ είναι μια ομάδα και $H \leq G$ είναι μια υποομάδα αυτής. Στο σύνολο $G \times G$ ορίζουμε τη σχέση: $a, b \in G$,

$$a \sim b \Leftrightarrow a^{-1}b \in H.$$

Η σχέση αυτή είναι μια σχέση ισοδυναμίας. Η κλάση ισοδυναμίας του στοιχείου a είναι το σύνολο $aH := \{ah | h \in H\}$.

Ορισμός Ι.7.6. Το πλήθος των κλάσεων ισοδυναμίας της H στην G, λέγεται *δείκτης* της H στην G και συμβολίζεται με $[G : H]$. Η τάξη μιας ομάδας $(G, \circ)$ συμβολίζεται με $|G|$.

Ο **Joseph-Louis Lagrange** (25 Ιανουαρίου 1736 – 10 Απριλίου 1813)

ήταν Ιταλός Μαθηματικός, Φυσικός και Αστρονόμος. Ήταν ένας από τους πρωτοπόρους του Λογισμού των μεταβολών και εργάστηκε σε όλα τα πεδία της μαθηματικής ανάλυσης αλλά και στην θεωρία Αριθμών, στις διαφορικές εξισώσεις αλλά και στην κλασική και ουράνια μηχανική. Η εργασία του Traité de Mécanique Analytique ήταν μια συστηματική μελέτη της κλασικής μηχανικής και επιρέασε την εξέλιξη της μαθηματικής φυσικής στην εποχή του. Στην ουράνια μηχανική μελέτησε το πρόβλημα των τριών σωμάτων και άφησε το όνομα του στα σημεία Lagrange που είναι ιδανικά σημεία για την τοποθέτηση δορυφόρων.

Στην θεωρία αριθμών απέδειξε ότι κάθε φυσικός είναι άθροισμα τεσσάρων τετραγώνων και είχε συνεισφορά στις Διοφαντικές εξισώσεις. Έκανε σημαντική δουλειά στην επίλυση πολυωνυμικών εξισώσεων (Lagrange resolvents) και παράλληλα έθεσε τις βάσεις για την θεωρία ομάδων προετοιμάζοντας το έδαφος για την θεωρία Galois.

Το παρακάτω είναι γνωστό ως θεώρημα του Lagrange .

Θεώρημα I.7.7. *οθέτουμε ότι η* G *είναι μια πεπερασμένη ομάδα και* $H \leq G$. *Ισχύει* $|G| = [G : H] \cdot |H|$. *Επομένως, η τάξη μιας υποομάδας μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας.*

Ομάδα πηλίκου

Έστω G μια ομάδα και $H \leq G$ μια υποομάδα αυτής. Στο σύνολο των κλάσεων ισοδυναμίας που ορίσαμε παραπάνω, έχουμε τις κλάσεις $\{aH|a \in G\}$. Θα θέλαμε να ορίσουμε ένα πολλαπλασιασμό στο σύνολο κλάσεων ώστε να αποκτήσει δομή ομάδας, την οποία ονομάζουμε ομάδα πηλίκου. Αυτό όμως δεν είναι πάντοτε δυνατό.

Ορισμός I.7.8. Έστω G μια ομάδα και $H \leq G$. Η H λέγεται *κανονική υποομάδα* της G όταν ισχύει $aH = Ha$ για κάθε $a \in G$, όπου $Ha = \{ha|h \in H\}$.

Αν τώρα G είναι ομάδα και H *κανονική υποομάδα* της G, τότε το σύνολο

$$G/H := \{aH|a \in G\}$$

με πράξη τον (καλά ορισμένο) πολλαπλασιασμό

$$(aH)(bH) = ab(H),$$

αποτελεί ομάδα.

Άμεση συνέπεια του θεωρήματος του Lagrange είναι ότι η τάξη της ομάδας G/H είναι ίση με $|G|/|H|$.

Αν τώρα G είναι αβελιανή, τότε κάθε υποομάδα αυτής H είναι κανονική και συνεπώς πάντοτε ορίζεται η ομάδα πηλίκου G/H.

I.7.2 Δακτύλιοι

Ορισμοί και παραδείγματα

Ορισμός I.7.9. Ένα μη-κενό σύνολο R εφοδιασμένο με δύο (διμελής) πράξεις, πρόσθεσης

$$+\left\{\begin{array}{c} R \times R \to R \\ (a,b) \mapsto a+b \end{array}\right\}$$

και πολλαπλασιασμού

$$\cdot\left\{\begin{array}{c} R \times R \to R \\ (a,b) \mapsto a \cdot b \end{array}\right\}$$

λέγεται δακτύλιος, όταν επαληθεύει τα ακόλουθα αξιώματα:

R1 Ο $(R,+)$ αποτελεί αβελιανή ομάδα.

R2 Για όλα τα στοιχεία $x,y,z \in R$ ισχύει (αξίωμα προσεταιριστικότητας)

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

R3 Για όλα τα στοιχεία $x, y, z \in R$ ισχύουν (αξιώματα επιμεριστικότητας)

$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Αν επιπλέον ισχύει το αξίωμα ύπαρξης μοναδιαίου

R4 Υπάρχει ένα στοιχείο $1_R \in R$, $1_R \neq 0$, τέτοιο ώστε για όλα τα στοιχεία $x \in R$ να ισχύει

$$1_R \cdot x = x \cdot 1_R,$$

τότε ο δακτύλιος R λέγεται δακτύλιος με μοναδιαίο.

Αν για τον R ισχύει επιπλέον το αξίωμα της αντιμετάθεσης

R5 Για όλα τα στοιχεία $x, y \in R$ ισχύει:

$$x \cdot y = y \cdot x,$$

τότε ο δακτύλιος R λέγεται αντιμεταθετικός δακτύλιος.

Τέλος αν ισχύουν τα αξιώματα (R4) και (R5) συγχρόνως τότε ο R λέγεται αντιμεταθετικός δακτύλιος με μοναδιαίο.

Παραδείγματα Ι.7.10. 1. Το σύνολο των ακέραιων $\mathbb{Z}$ με πράξεις τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο.

2. Για κάθε $m \in \mathbb{N}$, $m > 1$, το σύνολο των κλάσεων υπολοίπων $\bmod m$, $\mathbb{Z}_m$, με πράξεις τις (καλά ορισμένες) πράξεις πρόσθεσης κλάσεων

$$\oplus \left\{ \begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \\ (\overline{a}, \overline{b}) \mapsto \overline{a} \oplus \overline{b} \end{array} \right\}$$

και πολλαπλασιασμού κλάσεων

$$\odot \left\{ \begin{array}{c} \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n^* \\ (\overline{a}, \overline{b}) \mapsto \overline{a} \odot \overline{b} \end{array} \right\}$$

αποτελεί επίσης αντιμεταθετικό δακτύλιο με μοναδιαίο.

3. Το σύνολο των ακέραιων του Gauss

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

με πράξεις τις συνήθεις πράξεις μιγαδικών αποτελεί επίσης αντιμεταθετικό δακτύλιο με μοναδιαίο.

4. Ο δακτύλιος των πολυωνύμων $R[x]$ με συντελεστές από έναν αντιμεταθετικό δακτύλιο R αποτελεί αντιμεταθετικό δακτύλιο με μοναδιαίο. Για παράδειγμα, μπορούμε να θεωρήσουμε τον δακτύλιο $\mathbb{Z}[x]$, αλλά και να συνεχίσουμε επαγωγικά για να ορίζουμε τον δακτύλιο

$$\mathbb{Z}[x, y] = \mathbb{Z}[x][y].$$

5. Για να κατανοήσουμε ένα μαθηματικό ή γεωμετρικό αντικείμενο συχνά αρκεί να κατανοήσουμε το σύνολο των συναρτήσεων πάνω σε αυτό. Οι συναρτήσεις αυτές έρχονται εφοδιασμένες με την δομή ενός δακτυλίου. Για την ώρα το παράδειγμα αυτό δεν βγάζει και πολύ νόημα είναι η βασική ιδέα ενός δυναμικού κλάδου των Μαθηματικών της «Αλγεβρικής Γεωμετρίας».

Ορισμός I.7.11. Έστω R κάποιος αντιμεταθετικός δακτύλιος. Ένα στοιχείο $x \in R$, $x \neq 0$, λέγεται διαιρέτης του μηδενός αν και μόνο αν υπάρχει $y \in R$, $y \neq 0$ με $x \cdot y = 0$.

Ορισμός I.7.12. Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο λέγεται *ακέραια περιοχή*, όταν δεν έχει διαιρέτες του μηδενός.

Παραδείγματα I.7.13.

1. Ο δακτύλιος $(\mathbb{Z}, +, \cdot)$ είναι ακέραια περιοχή.
2. Οι δακτύλιοι $(\mathbb{Z}_m, +, \cdot)$ είναι ακέραιες περιοχές αν και μόνο αν ο m είναι πρώτος.
3. Ο δακτύλιος $\mathbb{Z}[i]$ είναι επίσης ακέραια περιοχή.

Ορισμός I.7.14. Ένα μη κενό υποσύνολο R_1 του αντιμεταθετικού δακτυλίου R λέγεται *υποδακτύλιος* του R όταν είναι δακτύλιος ως προς τις πράξεις πρόσθεσης και πολλαπλασιασμού του R.

Ισχύει:

Πρόταση I.7.15. *Ένα μη κενό υποσύνολο R_1 του αντιμεταθετικού δακτυλίου R, είναι υποδακτύλιος του R ακριβώς τότε όταν για όλα τα στοιχεία $x, y \in R_1$ ισχύει*

$$x - y \in R_1 \text{ και } x \cdot y \in R_1.$$

Ιδεώδη ενός αντιμεταθετικού δακτυλίου

Ορισμός I.7.16. Έστω R ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και I ένα μη-κενό υποσύνολο του R.

Το I λέγεται ιδεώδες όταν ισχύουν τα αξιώματα:

I1 Το I αποτελεί ομάδα ως προς την πρόσθεση,

I2 Για κάθε $r \in R$ και $x \in I$ ισχύει $rx \in I$.

Ορισμός I.7.17. Αν $\alpha \in R$, τότε το *κύριο ιδεώδες* του R το οποίο παράγεται από το στοιχείο α, ορίζεται

$$\langle \alpha \rangle := \{r\alpha | r \in R\}.$$

Αν ο R είναι ακέραια περιοχή και όλα τα ιδεώδη του R είναι κύρια, τότε ο R λέγεται *περιοχή κυρίων ιδεωδών*.

Παράδειγμα I.7.18. Η ακέραια περιοχή των ακέραιων αριθμών $(\mathbb{Z}, +, \cdot)$ όπως και ο δακτύλιος του Gauss είναι περιοχές κυρίων ιδεωδών.

Ορισμός Ι.7.19. Αν R ακέραια περιοχή, το στοιχείο $p \in R$ λέγεται *ανάγωγο*, όταν δεν είναι μονάδα του R, δηλαδή δεν είναι πολλαπλασιαστικό αντίστροφο του R, και δεν αναλύεται σε γινόμενο μη τετριμμένων παραγόντων, δηλαδή, αν $p = a \cdot b$, τότε ένα από τα a, b είναι μονάδα του R.

Ορισμός Ι.7.20. Μια ακέραια περιοχή R λέγεται *περιοχή μονοσήμαντης ανάλυσης*, όταν κάθε στοιχείο $a \neq 0$ αυτής είναι μονάδα ή ανάγωγο στοιχείο του R ή γινόμενο αναγώγων στοιχείων του R και επιπλέον η παράσταση αυτή είναι (ουσιαστικά) μονοσήμαντη.

Ισχύει η

Πρόταση Ι.7.21. *Κάθε περιοχή κυρίων ιδεωδών είναι και περιοχή μονοσήμαντης ανάλυσης.*

Παρατήρηση Ι.7.22. Δεν είναι κάθε ακέραια περιοχή, περιοχή μονοσήμαντης ανάλυσης. Για παράδειγμα στην ακέραια περιοχή

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

ο αριθμός 6 έχει δύο, διαφορετικές μεταξύ τους, γνήσιες αναλύσεις σε γινόμενο αναγώγων στοιχείων:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Παρατήρηση Ι.7.23. Αν ένα ιδεώδες I περιέχει ένα στοιχείο του $U(R)$, τότε $I = R$. Πράγματι, ένα τέτοιο ιδεώδες περιέχει το 1 του R και συνεπώς όλο τον δακτύλιο. Αυτό έχει ως συνέπεια ότι κάθε ιδεώδες ενός σώματος είναι ή μηδενικό ή όλος ο δακτύλιος R.

Παρατήρηση Ι.7.24. Το $\mathbb{Z}$ είναι ακέραια περιοχή αλλά όχι σώμα. Αν όμως έχουμε μια πεπερασμένη ακέραια περιοχή, τότε αναγκαστικά αυτή είναι σώμα. Πράγματι γράφουμε όλα τα στοιχεία της στην μορφή $a_1 = 0, a_2 = 1, \ldots, a_n$. Θεωρούμε στη συνέχεια ένα μη μηδενικό στοιχείο $a \in R$ και πολλάπλασιάζουμε κάθε στοιχείο με a. Τα στοιχεία

$$aa_1 = 0, aa_2, \ldots, aa_n$$

είναι ανά δύο διαφορετικά, αφού, αν $aa_i = aa_j$, τότε $a(a_i - a_j) = 0$ άρα αφού έχουμε ακέραια περιοχή και $a \neq 0$ θα έχουμε $a_i = a_j$. Άρα με τον πολλαπλασιασμό με a παίρνουμε κάθε στοιχείο του δακτυλίου R, άρα για κάποιο a_i θα πάρουμε $aa_i = 1$.

Ι.7.3 Σώματα

Ορισμός Ι.7.25. Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο στον οποίο κάθε μη-μηδενικό στοιχείο είναι αντιστρέψιμο, λέγεται σώμα.

Παραδείγματα Ι.7.26.

1. Οι αντιμεταθετικοί δακτύλιο με μοναδιαίο $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ είναι σώματα.
2. Αν p πρώτος αριθμός, τότε ο δακτύλιος $(\mathbb{Z}_p, \oplus, \odot)$ είναι σώμα.

3. Αν $d \in \mathbb{Z}\backslash\{0,1\}$ ελεύθερος τετραγώνου, τότε ο δακτύλιος
$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\},$$
είναι σώμα.

4. Αν K σώμα και x ανεξάρτητη μεταβλητή, τότε το σύνολο
$$K(x) = \left\{ \frac{f(x)}{g(x)} | f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$
είναι επίσης σώμα και λέγεται το σώμα των ρητών συναρτήσεων υπεράνω του K.

Κάθε σώμα K περιέχει (ισόμορφα) το σώμα των ρητών αριθμών $\mathbb{Q}$ ή ένα σώμα $\mathbb{Z}_p$ για κάποιο πρώτο αριθμό p. Στην πρώτη περίπτωση λέμε ότι το σώμα είναι χαρακτηριστικής μηδέν ενώ στην δεύτερη ότι το σώμα είναι χαρακτηριστικής p.

Παράδειγμα I.7.27. Αν επιλέξουμε ένα στοιχείο $f \in R$ μπορούμε να θεωρήσουμε το ιδεώδες fR που αποτελείται από όλα τα πολλαπλάσια του f. Ιδεώδη αυτής της μορφής θα λέγονται *κύρια*.

Θα αποδείξουμε στη συνέχεια ότι κάθε ιδεώδες των δακτυλίων $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου $\mathbb{F}$ είναι σώμα, είναι κύριο. Αντιθέτως στον δακτύλιο $\mathbb{F}[x, y]$ το ιδεώδες $\langle x, y \rangle$ που παράγεται από τα x, y δεν είναι κύριο.

Παρατήρηση I.7.28. Από τις ιδιότητες του δακτυλίου είναι άμεσο ότι $0 \cdot a = 0$. Πράγματι $0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$ άρα $0 \cdot a = 0$.

Ορισμός I.7.29. Ένας αντιμεταθετικός δακτύλιος με μοναδιαίο θα λέγεται ακέραια περιοχή αν και μόνο αν $x \cdot y = 0$ συνεπάγεται $x = 0$ ή $y = 0$.

Παράδειγμα I.7.30. Ο δακτύλιος $\mathbb{Z}$ είναι ακέραια περιοχή. Αντιθέτως, ο δακτύλιος $\mathbb{Z}/6\mathbb{Z}$ δεν είναι ακέραια περιοχή, αφού $2 \neq 0$ και $3 \neq 0$ όμως $2 \cdot 3 \equiv 0 \mathrm{mod} p$.

Ορισμός I.7.31. Μια ακέραια περιοχή θα λέγεται περιοχή κύριων ιδεωδών όταν κάθε ιδεώδες της είναι κύριο.

Ορισμός I.7.32. Ένα σύνολο G θα λέγεται ομάδα αν είναι εφοδιασμένο με μία πράξη
$$\cdot : G \times G \to G$$
$$(g, g') \mapsto gg'$$
ώστε για κάθε g_1, g_2, g_3 να ισχύουν
$$g_1(g_2 g_3) = (g_1 g_2) g_3$$
Υπάρχει στοιχείο $e \in G$ ώστε για κάθε $g \in G$
$$eg = ge = g$$
Για κάθε στοιχείο $g \in G$ υπάρχει $g^{-1} \in G$ ώστε
$$gg^{-1} = g^{-1}g = e$$

Αν επιπλέον για κάθε $g, g' \in G$ ισχύει
$$gg' = g'g$$
τότε η ομάδα λέγεται αντιμεταθετική ή αβελιανή.

Παραδείγματα Ι.7.33. 1. Η πράξη + σε κάθε δακτύλιο R δίνει στον R δομή αβελιανής ομάδας.

2. Σε κάθε δακτύλιο R μπορούμε να ορίσουμε την *ομάδα των μονάδων* $U(R) = \{x \in R$ για τα οποία υπάρχει $x^{-1} \in R$ ώστε $xx^{-1} = 1\}$.

   Παρατηρούμε ότι $U(\mathbb{Z}) = \{\pm 1\}$. Επίσης $U(\mathbb{R}[x]) = \mathbb{R}^*$. Τέλος ιδιαίτερα ενδιαφέρουσα είναι η δομή της ομάδας $U\big((\mathbb{Z}/n\mathbb{Z})^*\big)$ η οποία έχει $\phi(n)$ το πλήθος στοιχεία.

Ορισμός Ι.7.34. Ένας αντιμεταθετικός δακτύλιος R με μοναδιαίο στοιχείο 1_R για τον οποίο ισχύει $U(R) = R - \{0\}$ θα λέγεται *σώμα*.

Ι.7.4 Δακτύλιος πηλίκο

Όπως ακριβώς κάναμε στους δακτυλίους $\mathbb{Z}/m\mathbb{Z}$ ορίζουμε για ένα ιδεώδες I τη σχέση ισοδυναμίας
$$a \sim b \Leftrightarrow b - a \in I.$$
Το ότι το παραπάνω είναι μια σχέση ισοδυναμίας είναι άμεσο από τις ιδιότητες του ιδεώδους. Ως μια σχέση ισοδυναμίας χωρίζει τον δακτύλιο σε μια ξένη ένωση κλάσεων ισοδυναμίας. Το σύνολο πηλίκο R/I αποτελείται από αυτές τις κλάσεις ισοδυναμίας.

Ένα τυχαίο στοιχείο του R/I αποτελείται από στοιχεία της μορφής
$$a + I = \{a + i, i \in I\},$$
ενώ εξ ορισμού $a + I = b + I$ αν και μόνο αν $a = b + i$ για κάποιο $i \in I$.

Θα δείξουμε ότι το R/I μπορεί να εφοδιαστεί με δομή δακτυλίου. Πράγματι, ορίζουμε το άθροισμα των κλάσεων
$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I)(b + I) = ab + I.$$
Οι παραπάνω πράξεις ορίστηκαν με βάση τους αντιπροσώπους των κλάσεων. Θα πρέπει να δείξουμε ότι είναι καλά ορισμένες, δηλαδή ανεξάρτητες των αντιπροσώπων που ορίζουν μια κλάση. Πράγματι, ας υποθέσουμε ότι $a + I = a' + I$ και $b + I = b' + I$, δηλαδή $a' = a + x$, $b' = b + y$ για κάποια στοιχεία $x, y \in I$. Θα πρέπει να δείξουμε ότι $a + b \sim a' + b'$ και ότι $ab \sim a'b'$. Πράγματι, το πρώτο ισχύει αφού $a' + b' = a + b + x + y$ και $x + y \in I$. Για το δεύτερο έχουμε
$$a'b' = (a + x)(b + y) = ab + xb + xy + ay,$$
και το ζητούμενο ισχύει αφού από τις ιδιότητες του ιδεώδους $xb + xy + ay \in I$.

Από τη στιγμή που έχουμε δείξει ότι οι πράξεις είναι καλά ορισμένες οι υπόλοιπες ιδιότητες του δακτυλίου κληρονομούνται από αυτές του R.

Η μονάδα του δακτυλίου R/I είναι το στοιχείο $1 + I$ ενώ το μηδενικό είναι το στοιχείο $0 + I$.

I.7.5 Ομομορφισμοί δακτυλίων

Μία συνάρτηση $\phi : R \to S$ θα λέγεται ομομορφισμός δακτυλίων αν για κάθε $x, y \in R$

$$\phi(x + y) = \phi(x) + \phi(y)$$

και

$$\phi(xy) = \phi(x)\phi(y).$$

Ένας ομομορφισμός που είναι *επί* θα λέγεται επιμορφισμός, ένας ομορφισμός που είναι *1-1* θα λέγεται μονομορφισμός και ένας μονομορφισμός που είναι ταυτόχρονα και επιμορφισμός θα λέγεται ισομορφισμός.

Ορισμός I.7.35. Θα ονομάζουμε *πυρήνα* ένος ομομορφισμού και θα το συμβολίζουμε με $\ker(\phi)$ το σύνολο:

$$\ker(\phi) = \{x \in R : \phi(x) = 0\}.$$

Θα ονομάζουμε *εικόνα* ενός ομομορφισμού τον υποδακτύλιο του S που αποτελείται από τα στοιχεία y για τα οποία υπάρχει $x \in R$ ώστε $y = \phi(x)$. Την εικόνα θα τη συμβολίζουμε με $\mathrm{Im}(\phi)$.

Παρατήρησεις

1. Ο πυρήνας ενός ομορφισμού είναι ιδεώδες του δακτυλίου R.
2. Ένας ομομορφισμός ϕ είναι μονομορφισμός αν και μόνο αν $\ker\phi = \{0\}$.
3. Εξ ορισμού η συνάρτηση

$$\pi : R \to R/I$$
$$x \mapsto x + I$$

είναι επιμορφισμός.

Θεώρημα I.7.36. *Θεωρούμε έναν ομομορφισμό $\phi : R \to S$ δακτυλίων. Υπάρχει μονομορφισμός*

$$\overline{\phi} : R/\ker\phi \to \mathrm{Im}(\phi) \subset S$$

ο οποίος ικανοποιεί επιπλέον $\overline{\phi} \circ \pi = \phi$. Οι δακτύλιοι $R/\ker(\phi)$ και $\mathrm{Im}(\phi)$ είναι ισόμορφοι.

Απόδειξη: Θεωρούμε το σύνολο R/I το οποίο αποτελείται από τις κλάσεις $x+\ker(\phi)$. Ορίζουμε

$$\overline{\phi}(x + I) = \phi(x).$$

Η συνάρτηση αυτή, αν είναι καλά ορισμένη, είναι ομομορφισμός και ικανοποιεί εκ κατασκευής την ιδιότητα $\overline{\phi} \circ \pi = \phi$.

Χρειάζεται να αποδείξουμε ότι είναι καλά ορισμένη γιατί την ορίσαμε με βάση τον αντιπρόσωπο της κλάσης και πρέπει να δείξουμε ότι είναι ανεξάρτητη του αντιπροσώπου.

Όμως, αν $x + \ker(\phi) = y + \ker(\phi)$, τότε $x = y + h$, όπου $h \in \ker(\phi)$. Άρα

$$\phi(x) = \phi(x + h) = \phi(x) + \phi(h) = \phi(x).$$

Τέλος, για να δείξουμε ότι η ϕ είναι μονομορφισμός παρατηρούμε ότι

$$\ker(\overline{\phi}) = \{x + \ker(\phi) : \phi(x) = 0\}$$

και αυτό σημαίνει ότι $x \in \ker\phi$, δηλαδή ο πυρήνας της $\overline{\phi}$ είναι το μηδενικό στοιχείο του δακτυλίου $R/\ker(\phi)$. □

Για τις ανάγκες αυτού του μαθήματος θα χρειαστούμε τους δακτυλίους $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου το F είναι ένα σώμα. Οι δακτύλιοι αυτοί μοιράζονται πολλές ιδιότητες και οι ομοιότητές τους ήταν μία από τις κινητήριες δυνάμεις στην ανάπτυξη της θεωρίας αριθμών και της αριθμητικής γεωμετρίας

Και στους δύο δακτυλίους υπάρχει ένα θεώρημα διαίρεσης με πηλίκο και υπόλοιπο.

Ι.8 Πολυώνυμα και αναλυτικές συναρτήσεις

Ορισμός Ι.8.1. Θεωρούμε την ακέραια περιοχή R. Ορίζουμε τον δακτύλιο $R[x]$ να έχει ως στοιχεία του τα πολυώνυμα, δηλαδή πεπερασμένα αθροίσματα

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^n,$$

όπου $a_\nu \in R$. Το μεγαλύτερο ν ώστε $a_\nu \neq 0$ ονομάζεται βαθμός του πολυωνύμου και θα το συμβολίζουμε με $\deg(f)$.

Το άθροισμα δύο πολυωνύμων $f(t) = \sum_{\nu=0}^{n} a_\nu x^n$ και $g(t) = \sum_{\nu=0}^{m} b_\nu x^n$ το ορίζουμε ως

$$f(t) + g(t) = \sum_{\nu=0}^{n} (a_\nu + b_\nu) x^n,$$

όπου αν $n < m$ θέσαμε $a\nu = 0$ για τα $\nu > n$.

Το γινόμενο δύο πολυωνύμων ορίζεται ως εξής:

$$f(t) \cdot g(t) = \sum_{\nu=0}^{n} \sum_{\mu=0}^{m} a_\nu b_\mu x^{\nu+\mu}$$

$$= \sum_{\nu=0}^{n+m} \sum_{\mu=0}^{\nu} a_\nu b_{\nu-\mu} x^\nu$$

Με $\mathbb{F}$ θα συμβολίζουμε ένα σώμα. Η συνάρτηση βαθμού

$$\deg : \mathbb{F}[x] - \{0\} \to \mathbb{N},$$

ικανοποιεί

$$\deg(f + g) \leq \max(\deg(f), \deg(g))$$

$$\deg(fg) = \deg(f) + \mathrm{def}(g). \tag{I.8}$$

Παρατηρήστε ότι δεν ορίζουμε τον βαθμό του μηδενικού πολυωνύμου.

Θεώρημα Ι.8.2.

1. *Για κάθε δύο στοιχεία $a, b \in \mathbb{Z}$ υπάρχουν στοιχεία $\pi, u \in \mathbb{Z}$ ώστε $a = b\pi + u$ με $0 \leq u < |b|$.*
2. *Για κάθε δύο στοιχεία $a, b \in \mathbb{F}[x]$ υπάρχουν στοιχεία $\pi, u \in \mathbb{F}[x]$ ώστε $a = b\pi + u$ με $u = 0$ ή $deg u < deg(b)$.*

Και στις δύο περιπτώσεις, τα στοιχεία π, u είναι μοναδικά.

Απόδειξη. Για την περίπτωση $a, b \in \mathbb{Z}$ πρώτα. Αν $b \mid a$ τότε το θεώρημα ισχύει με προφανή τρόπο. Διαφορετικά θεωρούμε το σύνολο

$$S = \{a - bt \geq 0 : t \in \mathbb{Z}\} \subset \mathbb{N}.$$

Το παραπάνω σύνολο είναι μη κενό. Πράγματι, αν $b < 0$ τότε ο $a - b|a| \geq 0$ ενώ αν $b > 0$ τότε ο $a - b(-|a|) \geq 0$. Το σύνολο S έχει ένα ελάχιστο στοιχείο $u = a - b\pi$ για κάποιο $\pi \in \mathbb{Z}$ σύμφωνα με το αξίωμα I.6.5. Ισχύει ότι $0 \leq u < |b|$. Πράγματι η πρώτη ανισότητα προκύπτει από τον ορισμό του u ενώ παρατηρούμε ότι αν $u \geq |b|$ τότε ο

$$0 \leq u - |b| = \begin{cases} u - b = a - b\pi - b = a - b(\pi + 1), & \text{αν } b > 0 \\ u + b = a - b\pi + b = a - b(\pi + 1), & \text{αν } b < 0 \end{cases}$$

είναι στοιχείο του S, μικρότερος του u, άτοπο. Για να αποδείξουμε την μοναδικότητα θεωρούμε ένα ακόμα ζευγάρι π', u' ώστε

$$a = b\pi' + u', \text{ με } 0 \leq u' < |b|.$$

Αφαιρώντας κατά μέλη καταλήγουμε στην σχέση

$$b(\pi - \pi') = u' - u. \tag{I.9}$$

Αν $\pi' \neq \pi$ τότε έχουμε

$$|b(\pi - \pi')| = |u' - u|$$

το οποίο είναι άτοπο, αφού

$$|u' - u| < b \leq |b(\pi^* - \pi).$$

Τέλος, παρατηρούμε ότι αν $\pi' = \pi$ τότε και $u' = u$, από την (I.9).

Τώρα θα μελετήσουμε την περίπτωση $a, b \in \mathbb{F}[x]$. Γράφουμε

$$a = a_0 + a_1 x + \cdots + a_n x^n \text{ και } b = b_0 + b_1 x + \cdots + b_m x^m,$$

με $a_n \neq 0$ και $b_m \neq 0$, δηλαδή $\deg a = n$ και $\deg b = m$. Αν $n < m$ τότε θέτουμε $\pi = 0$ και $u = a$. Υποθέτουμε ότι $n \geq m$. Αν $n = 0$ τότε θα πρέπει και $m = 0$ οπότε $a = bb_0^{-1}a$, δηλαδή $\pi = b_0^{-1}a$ και $u = 0$.

Υποθέτουμε ότι το θεώρημα ισχύει για όλα τα πολυώνυμα βαθμού μικρότερου του n και θεωρούμε το πολυώνυμο

$$a^* = a - a_n b_m^{-1} x^{n-m} b.$$

Είναι σαφές ότι $\deg a^* < \deg a = n$, συνεπώς υπάρχουν πολυώνυμα π^* και u ώστε

$$a^* = b\pi^* + u, \quad \deg u < \deg b.$$

Καταλήγουμε στο ότι

$$a = b(a_n b_m^{-1} x^{n-m} + \pi^*) + u,$$

δηλαδή

$$a = b\pi + u,$$

όπου $\pi = a_n b_m^{-1} x^{n-m} + \pi^*$.

Για να αποδείξουμε ότι τα στοιχεία π, u είναι μοναδικά θεωρούμε ότι υπάρχει ακόμα ένα ζευγάρι π', u', ώστε $a = \pi' b + u'$ με $\deg u' < \deg b$. Καταλήγουμε στο ότι

$$b(\pi - \pi') = u' - u.$$

Αν ισχύει ότι $\pi' \neq \pi$. Έχουμε τώρα ότι

$$\deg b(\pi - \pi') \geq \deg b,$$

το οποίο είναι άτοπο αφού ισχύει ότι

$$\deg b(\pi - \pi') = \deg(u' - u) < \deg b.$$

Συνεπώς $\pi' = \pi$ και έχουμε ότι και $u' = u$. □

Άμεση εφαρμογή του παραπάνω Θεωρήματος είναι το

Θεώρημα Ι.8.3. *Κάθε ιδεώδες του δακτυλίου $\mathbb{Z}$ ή $\mathbb{F}[x]$ είναι κύριο.*

Απόδειξη Αν έχουμε ένα ιδεώδες του $\mathbb{Z}$ το οποίο είναι μη μηδενικό, τότε έχει ένα στοιχείο που είναι θετικό. Θεωρούμε το ελάχιστο στοιχείο n του μη κενού συνόλου των θετικών στοιχείων του ιδεώδους I. Κάθε στοιχείο a του I είναι πολλαπλάσιο του n. Αυτό γιατί αν γράψουμε το τυχαίο στοιχείο $a \in I$ ως

$$a = \pi n + u, 0 \leq u < n,$$

τότε το $u \in I$ και συνεπώς είναι μηδενικό, αλλιώς το n δεν θα ήταν το ελάχιστο θετικό στοιχείο του ιδεώδους.

Στην περίπτωση που το I δεν είναι μηδενικό ιδεώδες του δακτυλίου $\mathbb{F}[x]$ θα έχει ένα στοιχείο g ελαχίστου βαθμού. Κάθε στοιχείο $a \in I$ είναι αναγκαστικά πολλαπλάσιο του g. Σε διαφορετική περίπτωση γράφουμε

$$a = g\pi + u, \deg(u) < \deg(g)$$

και αφού το $u \in I$, καταλήγουμε σε άτοπο (το g κατασκευάστηκε να είναι ελαχίστου βαθμού στο ιδεώδες). □

Ι.8.1 Μέγιστος κοινός διαιρέτης - Ελάχιστο κοινό πολλαπλάσιο

Η διαίρεση στους ακεραίους είναι ένα από τα αντικείμενα μελέτης της θεωρίας αριθμών. Θα δούμε ότι τα πολυώνυμα $\mathbb{F}[x]$ πάνω από ένα σώμα $\mathbb{F}$, έχουν παρόμοιες ιδιότητες.

Παρατηρούμε ότι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$, δηλαδή τα στοιχεία $a \in \mathbb{Z}$ ώστε να υπάρχει ένα στοιχείο $a' \in \mathbb{Z}$, είναι τα ± 1. Πράγματι, αν $a \in \mathbb{Z}$ και $|a| > 1$, τότε $0 < |1/a| < 1$ και συνεπώς $1/a \notin \mathbb{Z}$. Παρομοίως, τα αντιστρέψιμα στοιχεία στον δακτύλιο $\mathbb{F}[x]$, είναι τα σταθερά πολυώνυμα $c \in \mathbb{F}\backslash\{0\}$. Πράγματι, παρατηρούμε ότι αν $f(x) \in \mathbb{F}[x]$ και $\deg f > 1$ αντιστρέψιμο στοιχείο, δηλαδή υπάρχει $g \in \mathbb{F}[x]$ ώστε $gf = 1$ τότε από τον τύπο I.8 έχουμε $\deg(f) + \deg(g) = 0$, δηλαδή $\deg(g) < -1$, άτοπο.

Παρατηρούμε ότι για κάθε ακέραιο a υπάρχει ένα αντιστρέψιμο στοιχείο $c \in \{\pm 1\}$, ώστε $ca \in \mathbb{N}$. Για τα πολυώνυμα μπορούμε να ορίσουμε ως ανάλογο των φυσικών τα *μονικά πολυώνυμα*.

Ορισμός Ι.8.4. Ένα πολυώνυμο $f(x) \in \mathbb{F}[x]$ θα λέγεται μονικό αν ο συντελεστής του μεγιστοβάθμιου όρου του είναι ίσος με 1, δηλαδή ένα πολυώνυμο της μορφής:

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i.$$

Παρατηρούμε ότι ένα τυχαίο πολυώνυμο βαθμού n $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ γίνεται μονικό αν πολλαπλασιαστεί με a_n^{-1}.

Ορισμός Ι.8.5. Θεωρούμε τους ακέραιους a, b. Θα ονομάζουμε μέγιστο κοινό διαιρέτη των a, b και θα τον συμβολίζουμε με (a, b), έναν φυσικό αριθμό d ο οποίος ικανοποιεί:

1. $d \mid a$ και $d \mid b$
2. Αν $\delta \mid a$ και $\delta \mid b$ τότε $\delta \mid d$.

Αντίστοιχα στα πολυώνυμα $\mathbb{F}[x]$ θεωρούμε τον αντίστοιχο ορισμό:

Ορισμός I.8.6. Θεωρούμε τα πολυώνυμα $a, b \in \mathbb{F}[x]$. Θα ονομάζουμε μέγιστο κοινό διαιρέτη των a, b και θα τον συμβολίζουμε με (a, b), ένα μονικό πολυώνυμο d το οποίος ικανοποιεί:

1. $d \mid a$ και $d \mid b$
2. Αν $\delta \mid a$ και $\delta \mid b$ τότε $\delta \mid d$.

Παρατήρηση I.8.7. Παρατηρούμε ότι αν θεωρήσουμε το ιδεώδες I του δακτυλίου $R = \mathbb{Z}$ ή του $R = \mathbb{F}[x]$ που παράγεται από τα στοιχεία $a, b \in R$, δηλαδή το σύνολο $I = \{xa + yb : x, y \in R\}$ αυτό το ιδεώδες είναι κύριο δηλαδή $I = d'R$. Ο μέγιστος κοινός διαιρέτης είναι το $d = |d'|$ αν $R = \mathbb{Z}$ ή το μονικό πολυώνυμο d που αντιστοιχεί στο d', αν $R = \mathbb{F}[x]$. Και στις δύο περιπτώσεις $d = cd'$, όπου το d είναι αντιστρέψιμο στοιχείο του R. Παρατηρούμε ότι τα $a, b \in I$ και συνεπώς $d|a$, $d|b$. Επίσης αν $\delta \mid a$, $\delta \mid b$, τότε αφού $d \in I$, το d γράφεται ως

$$d = x_0 a + y_0 b \tag{I.10}$$

για κάποια $x_0, y_0 \in R$, συνεπώς $\delta|d$.

Λήμμα I.8.8. *Θεωρούμε την διαίρεση με πηλίκο και υπόλοιπο:*

$$a = b\pi + u$$

Ισχύει ότι ο μέγιστος κοινός διαιρέτης (a, b) των a, b είναι ίσος με τον μέγιστο κοινό διαιρέτη (b, u) των b, u.

Απόδειξη. Παρατηρούμε ότι $d \mid a, b$ αν και μόνο αν $d \mid b, u$. □

Με βάση το παραπάνω προκύπτει ο παρακάτω αλγόριθμος ο οποίος είναι γνωστός ως αλγόριθμος του Ευκλείδη ο οποίος έχει ως είσοδο $a, b \in R$, όπου $R = \mathbb{Z}$ ή $R = \mathbb{F}[x]$ και βάζει ως έξοδο τον μέγιστο κοινό διαιρέτη d αλλά και στοιχεία $x_0, y_0 \in R$ ώστε $d = x_0 a + y_0 b$.

Μέθοδος 1 (Εύρεση μέγιστου κοινού διαιρέτη)**.** *Εκτελούμε τα παρακάτω βήματα:*

1. *Εκτελούμε την διαίρεση με πηλίκο και υπόλοιπο $a = b\pi_1 + u_1$. Συμβολίζουμε με $a_1 = a, b_1 = b$.*
2. *Αν $u_1 = 0$ ο μέγιστος κοινός διαιρέτης των a, b είναι το b. Αν όχι θέτουμε $a_2 = b, b_2 = u$ και εκτελούμε την διαίρεση με πηλίκο και υπόλοιπο $a_2 = b_2\pi_2 + u_2$.*
3. *Αν $u_2 = 0$ ο μέγιστος κοινός διαιρέτης των a_2, b_2 είναι το b_2. Επίσης $(a_2, b_2) = (a_1, b_1)$. Αν $u_2 \neq 0$ θέτουμε $a_3 = b_2$ και $b_3 = u_2$.*
4. *Συνεχίζουμε αναδρομικά μέχρι να βρούμε ένα υπόλοιπο $u_{n+1} = 0$, οπότε ο μέγιστος κοινός διαιρέτης είναι το u_n.*

5 *Έχουμε την ακολουθία*

$$\begin{aligned} a &= b\pi_1 + u_1 \\ b &= u_1\pi_2 + u_2 \\ u_1 &= u_2\pi_3 + u_3 \\ &\cdots\cdots \\ u_{n-2} &= u_{n-1}\pi_{n+1} + u_n \\ u_{n-1} &= u_n\pi_{n+2} + 0 \end{aligned}$$

Για να υπολογίσουμε τους x_0, y_0 *ξεκινάμε ανάποδα γράφοντας* $u_n = u_{n-2} - u_{n-1}\pi_{n+1}$ *και ανεβαίνουμε προς τα πάνω βήμα βήμα κάνοντας αντικαταστάσεις.*

Θα δώσουμε ένα παράδειγμα εφαρμογής του αλγορίθμου του Ευκλείδη όταν το $R = \mathbb{F}[x]$. Για παραδείγματα όταν το $R = \mathbb{Z}$ δείτε ένα βιβλίο θεωρίας αριθμών, για παράδειγμα [17, 1.1.6].

Παράδειγμα Ι.8.9. Να βρεθεί ο μέγιστος κοινός διαιρέτης των $a = 4x^3+12x^2+10x+2$, $b = 2x^2+4x+2$. Στην συνέχεια να υπολογιστούν $x_0, y_0 \in \mathbb{Q}[x]$ ώστε $(a, b) = x_0a + y_0b$.

Αρχικά κατασκευάζουμε μια ακολουθία διαιρέσεων με πηλίκο και υπόλοιπο

$$\begin{aligned} 4x^4 + 12x^2 + 10x + 2 &= (2x^2 + 4x + 2)(2x^2 - 4x + 12) + (-30x - 22) \\ 2x^2 + 4x + 2 &= (-30x - 22)(-\frac{x}{15} - \frac{19}{225}) + \frac{32}{225} \\ -\frac{x}{15} - \frac{19}{225} &= \frac{32}{225}(-\frac{15x}{32} - \frac{19}{32}) + 0 \end{aligned}$$

Το ελάχιστο κοινό πολλαπλάσιο είναι το $32/225$, το οποίο αντιστοιχεί στο μονικό πολυώνυμο 1 το οποίο είναι ο μέγιστος κοινός διαιρέτης.

Για να υπολογίσουμε τα x_0, y_0 ξεκινάμε από την προτελευταία σχέση

$$1 = b\frac{225}{32} - (30x + 22)\left(\frac{x}{15} + \frac{19}{225}\right)\frac{225}{32}$$

στην οποία αντικαθιστούμε την τιμή του $30x + 22 = -a + b(2x^2 - 4x + 12)$ από την πρώτη σχέση για να καταλήξουμε στην

$$1 = a\left(\frac{15x}{32} + \frac{19}{32}\right) + b\left(-\frac{15x^3}{16} + \frac{11x^2}{16} - \frac{13x}{4} - \frac{3}{32}\right).$$

Ο **Ευκλείδης** (300 π.Χ.)

ήταν αρχαίος Έλληνας Μαθηματικός που δραστηριοποιήθηκε στην Γεωμετρία, στην Θεωρία Αριθμών και στη Λογική. Θεωρείται ο πατέρας της Γεωμετρίας και είναι γνωστός για τα «Στοιχεία» του τα οποία καθόρισαν την Γεωμετρία για τους επόμενους αιώνες. Θεωρείται ένας από τους μεγαλύτερους Μαθηματικούς της αρχαιότητας.

Στα «Στοιχεία» ο Ευκλείδης θεμελίωσε τα Μαθηματικά ως ένα αυστηρά δομημένο και συνεκτικό σύστημα προτάσεων με βάση ένα σύνολο ορισμών, κοινών εννοιών και 5 μόνο αρχικών αναπόδεικτων προτάσεων (αιτήματα). Στο βιβλίο αυτό εμφανίζονται έννοιες και από τα σύγχρονα Μαθηματικά. Αντιγράφοντας από τους συγγραφείς της εξαιρετικής απόδοσης των «Στοιχείων» σε σύγχρονη ορολογία από τους Νίκο Ροκοπάνο, Στέλλα Σακελλάρη και Αντώνη Τσολομύτη [23]: « *....Στο κείμενο θα βρεις Προτάσεις που σίγουρα θα σε εκπλήξουν. Χαρακτηριστικό παράδειγμα είναι η Πρόταση 1 στο Βιβλίο 10, σελ. 229 στην οποία ο Ευκλείδης σε μία πρόταση εισάγει τις κεντρικότερες έννοιες της ανάλυσης, όπως όριο με έψιλον επιχείρημα, σειρές και άπειρες διαδικασίες. Πολλοί θα πουν «εννοείτε ότι ο Ευκλείδης ήξερε όρια;». Εμείς λέμε ότι αυτή είναι η λάθος ερώτηση. Η σωστή ερώτηση είναι αν ο Bolzano που χρησιμοποίησε την έννοια του ορίου στα γραπτά του, αν ο Cauchy που έγραψε αποδείξεις με αυτό στο Cours d Analyse, και τέλος αν ο Weierstrass που έδωσε τον ε-ορισμό για το όριο, είχαν ή όχι διαβάσει τα Στοιχεία; Και αν στο έργο τους έχουν τις πρέπουσες αναφορές; Και αν τις έχουν γιατί εμείς δεν τις πληροφορηθήκαμε ποτέ; Και το ίδιο ισχύει για σειρά άλλων θεμάτων όπως ο ορισμός των πραγματικών αριθμών με τις «τομές Dedekind» της σύγχρονης εποχής, το ολοκλήρωμα Riemann και πολλά άλλα. Ή μήπως τα Στοιχεία ήταν απλώς κλειδωμένα στις διάφορες βιβλιοθήκες και υπόγεια μοναστηριών, ευ πολλοίς ανυπεράσπιστα, και παραμένουν στην αφάνεια για τη σύγχρονη Μαθηματική κοινότητα;....»*

Ορισμός I.8.10. Θεωρούμε τα στοιχεία $a, b \in \mathbb{Z}$. Θα ονομάζουμε ελάχιστο κοινό πολλαπλάσιο των a, b και θα τον συμβολίζουμε με $[a, b]$, έναν φυσικό αριθμό m το οποίο ικανοποιεί:

1. $a \mid m$ και $b \mid m$
2. Αν $a \mid \mu$ και $b \mid \mu$ τότε $m \mid \mu$.

Αντίστοιχα στα πολυώνυμα $\mathbb{F}[x]$ θεωρούμε τον αντίστοιχο ορισμό:

Ορισμός I.8.11. Θεωρούμε τα πολυώνυμα $a, b \in \mathbb{F}[x]$. Θα ονομάζουμε ελάχιστο κοινό πολλαπλάσιο των a, b και θα το συμβολίζουμε με $[a, b]$, ένα μονικό πολυώνυμο m το οποίο ικανοποιεί:

1. $a \mid m$ και $b \mid m$
2. Αν $a \mid \mu$ και $b \mid \mu$ τότε $m \mid \mu$.

I.8.2 Ανάγωγα πολυώνυμα

Ορισμός Ι.8.12. Κάθε πολυώνυμο $f(x)$ ορίζει μια συνάρτηση

$$\begin{aligned} ev_a : \mathbb{F}[x] &\longrightarrow \mathbb{F} \\ f(x) &\longrightarrow f(a) \end{aligned}$$

Παρατήρηση Ι.8.13. Παρατηρούμε ότι το $f(a) \in \mathbb{F}$ είναι το υπόλοιπο της διαίρεσης του $f(x)$ με το $x - a$. Πράγματι

$$f(x) = p(x)(x-a) + u, \text{ όπου } u \in \mathbb{F}$$

και $f(a) = p(a)(a-a) + u$ από όπου προκύπτει ότι $f(a) = u$.

Πόρισμα Ι.8.14. *Το $a \in \mathbb{F}$ είναι ρίζα του $f(x) \in \mathbb{F}[x]$ αν και μόνο αν $(x-a) \mid f(x)$.*

Ορισμός Ι.8.15. Ένας φυσικός αριθμός $p > 1$ λέγεται πρώτος αν οι μοναδικοί φυσικοί διαιρέτες του είναι ο εαυτός του και το 1. Ένα μονικό μη σταθερό πολυώνυμο p θα λέγεται πρώτο αν οι μοναδικοί μονικοί διαιρέτες του είναι ο εαυτός του και η μονάδα.

Ένας ακέραιος $p \in \mathbb{Z}$ θα λέγεται ανάγωγος αν μοναδικοί διαιρέτες του είναι στοιχεία της μορφής c, cp με $c \in \{\pm 1\}$. Ένα μη σταθερό πολυώνυμο $p \in \mathbb{F}[x]$ θα λέγεται ανάγωγο αν οι μοναδικοί διαιρέτες του είναι στοιχεία της μορφής c, cp, με $c \in \mathbb{F}\backslash\{0\}$.

Η μελέτη των πρώτων αριθμών είναι ένα κομμάτι της θεωρίας των αριθμών.

Λήμμα Ι.8.16. *Αν ένας πρώτος $p \in R$, $R = \mathbb{Z}$ ή $R = \mathbb{F}[x]$ και $p \mid a, b$ τότε $p \mid a$ ή $p \mid b$.*

Απόδειξη. Αν $p \mid a$ τότε το αποτέλεσμα είναι σαφές. Αν όχι τότε $(a, p) = 1$ συνεπώς υπάρχουν $x, y \in R$ με $xa + yp = 1$. Πολλαπλασιάζουμε την τελευταία σχέση με b και έχουμε $ab + ypb = b$ από όπου προκύπτει το ζητούμενο. □

Πρόταση Ι.8.17. *Κάθε $a \in \mathbb{Z}, a \neq 0$ γράφεται με μονοσήμαντο τρόπο ως γινόμενο πρώτων $p_1, \ldots, p_s$ επί $c \in \{\pm 1\}$:*

$$a = cp_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}, \qquad n_1, \ldots, n_s \in \mathbb{N}.$$

Κάθε πολυώνυμο $a \in \mathbb{F}[x], a \neq 0$ γράφεται με μονοσήμαντο τρόπο ως γινόμενο πρώτων, δηλαδή αναγώγων μονικών πολυωνύμων, $p_1, \ldots, p_s$, επί ένα $c \in \mathbb{F}\backslash\{0\}$

$$a = cp_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}, \qquad n_1, \ldots, n_s \in \mathbb{N}.$$

Απόδειξη. Η απόδειξη θα γίνει και στις δύο περιπτώσεις με επαγωγή.

Για την περίπτωση των ακεραίων θα κάνουμε επαγωγή στο $|a|$. Αν $|a| = 1$ τότε το ζητούμενο ισχύει (όλα τα $n_1, \ldots, n_s$ είναι μηδενικά). Έστω ότι το ζητούμενο ισχύει για όλους τους ακέραιους a με $|a| < n$. Θεωρούμε ένα a, με $|a| = n$. Μπορούμε να υποθέσουμε ότι για $c \in \{\pm 1\}$ $a = ca'$ με $a' \in \mathbb{N}$. Αν το a' είναι ανάγωγο τότε τελειώσαμε. Αν όχι τότε εξ ορισμού υπάρχει γνήσιος διαιρέτης b, με $b \mid a'$. Έχουμε $a' = bb'$ με $0 < b, b' < a$. Το ζητούμενο της ανάλυσης σε πρώτους προκύπτει από την επαγωγική υπόθεση.

Για την περίπτωση των πολυωνύμων θα κάνουμε επαγωγή στο $\deg a$. Αν $\deg a = 0$ τότε το ζητούμενο ισχύει (όλα τα $n_1, \ldots, n_s$ είναι μηδενικά). Έστω ότι το ζητούμενο ισχύει για όλα τα

πολυώνυμα a με $\deg a < n$. Θεωρούμε ένα a, με $\deg a = n$. Μπορούμε να υποθέσουμε ότι για $c \in \mathbb{F}\backslash\{0\}$, $a = ca'$ με a' μονικό. Αν το a' είναι ανάγωγο τότε τελειώσαμε. Αν όχι τότε εξ ορισμού υπάρχει γνήσιος διαιρέτης b, με $b \mid a'$. Έχουμε $a' = bb'$ με $\deg b, \deg b' < n$. Το ζητούμενο της ανάλυσης σε πρώτους προκύπτει από την επαγωγική υπόθεση.

Για το μονοσήμαντο της ανάλυσης υποθέτουμε ότι

$$a = cp_1^{a_1} \cdot p_s^{a_s} = c' q_1^{b_1} \cdots q_r^{b_r}$$

δύο διαφορετικές αναλύσεις του a σε γινόμενο πρώτων του R, με c, c' αντιστρέψιμα στοιχεία του R. Υποθέτουμε ότι $s \leq r$. Ο πρώτος p_1 διαιρεί το γινόμενο στο δεξί μέρος και άρα διαιρεί κάποιον από τους q_i και συνεπώς ταυτίζεται με αυτόν. Διαγράφουμε τους πρώτους p_1, q_i και συνεχίζουμε με τον ίδιο τρόπο μέχρι να εξαντληθούν οι πρώτοι στο αριστερό μέρος. Επειδή το γινόμενο πρώτων δεν μπορεί να είναι αντιστρέψιμο στοιχείο ταυτόχρονα θα εξαντληθούν οι πρώτοι και στο δεξί μέρος, οπότε προκύπτει το ζητούμενο. □

Παρατήρηση I.8.18. Κάθε πολυώνυμο βαθμού 1 είναι ανάγωγο. Πράγματι αν ένα πολυώνυμο p βαθμού ένα έχει διάσπαση $p = ab$ τότε θα έπρεπε $1 = \deg p = \deg a + \deg b$, συνεπώς ένα από τα a, b είναι μη μηδενική σταθερά.

Το αντίστροφο δεν είναι αληθές αφού για παράδειγμα το $x^2 + 1 \in \mathbb{R}[x]$ δεν έχει διάσπαση ως γινόμενο πολυωνύμων του $\mathbb{R}[x]$ μικρότερου βαθμού. Πράγματι μια τέτοια διάσπαση $x^2 + 1 = ab$ όπου $\deg a = \deg b = 1$ θα είχε ως αποτέλεσμα ότι το πολυώνυμο αυτό έχει μια πραγματική ρίζα.

Πρόταση I.8.19. *Τα ανάγωγα μονικά πολυώνυμα του $\mathbb{C}[x]$ είναι αυτά της μορφής $x - \rho$, για $\rho \in \mathbb{C}$. Τα ανάγωγα μονικά πολυώνυμα του $\mathbb{R}[x]$ είναι της μορφής x^2+bx+c, με $b, c \in \mathbb{R}$, $b^2-4c < 0$ ή της μορφής $x - \rho$ για $x \in \mathbb{R}$.*

Απόδειξη. Παρατηρούμε ότι σύμφωνα με το θεώρημα I.6.29, κάθε πολυώνυμο $f(x) \in \mathbb{C}[x]$ έχει μία ρίζα, έστω $\rho \in \mathbb{C}$ άρα είναι διαιρετά με το $x - \rho$. Άρα κάθε ανάγωγο μονικό είναι της μορφής $x - \rho$.

Ένα πραγματικό πολυώνυμο $f(x)$ αν θεωρηθεί ως πολυώνυμο στο $\mathbb{C}[x]$ έχει μια ανάλυση σε γινόμενο αναγώγων μονικών πολυωνύμων του $\mathbb{C}[x]$, δηλαδή μια ανάλυση της μορφής:

$$f(x) = c \prod_{i=1}^{n} (x - \rho_i).$$

Σύμφωνα με την άσκηση I.22 οι παραπάνω ρίζες είναι ή πραγματικές ή ζευγάρια διαφορετικών μιγαδικών ριζών, $\rho = a + ib, \overline{\rho} = a - ib$, $a, b \in \mathbb{R}$. Παρατηρούμε ότι ένα τέτοιο ζευγάρι δίνει

$$(x - \rho)(x - \overline{\rho}) = x^2 + (\rho + \overline{\rho})x + \rho\overline{\rho} = x^2 + 2ax + (a^2 + b^2) \in \mathbb{R}[x].$$

Άρα ένα μονικό ανάγωγο πολυώνυμο με πραγματικούς συντελεστές αν έχει μια μιγαδική ρίζα είναι ένα τετραγωνικό πολυώνυμο αρνητικής διακρίνουσας. □

Παρατήρηση I.8.20. Τα ανάγωγα πολυώνυμα του $\mathbb{Q}[x]$ είναι αρκετά πολύπλοκα και η μελέτη τους αποτελεί σημαντικό κομμάτι της αλγεβρικής θεωρίας αριθμών [20]. Αυτά μπορεί να έχουν οσοδήποτε μεγάλο βαθμό, για παράδειγμα για κάθε πρώτο p το πολυώνυμο $1 + x + x^2 + \cdots + x^{p-1} \in \mathbb{Q}[x]$ είναι ανάγωγο, [18, σελ. 37], [20, VI.6.3].

Πρόταση I.8.21. *Για δύο στοιχεία $a, b \in R$, $R = \mathbb{Z}$ ή $R = \mathbb{F}[x]$ με*

$$a = cp_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} \quad b = c' p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s}$$

ισχύει ότι

$$(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_s^{\min(a_s,b_s)}$$
$$[a,b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_s^{\max(a_s,b_s)}$$

Απόδειξη. Παρατηρούμε ότι κάθε γινόμενο πρώτων $p_1^{\nu_1} \cdots p_s^{\nu_s}$ που οι εκθέτες $\nu_i < a_i, b_i$ για $1 \le i \le s$ είναι κοινός διαιρέτης των a, b. Ο μέγιστος κοινός διαιρέτης προκύπτει όταν το ν_i πάρει την μέγιστη τιμή που είναι μικρότερη και από τους δύο δηλαδή το $\min(a_i, b_i)$.

Ομοίως κάθε γινόμενο πρώτων $p_1^{\nu_1} \cdots p_s^{\nu_s}$ που οι εκθέτες $\nu_i > a_i, b_i$ για $1 \le i \le s$ είναι κοινό πολλαπλάσιο των a, b. Το ελάχιστο κοινό πολλαπλάσιο προκύπτει όταν το ν_i πάρει την ελάχιστη τιμή που είναι μεγαλύτερη και από τους δύο δηλαδή το $\max(a_i, b_i)$. □

Πόρισμα Ι.8.22. *Θα συμβολίζουμε με $|a|$ την απόλυτη τιμή του a αν $a \in \mathbb{Z}$ και με $|a|$ το μονικό πολυώνυμο που αντιστοιχεί στο πολυώνυμο a αν $a \in \mathbb{F}[x]$ Ισχύει ότι*

$$|a \cdot b| = (a,b)[a,b].$$

Απόδειξη. Παρατηρούμε ότι $a_i + b_i = \max(a_i, b_i) + \min(a_i, b_i)$. Τα αντιστρέψιμα στοιχεία c, c' μπροστά στα στοιχεία a, b δεν εμφανίζονται στον μέγιστο κοινό διαιρέτη και στο ελάχιστο κοινό πολλαπλάσιο τα οποία είναι εξ ορισμού μονικά οπότε θα πρέπει να φύγουν και από το γινόμενο των a, b. □

Στον παρακάτω πίνακα παραθέτουμε τις ομοιότητες ανάμεσα στους δακτύλιους $\mathbb{Z}$ και $\mathbb{F}[x]$

Δακτύλιος	Αντιστρέψιμα	θετικοί	Αδιάσπαστα στοιχεία
$\mathbb{Z}$	$\{\pm 1\}$	$\mathbb{N}$	Πρώτοι αριθμοί
$\mathbb{F}[x]$	$\mathbb{F}\backslash\{0\}$	μονικά πολυώνυμα	Ανάγωγα μονικά

Πίσω από αυτή την ομοιώτητα κρύβεται η έννοια του Ευκλείδιου δακτύλιου, δείτε [12, 4.6]

Ασκήσεις

Άσκηση Ι.22 Δείξτε ότι αν ένα πολυώνυμο $f(x) \in \mathbb{R}[x]$ έχει μια ρίζα $\rho \in \mathbb{C}$, τότε έχει και την συζυγή της.

Ι.8.3 Χαρακτηριστική δακτυλίου

Παρατήρηση Ι.8.23. Αν ένα σύνολο Σ παράγει τον δακτύλιο R και δεν υπάρχουν αλγεβρικές σχέσεις μεταξύ των στοιχείων του Σ, δηλαδή κάθε στοιχείο του R μπορεί να γραφεί με μοναδικό τρόπο ως αποτέλεσμα των δύο πράξεων του δακτυλίου με πράξεις μεταξύ των στοιχείων του Σ, τότε κάθε συνάρτηση $\phi : \Sigma \to S$ μπορεί να επεκταθεί σε ομομορφισμό $\phi : R \to S$.

Περισσότερο συγκεκριμένα ένας μη μηδενικός ομομορφισμός $\mathbb{Z} \to S$ προσδιορίζεται μονοσήμαντα αν γνωρίζουμε το $\phi(1)$ το οποίο στην περίπτωση που ο S είναι ακέραια περιοχή δεν μπορεί να είναι άλλο από το μοναδιαίο του S. Πράγματι

$$\phi(1_{\mathbb{Z}}) = \phi(1_{\mathbb{Z}} \cdot 1_{\mathbb{Z}}) = \phi(1_{\mathbb{Z}})\phi(1_{\mathbb{Z}})$$

Δηλαδή

$$\phi(1_{\mathbb{Z}})(1_S - \phi(1_{\mathbb{Z}})) = 0$$

από όπου προκύπτει το ζητούμενο.

Ορισμός I.8.24. Έστω S δακτύλιος αντιμεταθετικός με μοναδιαίο θεωρούμε τον ομομορφισμό

$$\phi : \mathbb{Z} \to S$$

$$1_{\mathbb{Z}} \mapsto 1_S.$$

Ο πυρήνας είναι ένα κύριο ιδεωδές του $\mathbb{Z}$, δηλαδή $\ker(\phi) = n\mathbb{Z}$. Τον αριθμό n θα τον λέμε χαρακτηριστική του δακτυλίου S.

Παρατηρήσεις:

1. Αν ο πυρήνας του ϕ είναι μηδενικός, τότε ο δακτύλιος S έχει χαρακτηριστική 0 και σε αυτή την περίπτωση ο δακτύλιος S είναι άπειρος.
2. Από το θεώρημα ισομορφισμού ο $\mathbb{Z}/n\mathbb{Z}$ είναι ένας υποδακτύλιος του S. Αν ο S είναι ακέραια περιοχή, τότε αναγκαστικά n είναι πρώτος αριθμός.
3. Κάθε πεπερασμένο σώμα περιέχει το $\mathbb{Z}/p\mathbb{Z}$ για κάποιο πρώτο p ως υπόσωμα.

Ορισμός I.8.25. Ένα ιδεώδες P του δακτυλίου R θα λέγεται πρώτο αν και μόνο αν για κάθε $a, b \in R$
$ab \in P$ συνεπάγεται $a \in P$ είτε $b \in P$.
Το ιδεώδες M θα λέγεται μέγιστο αν κάθε ιδεώδες I του R ώστε $M \subset I$ επιβάλλει $I = R$ ή $I = M$.

Θεώρημα I.8.26. *Ένα ιδεώδες P είναι πρώτο αν και μόνο αν ο δακτύλιος R/P είναι ακέραια περιοχή.*

Απόδειξη Θεωρούμε το γινόμενο $(a + P)(b + P) = ab + P$. Παρατηρούμε ότι $ab \in P$ είναι ισοδύναμο με το $ab+P = 0_{R/P}$ είναι 0 στον δακτύλιο R/P. Ομοίως $a+P = 0_{R/P}$ (αντίστοιχα $b+P = 0_{R/P}$) είναι ισοδύναμο με $a \in P$ (αντίστοιχα $b \in P$). Το ζητούμενο είναι σαφές από τον ορισμό της ακέραιας περιοχής. □

Θεώρημα I.8.27. *Ένα ιδεώδες M είναι μέγιστο αν και μόνο αν ο δακτύλιος R/M είναι σώμα.*

Απόδειξη. Ας υποθέσουμε ότι το M είναι ένα μέγιστο ιδεώδες. Η κλάση $x + M$ είναι μη μηδενική κλάση αν και μόνο αν $x \notin M$. Σε αυτή την περίπτωση το ιδεώδες $M + xR$, που παράγεται από τα στοιχεία του M και το x είναι ένα ιδεώδες που περιέχει γνήσια το M.

Στην περίπτωση που το M είναι μέγιστο το $M + xR$ είναι όλος ο δακτύλιος R άρα το μοναδιαίο 1_R του δακτυλίου γράφεται ως $1_R = m + xa$ για κάποια στοιχεία $m \in M$ και $a \in R$. Αυτό όμως σημαίνει ότι $(a + M)(x + M) = 1 + M$, άρα η τυχαία μη μηδενική κλάση $x + M$ είναι αντιστρέψιμη και το R/M είναι σώμα.

Αντιστρόφως, έστω ότι R/M είναι σώμα. Αν το M περιέχεται γνήσια σε ένα ιδεώδες I, τότε το I περιέχει ένα στοιχείο $x \notin M$, και συνεπώς η κλάση $x + M$ είναι αντιστρέψιμη, δηλαδή υπάρχει $a \in R$ ώστε $(x + M)(a + M) = 1 + M$. Η τελευταία σχέση είναι ισοδύναμη με το ότι $xa = 1_R + m$ για κάποιο στοιχείο $m \in M$. Τότε όμως το $1_R = xa - m$ είναι στοιχείο του I και συνεπώς $I = R$. □

Παρατηρήσεις

1. Το ιδεώδες $p\mathbb{Z}$ για p πρώτο αριθμό είναι πρώτο και μέγιστο ιδεώδες του $\mathbb{Z}$.
2. Αν f είναι ένα ανάγωγο πολυώνυμο του $\mathbb{F}[x]$, τότε το ιδεώδες $f(x)\mathbb{F}[x]$ είναι και πρώτο και μέγιστο.
3. Το μηδενικό ιδεώδες είναι πρώτο αν και μόνο αν ο δακτύλιος R είναι ακέραια περιοχή.
4. Κάθε μέγιστο ιδεώδες είναι πρώτο.
5. Υπάρχουν πρώτα ιδεώδη που δεν είναι μέγιστα όπως το $p\mathbb{Z}[x] \subset \mathbb{Z}[x]$ ή το $x\mathbb{F}[x,y] \subset \mathbb{F}[x,y]$.

Ι.8.4 Σχέσεις ριζών συντελεστών

Στοιχειώδη συμμετρικά πολυώνυμα, τύποι του Newton

Ορισμός Ι.8.28 (Στοιχειώδη συμμετρικά πολυώνυμα)**.** Το k στοιχειώδες συμμετρικό πολυώνυμο σε n-μεταβλητές ορίζεται ως

$$e_k(z_1,\dots,z_n) = \sum_{1\le i_1<\cdots<i_k\le n} .z_{i_1}\cdots z_{i_k}.$$

Είναι αναλλοίωτο κάτω από τις μεταθέσεις των μεταβλητών.

Παράδειγμα Ι.8.29. Σε 4 μεταβλητές τα στοιχειώδη συμμετρικά πολυώνυμα είναι τα

$$\begin{aligned}
e_0(z_1,z_2,z_3,z_4) &= 1\\
e_1(z_1,z_2,z_3,z_4) &= z_1+z_2+z_3+z_4\\
e_2(z_1,z_2,z_3,z_4) &= z_1z_2+z_1z_3+z_1z_4+z_2z_3+z_2z_4+z_3z_4\\
e_3(z_1,z_2,z_3,z_4) &= z_1z_2z_3+z_1z_2z_4+z_1z_3z_4+z_2z_3z_4\\
e_4(z_1,z_2,z_3,z_4) &= z_1z_2z_3z_4
\end{aligned}$$

Πρόταση Ι.8.30 (Vieta)**.** *Για ένα πολυώνυμο βαθμού n με ρίζες $\rho_1,\dots,\rho_n$ δηλαδή*

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu = a_n \prod_{\nu=1}^{n}(x-\rho_\nu)$$

έχουμε

$$\frac{a_k}{a_n} = (-1)^{n-k} e_{n-k}(\rho_1,\dots,\rho_n)$$

Απόδειξη. Παρατηρούμε ότι αρκεί να αποδείξουμε την περίπτωση που $a_n = 1$. Θα προσθέσουμε στον συμβολισμό των στοιχειωδών συμμετρικών συναρτήσεων και ένα δείκτη για το πλήθος των μεταβλητών, δηλαδή

$$e_{r,s} = e_r(z_1,\dots,z_s).$$

θα δώσουμε μια απόδειξη με επαγωγή στο πλήθος n των ριζών. Αν $n = 1$ το αποτέλεσμα είναι προφανές:

$$e_{0,1}x - e_{1,1} = x-\rho_1, \qquad e_{0,1}=1, e_{1,1}=\rho_1.$$

Υποθέτουμε ότι ισχύει

$$\prod_{\nu=1}^{n}(x-\rho_\nu) = \sum_{\nu=0}^{n}(-1)^j e_{j,n}x^{n-j}$$

Και υπολογίζουμε

$$\begin{aligned}\prod_{\nu=1}^{n+1}(x-\rho_\nu) &= \sum_{\nu=0}^{n}(-1)^\nu e_{\nu,n}x^{n-\nu}(x-\rho_{n+1})\\ &= x\left(\sum_{\nu=0}^{n}(-1)^\nu e_{\nu,n}x^{n-\nu}\right)-\rho_{n+1}\left(\sum_{\nu=0}^{n}(-1)^\nu e_{\nu,n}x^{n-\nu}\right)\\ &= \sum_{\nu=0}^{n}(-1)^\nu e_{\nu,n}x^{n-(\nu-1)}-\rho_{n+1}\left(\sum_{\nu=1}^{n+1}(-1)^{\nu-1}e_{\nu-1,n}x^{n-(\nu-1)}\right)\\ &= e_{0,n}x^{n+1}+\sum_{\nu=1}^{n}(-1)^\nu(e_{\nu,n}+\rho_{n+1}e_{\nu-1,n})x^{n-(\nu-1)}-\rho_{n+1}(-1)^n e_{n,n}\\ &= \sum_{\nu=0}^{n+1}(-1)^\nu e_{\nu,n+1}x^{n-(\nu-1)}.\end{aligned}$$

□

Παράδειγμα I.8.31.

$$\begin{aligned}(x-\rho_1)(x-\rho_2)(x-\rho_3)(x-\rho_4) = x^4-(\rho_1+\rho_2+\rho_3+\rho_4)x^3+(\rho_1\rho_2+\rho_1\rho_3+\rho_1\rho_4+\rho_2\rho_3+\rho_2\rho_4+\rho_3\rho_4)x^2\\ -(\rho_1\rho_2\rho_3+\rho_1\rho_2\rho_4+\rho_1\rho_3\rho_4+\rho_2\rho_3\rho_4)x+\rho_1\rho_2\rho_3\rho_4\end{aligned}$$

Ορισμός I.8.32. Θα συμβολίζουμε για $k\geq 1$ το k-άθροισμα δυνάμεων

$$p_k(z_1,\dots,z_n)=\sum_{\nu=1}^{n}z_\nu^k=z_1^k+\cdots+z_n^k.$$

Πρόταση I.8.33 (Ταυτότητες Newton)**.**

$$ke_k(z_1,\dots,z_n)=\sum_{\nu=1}^{k}(-1)^{\nu-1}e_{k-\nu}(z_1,\dots,z_n)p_\nu(z_1,\dots,z_n)\ \textit{για κάθε}\ 1\leq k\leq n.$$

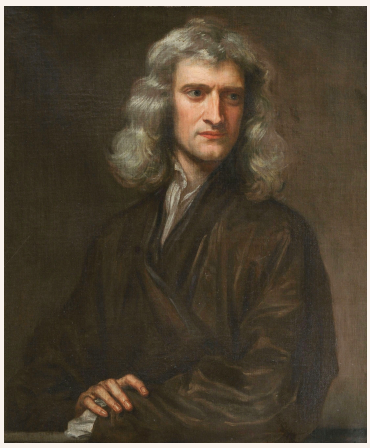
Επίσης ισχύει

$$0=\sum_{i=k-n}^{k}e_{k-i}(z_1,\dots,z_n)p_i(z_1,\dots,z_n)\ \textit{για κάθε}\ 1\leq n<k.$$

Απόδειξη. Υπάρχουν πολλές αποδείξεις για αυτή την ταυτότητα, επαγωγικές με γεννήτριες συναρτήσεις κτλ. Θα δώσουμε μια απόδειξη βασισμένη στην γραμμική άλγεβρα στην εφαρμογή 1. □

Παράδειγμα I.8.34. Για μικρές τιμές του k έχουμε

$$\begin{aligned}e_1 &= p_1\\ 2e_2 &= e_1p_1-p_2=p_1^2-p_2\\ 3e_3 &= e_2p_1-e_1p_2+p_3=\frac{1}{2}p_1^3-\frac{3}{2}p_1p_2+p_3\\ 4e_4 &= e_3p_1-e_2p_2+e_1p_3-p_4=\frac{1}{6}p_1^4-p_1^2p_2+\frac{4}{3}p_1p_3+\frac{1}{2}p_2^2-p_4.\end{aligned}$$



Ο **Sir Isaac Newton** (25 Δεκεμβρίου 1642 - 20 Μαρτίου 1726) ήταν Άγγλος Μαθηματικός, Αστρονόμος και Φυσικός. Η συνεισφορά του ήταν σημαντικότατη στην επιστημονική επανάσταση η οποία διαμόρφωσε τον τρόπο με τον οποίο κατανοούμε το φυσικό κόσμο. Το βιβλίο του Philosophiæ Naturalis Principia Mathematica, το οποίο εκδόθηκε το 1687 τέθηκαν οι αρχές του Απειροστικού λογισμού ο οποίος χρησιμοποιήθηκε για να εκφραστούν οι νόμοι της κίνησης και της βαρύτητας. Σε αυτό αποδείχθηκαν οι νόμοι του Kepler της κίνησης των πλανητών και εξηγήθηκαν μια σειρά από φαινόμενα όπως οι παλίρροιες, η μετάπτωση των ισημεριών καθιερώνοντας πέρα από κάθε αμφιβολία το ηλιοκεντρικό σύστημα του Κοπέρνικου. Είχε σημαντική συνεισφορά στην οπτική, κατασκεύασε το πρώτο κατοπτρικό τηλεσκόπιο αλλά και στην μελέτη του ήχου και των ρευστών.

Στα Μαθηματικά πάρα από την ανακάλυψη (ανεξάρτητα μαζί με τον G. W. Leibniz) του απειροστικού λογισμού, είχε σημαντική συνεισφορά στην μελέτη των δυναμοσειρών, στην γενίκευση του διωνυμικού θεωρήματος για μη ακέρους εκθέτες, στην εύρεση ριζών πολυωνύμων και στην ταξινόμηση των επίπεδων κυβικών καμπυλών. θεωρείται ένας από τους μεγαλύτερους Μαθηματικούς όλων των εποχών.

I.8.5 Δράσεις

Δράσεις Ομάδων

Μια πολύ σημαντική σχέση ισοδυναμίας δίνεται από μια δράση ομάδας G επί ενός χώρου X, δηλαδή μια συνάρτηση

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto gx \end{aligned}$$

η οποία ικανοποιεί τις ιδιότητες

- $\mathrm{id}_G x = x$, με id_G συμβολίζουμε το ταυτοτικό στοιχείο της G.
- $g(hx) = (gh)x$ για κάθε $g, h \in G$, $x \in X$.

Ορίζουμε μια σχέση ισοδυναμίας $x \sim y$ αν και μόνο αν υπάρχει $g \in G$ με $y = gx$. Αυτή είναι μια σχέση ισοδυναμίας αφού

- $x \sim x$, αρκεί να πάρουμε $\mathrm{id}_G \in G$ για να έχουμε $\mathrm{id}_G x = x$.
- Αν $x \sim y$ τότε και $y \sim x$, αφού αν υπάρχει $g \in G$ ώστε $y = gx$, τότε $g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = \mathrm{id}_G x = x$.
- Αν $x \sim y$ και $y \sim z$ τότε $y = gx$ και $z = hy$ για στοιχεία $g, h \in G$ οπότε $z = hy = h(gx) = (hg)x$, άρα $x \sim z$.

Ορισμός I.8.35. Ο χώρος πηλίκο $X/\sim$ θα συμβολίζεται με X/G και θα λέγεται ο «χώρος τροχιών» της ομάδας G, ενώ η κλάση ισοδυναμίας

$$Gx = \{gx : g \in G\} \text{ όπου } x \in G$$

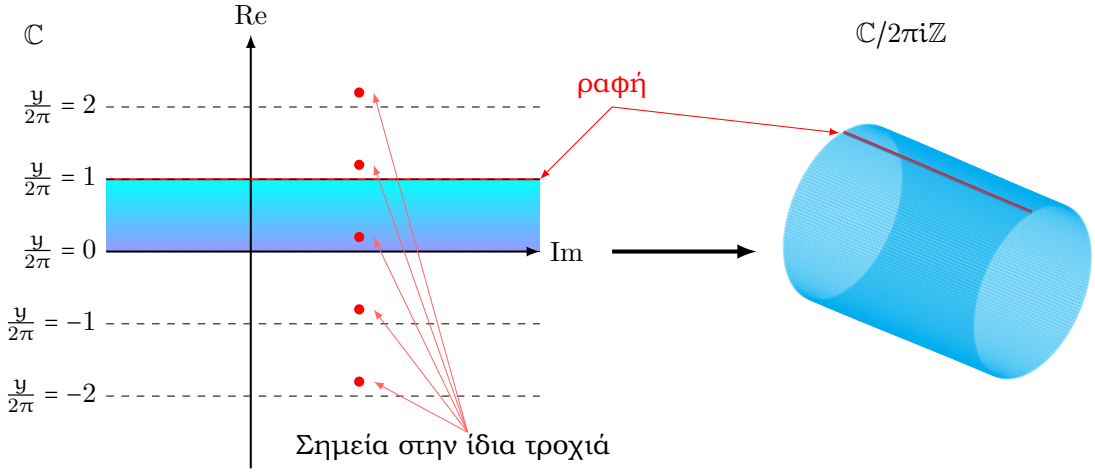
θα λέγεται τροχιά[α].

[α] Θα εξηγήσουμε την επιλογή της λέξης «τροχιά» στην παράγραφο VII.5.5 του x

Παράδειγμα I.8.36. Θεωρούμε ως σύνολο των μιγαδικών αριθμών $\mathbb{C}$ στο οποίο δρα η ομάδα $G = 2\pi i\mathbb{Z}$ και θεωρούμε την σχέση ισοδυναμίας

$$x \sim y \Leftrightarrow y - x \in G \Leftrightarrow y = gx$$

όπου $gx = x + 2\pi ik$ και κάποιο $k \in \mathbb{Z}$.



Σχήμα I.15: Το πηλίκο του $\mathbb{C}$ δια της δράσης του $2\pi i\mathbb{Z}$ και μία γεωμετρική αναπαράσταση του χώρου τροχιών ως κύλινδρος.

Δράσεις Δακτυλίων

εδώ θέλουμε τον ορισμό του module...

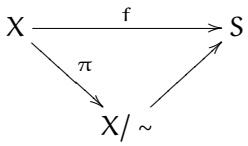
Υλοποιήσεις

Ο ορισμός του πηλίκου είναι αρκετά αφηρημένος και συχνά θέλουμε να υλοποιήσουμε τον χώρο πηλίκο και να του δώσουμε μια γεωμετρική δομή ώστε να είναι καλύτερα αντιληπτός συνήθως ως ένα υποσύνολο ενός καλά αντιληπτού χώρου για παράδειγμα του $\mathbb{R}^n, \mathbb{C}^n$ κτλ.

Ορισμός I.8.37. Μια υλοποίηση S ενός πηλίκου δίνεται από μια συνάρτηση $f : X \to S$ η οποία ικανοποιεί

- Παίρνει η ίδια τιμή σε κάθε αντιπρόσωπο της κλάσεις, δηλαδή $f(x) = f(y)$ αν $x \sim y$
- Ξεχωρίζει τις κλάσεις, δηλαδή σε διαφορετικές κλάσεις παίρνει διάφορες τιμές δηλαδή $f(x) \neq f(y)$ αν $x \not\sim y$.

Η συνάρτηση f επάγει την παρακάτω 1-1 συνάρτηση $\bar{f} : (X/\sim) \to S$:



όπου $\pi : X \to X/\sim$ είναι η συνάρτηση προβολής $\pi(x) = [x]$.

Το παράδειγμα I.8.36 δίνει μια υλοποίηση των κλάσεων του πηλίκου $\mathbb{C}/2\pi i\mathbb{Z}$, ενώ θα δούμε άλλη μια υλοποίηση στο **??**.

Το πρόβλημα της υλοποίησης πηλίκων είναι ένα από τα περισσότερο ενδιαφέροντα προβλήματα στα Μαθηματικά και έχει πολλές τεχνικές δυσκολίες ιδιαίτερα στις δράσεις άπειρων ομάδων όταν οι τροχιές έχουν «σημεία συσσώρευσης».

I.8.6 Τύπος Taylor

Ορισμός I.8.38 (Παραγώγιση πολυωνύμου)**.** θεωρούμε την συνάρτηση

$$D : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]$$
$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=1}^{n} a_i i x^{i-1}$$

Επίσης ορίζουμε

$$D^{(n)} = \underbrace{D \circ D \circ \cdots \circ D}_{n-\text{φορές}}.$$

την επαναλαμβανόμενη n-φορές εφαρμογή της παραγώγου D για $n \in \mathbb{N}, n > 1$. Τέλος ορίζουμε $D^{(0)}(f(x)) = f(x)$, δηλαδή $D^{(0)} = \mathrm{Id}_{\mathbb{F}[x]}$.

Παρατήρηση I.8.39. Είναι σαφές από τον ορισμό ότι

$$D(\lambda f + \mu g) = \lambda D(f) + \mu D(g) \text{ για κάθε } f, g \in \mathbb{F}[x], \lambda, \mu \in \mathbb{F}.$$

Επίσης παρατηρούμε ότι

$$D(fg) = fD(g) + D(f)g \text{ για κάθε } f, g \in \mathbb{F}[x].$$

Πράγματι αν

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad g(x) = \sum_{j=0}^{m} b_j x^j$$

τότε

$$\begin{aligned} D\big(f(x)g(x)\big) = D\Big(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j}\Big) &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j D(x^{i+j}) \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j (i+j) x^{i+j-1} \\ &= \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j j x^{j-1} + \sum_{j=0}^{m} b_j x^j \sum_{i=0}^{m} a_i i x^{i-1} \\ &= f(x)D(g(x)) + D(f(x))g(x). \end{aligned}$$

Μπορούμε, να θεωρήσουμε το υπόλοιπο της διαίρεσης του $f(x)$ με το $(x-a)^k$, όπου $k \geq 1$ το οποίο θα είναι ένα πολυώνυμο βαθμού $k-1$.

Πρόταση I.8.40. *Για την διαίρεση ένος πολυωνύμου βαθμού n και ένα ακέραιο $k \geq 1$ έχουμε*

$$f(x) = p(x)(x-a)^k + u(x),$$

όπου

$$u(x) = \sum_{i=0}^{k-1} \frac{ev_a D^{(i)}(f(x))}{n!}(x-a)^i.$$

Απόδειξη. Θα το αποδείξουμε με επαγωγή στο $k \geq 1$. Η περίπτωση $k = 1$, ισχύει σύμφωνα με την παρατήρηση I.8.13. Υποθέτουμε την αλήθεια της πρότασης για $k-1$

$$\begin{aligned} f(x) &= ev_a D^{(0)} f(x) + ev_a D^{(1)} f(x) + \frac{ev_a D^{(1)} f(x)}{2!} + \cdots + \frac{ev_a D^{(k-2)} f(x)}{(k-2)!} + (x-a)^k p(x) \\ &= ev_a D^{(0)} f(x) + ev_a D^{(1)} f(x) + \frac{ev_a D^{(1)} f(x)}{2!} + \cdots + \frac{ev_a D^{(k-2)} f(x)}{(k-2)!} + b(x-a)^k + (x-a)^{k+1} q(x) \end{aligned}$$

όπου στην τελευταία σχέση γράψαμε $p(x) = b + q(a)$. Παρατηρούμε ότι

$$\begin{aligned} 0 &= D^{(k)} \left(ev_a D^{(0)} f(x) + ev_a D^{(1)} f(x) + \frac{ev_a D^{(1)} f(x)}{2!} + \cdots + \frac{ev_a D^{(k-2)} f(x)}{(k-2)!} \right) \\ bk! &= D^{(k)} b(x-a)^k \\ 0 &= ev_a (D^{(k)} \left((x-a)^{k+1} q(X) \right), \end{aligned}$$

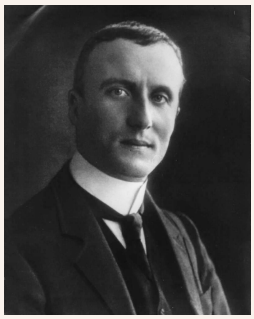
συνεπώς

$$ev_a D^{(k)} f(x) = k! b,$$

δηλαδή το ζητούμενο. □

I.8.7 Παραγώγιστη Συναρτήσεων

Θα δώσουμε ένα ασυνήθιστο τρόπο να ορίσουμε πότε μια συνάρτηση είναι παραγωγίσιμη ο οποίος είναι ισοδύναμος με αυτόν που θα δείτε σε άλλα μαθήματα Ανάλυσης και οφείλεται στον Κ. Καραθεοδωρή, ακολουθώντας το άρθρο [9].



Ο **Κωσταντίνος Καραθεοδωρή** (13 Σεπτεμβρίου 1873 - 2 Φεβρουαρίου 1950) ήταν Έλληνας Μαθηματικός που πέρασε το μεγαλύτερο μέρος της ζωής του στην Γερμανία. Είχε σημαντικότατη συνεισφορά στην πραγματική και μιγαδική ανάλυση, στον λογισμό των μεταβολών και την θεωρία μέτρου. Επίσης εργάστηκε πάνω στην αξιωματική διατύπωση της θερμοδυναμικής. Θεωρείται ένας από τους περισσότερο αξιόλογους Μαθηματικούς της εποχής του. Αναμίχθηκε με την οργάνωση των Ελληνικών πανεπιστημίων και ιδιαίτερα με το Ελληνικό Πανεπιστήμιο της Σμύρνης μετά από πρόσκληση του Ελευθέριου Βενιζέλου, στο και παρέμεινε μέχρι την Μικρασιατική Καταστροφή. Στην συνέχεια δίδαξε στο Πανεπιστήμιο Αθηνών μέχρι το 1924 που κατέλαβε θέση καθηγητή στο Πανεπιστήμιο του Μονάχου.

Ορισμός I.8.41 (Καραθεοδωρή)**.** Η συνάρτηση $f : (a, b) \to \mathbb{R}$ είναι παραγωγίσιμη στο σημείο $x_0 \in (a, b)$ αν και μόνο αν υπάρχει συνάρτηση ϕ_{x_0} η οποία είναι συνεχής στο $x = x_0$ και ικανοποιεί την σχέση

$$f(x) - f(x_0) = \phi_{x_0}(x)(x - x_0) \text{ για κάθε } x \in (a, b). \tag{I.11}$$

Παρατήρηση Ι.8.42. 1. Αν η συνάρτηση f είναι παραγωγίσιμη στο x_0 τότε είναι συνεχής στο x_0.

2. Υπάρχει το πολύ μια συνάρτηση ϕ_{x_0} που να ικανοποιεί τον ορισμό, οπότε θέτουμε για την παράγωγο της f στο x_0, $f'(x_0) = \phi_{x_0}(x_0)$.

Αυτά είναι άμεσα από την εξίσωση (Ι.11).

Παρατήρηση Ι.8.43. Ο παραπάνω ορισμός της παραγωγίσιμης συνάρτησης είναι αλγεβρικός. Στον δακτύλιο των συνεχών συναρτήσεων σε ένα ανοιχτό διάστημα που περιλαμβάνει το x_0 η συνεχής συνάρτηση f είναι παραγωγίσιμη στο x_0 αν η συνεχής συνάρτηση $x - x_0$ διαιρεί την συνεχή συνάρτηση $f(x) - f(x_0)$ δηλαδή αν και μόνο αν η συνάρτηση

$$\phi(x) = \frac{f(x) - f(x_0)}{x - x_0}$$

είναι στοιχείο του δακτυλίου των συνεχών συναρτήσεων σε ανοιχτό διάστημα που περιλαμβάνει το x_0.

Θεώρημα Ι.8.44. *Αν f, g είναι διαφορίσιμες στο x_0, $k, l \in \mathbb{R}$ και $n \in \mathbb{N}$ τότε*

1. $(kf + lg)'(x_0) = kf'(x_0) + lg'(x_0)$
2. $(fg)'(x_0) = f(x_0)g'(x_0) = f'(x_0)g(x_0)$
3. *Αν $f(x) = x^n$ τότε $f'(x_0) = nx_0^{n-1}$*

Απόδειξη. Από την παραγωγισιμότητα των f, g έχουμε ότι στα ανοιχτά διαστήματα U, V τα οποία περιέχουν το x_0 και κατά συνέπεια και στο ανοιχτό διάστημα $U \cap V$ γράφουμε

$$f(x) - f(x_0) = \phi(x)(x - x_0)$$
$$g(x) - g(x_0) = \psi(x)(x - x_0)$$

οπότε

$$(kf - lg)(x) - (kf - lg)(x_0) = k\big(f(x) - f(x_0)\big) + l\big(g(x) - g(x_0)\big)$$
$$k\phi(x)(x - x_0) + l\psi(x)(x - x_0) = \big(k\phi(x) + l\psi(x)\big)(x - x_0)$$

συνεπώς $(kf + lg)'(x_0) = kf'(x_0) + lg'(x_0)$.

Για κάθε $x \in U \cap V$ έχουμε

$$\begin{aligned}(fg)(x) - (fg)(x_0) &= f(x)g(x) - f(x_0)g(x_0) = f(x)g(x) - f(x)g(x_0) + f(x)g(x_0) - f(x_0)g(x_0)\\ &= f(x)\big(g(x) - g(x_0)\big) + \big(f(x) - f(x_0)\big)g(x_0)\\ &= f(x)\psi(x)(x - x_0) + \phi(x)(x - x_0g(x_0))\\ &= \big(f(x)\psi(x) + \phi(x)g(x_0)\big)(x - x_0)\end{aligned}$$

από όπου προκύπτει το ζητούμενο.

Παρατηρούμε ότι

$$x^n - x_0^n = (x^{n-1} + x^{n-1}x_0 + x^{n-3}x_0^2 + \cdots + xx_0^{n-2} + x_0^{n-1})(x - x_0)$$

οπότε για την συνάρτηση

$$\phi(x) = x^{n-1} + x^{n-1}x_0 + x^{n-3}x_0^2 + \cdots + xx_0^{n-2} + x_0^{n-1}$$

ισχύει ο ορισμός της παραγώγου και καταλήγουμε στο $\phi(x_0) = nx^{n-1}$, όπως έπρεπε. □

Παρατήρηση I.8.45. Το παραπάνω θεώρημα μας δίνει ότι οι πολυωνυμικές συναρτήσεις είναι παραγωγίσιμες και η παράγωγος τους υπολογίζεται ακριβώς όπως την ορίσαμε στο I.8.38.

Η δύναμη του παραπάνω ορισμού φαίνεται στις αποδείξεις σημαντικών θεωρημάτων σχετικά με την παράγωγο:

Θεώρημα I.8.46 (Κανόνας Αλυσίδας)**.** *Αν η* f *είναι παραγωγίσιμη στο σημείο* x_0 *και η* y *είναι παραγωγίσιμη στο σημείο* $y_0 = f(x_0)$*, τότε η σύνθεση τους* $h = g \circ f$ *είναι παραγωγίσιμη στο* x_0 *και μάλιστα ισχύει:*

$$h'(x_0) = g'(y_0)f'(x_0).$$

Απόδειξη. Αφού η f είναι παραγωγίσιμη στο x_0 υπάρχει συνάρτηση $\phi_{x_0}(x)$ συνεχής στο x_0 και ορισμένη σε ένα ανοιχτό διάστημα V που περιλαμβάνει το x_0 με

$$f(x) - f(x_0) = \phi_{x_0}(x - x_0) \text{ για κάθε } x \in V.$$

Ομοίως υπάρχει μια συνάρτηση $\psi_{y_0}(x)$ συνεχής στο y_0 ορισμένη σε ένα ανοιχτό διάστημα U που να περιέχει το y_0 και

$$g(y) - g(y_0) = \psi_{y_0}(y - y_0) \text{ για κάθε } y \in U.$$

Υπολογίζουμε ότι

$$\begin{aligned} h(x) - h(x_0) &= g(f(x)) - g(f(x_0)) = \psi_{y_0}(f(x))(f(x) - f(x_0)) \\ &= \psi(f(x))\phi_{x_0}(x - x_0) \text{ για κάθε } x \in V \text{ με } f(x) \in U. \end{aligned}$$

Η συνάρτηση $(\psi_{y_0} \circ f)(x)\phi_{x_0}(x)$ είναι συνεχής στο x_0 και έχει την τιμή $g'(f(x_0))f'(x_0)$, δηλαδή το ζητούμενο. □

Θεώρημα I.8.47. *Μία* f *συνεχής και γνήσια μονότονη στο ανοιχτό διάστημα* I *που περιλαμβάνει το* x_0 *ώστε να είναι παραγωγωγίσιμη στο* x_0*, με* $f'(x_0) \neq 0$*. Τότε η αντίστροφη συνάρτηση* $g = f^{-1}$ *είναι διαφορίσιμη στο* $y_0 = f(x_0)$ *και* $g'(y_0) = \frac{1}{f'(x_0)}$.

Απόδειξη. Έχουμε ότι

$$f(x) - f(x_0) = \phi_{x_0}(x)(x - x_0),$$

όπου η ϕ_{x_0} είναι συνεχής στο x_0 και $\phi_{x_0}(x) \neq 0$ για όλα τα $x \in I$, περιορίζοντας το διάστημα I αν χρειάζεται. Έστω V το πεδίο ορισμού της $g = f^{-1}$. Τότε

$$y - y_0 = f(g(y)) - f(x_0) = \phi(g(y))(g(y) - x_0) \text{ για κάθε } y \in V,$$

δηλαδή

$$g(y) - x_0 = \frac{1}{\phi(g(y))}(y - y_0) \text{ για όλα τα } y \in V$$

Αφού η g είναι συνεχής στο V, η $1/\phi \circ g$ είναι επίσης συνεχής και το ζητούμενο έπεται. □

Θεώρημα I.8.48. *Θεωρούμε την* $f : U \to \mathbb{R}$*, όπου το* U *είναι ένα ανοιχτό διάστημα που περιλαμβάνει το σημείο* x_0*. Αν η* $f(x)$ *είναι ένα τοπικό ακρότατο στο* x_0 *τότε είτε* $f'(x_0) = 0$ *είτε δεν υπάρχει η παράγωγος στο* x_0*.*

Απόδειξη. Υποθέτουμε ότι το $f(x_0)$ είναι ένα τοπικό μέγιστο. Θα δείξουμε ότι αν υπάρχει η $f'(x_0)$ τότε $f'(x_0) = 0$. Υποθέτουμε ότι για ένα ανοιχτό διάστημα $I \subset U$ υπάρχει μια συνεχής συνάρτηση ϕ, ώστε

$$f(x) - f(x_0) = \phi(x)(x - x_0) \text{ για κάθε } x \in I.$$

Έχουμε ότι $f(x) - f(x_0) \leq 0$ για κάθε $x \in I_1 \subset I$. Συνεπώς για $x - x_0 \leq 0$ έχουμε ότι $f(x) \geq 0$ ενώ για $x - x_0 \geq 0$ έχουμε ότι $f(x) \leq 0$. Η συνέχεια της ϕ στο x_0 επιβάλει ότι $f(x_0) = 0$. □

Ι.8.8 Αναλυτικές συναρτήσεις

Δεν είναι όλες οι συναρτήσεις πολυωνυμικές. Για παράδειγμα κάθε πολυώνυμο βαθμού n μηδενίζεται μετά από $n+1$ παραγωγίσεις, ενώ συναρτήσεις όπως η εκθετική παραμένουν αναλλοίωτες όταν τις παραγωγίσουμε.

Ορισμός Ι.8.49. Ο δακτύλιος των τυπικών δυναμοσειρών $\mathbb{F}[[x]]$ έχει ως στοιχεία εκφράσεις

$$\mathbb{F}[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in \mathbb{F} \right\},$$

με πράξεις

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} \sum_{\substack{\nu+\mu=i \\ \nu \geq 0, \mu \geq 0}} a_\nu b_\mu x^i.$$

Παρατήρηση Ι.8.50. Σε ένα στοιχείο $f \in \mathbb{F}[[z]]$, μπορούμε να ορίσουμε την n-στή παράγωγο

$$D^{(n)} \left(\sum_{i=0}^{\infty} a_i x^i \right) \sum_{i=0}^{\infty} a_i D^{(n)} x^i = \sum_{i=n}^{\infty} a_i i(i-1)(i-2)\cdots(i-n+1) x^{i-n}$$

Αν θέλουμε από μία τυπική δυναμοσειρά $f(x) = \sum_{i=0}^{\infty} a_i x^i$ να πάρουμε μία συνάρτηση

$$\mathbb{F}[[x]] \longrightarrow \mathbb{F}[[x]]$$

$$a \longmapsto f(a) = \sum_{i=0}^{\infty} a_i a^i$$

θα πρέπει να δώσουμε μια ερμηνεία στο άπειρο άθροισμα στα δεξιά του παραπάνω τύπου. Αυτό μπορούμε να το κάνουμε στην περίπτωση που $\mathbb{F} = \mathbb{R}$ ή $\mathbb{F} = \mathbb{C}$ και χρειάζεται να εισάγουμε την έννοια της σύγκλισης.

Ορισμός Ι.8.51. Θα λέμε ότι η σειρά $\sum_{i=0}^{n} a_i$ συγκλίνει απολύτως αν υπάρχει το όριο

$$\lim_{\nu \to \infty} \sum_{i=0}^{n} |a_i| = \sum_{i=0}^{\infty} |a_i|.$$

Θα λέμε ότι η σειρά $f(x) = \sum_{i=0}^{\infty} a_i a^i \in \mathbb{C}[[x]]$ συγκλίνει ομοιόμορφα σε ένα υποσύνολο $K \subset \mathbb{C}$ αν για κάθε $a \in K$ και κάθε $\epsilon > 0$ υπάρχει $n_0 \in \mathbb{N}$, ώστε για κάθε $n > n_0$

$$\left| \sum_{i=0}^{n} |a_i||a|^i - g(a) \right| < \epsilon.$$

Στον παραπάνω ορισμό η επιλογή του $n_0 \in \mathbb{N}$ είναι ανεξάρτητη του $a \in K$. Την ποσότητα $g(a)$ την γράφουμε και ως

$$g(a) = \sum_{i=0}^{\infty} |a_i||a|^i.$$

Πρόταση I.8.52. *Για κάθε δυναμοσειρά $\sum_{i=0}^{n} a_i x^i$ υπάρχει μια ακτίνα σύγκλισης $R \in \mathbb{R}$, $0 \leq R \leq +\infty$ ώστε η σειρά συγκλίνει απολύτως και ομοιόμορφα για $|x| < R$ και δεν συγκλίνει αν $|x| > R$. Η ακτίνα σύγκλισης ικανοποιεί*

$$\frac{1}{R} = d = \operatorname{limsum} \sqrt[n]{|a_n|}. \tag{I.12}$$

Στο παραπάνω αν $d = 0$ τότε η ακτίνα σύγκλισης είναι άπειρη και η σειρά συγκλίνει ομοιόμορφα για κάθε $a \in \mathbb{C}$. Αν υπάρχει το όριο $\lim_{n\to\infty} \frac{|a_{n+1}|}{|a_n|}$ τότε αυτό είναι ίσο με την ποσότητα d της εξίσωσης (I.12).

Παράδειγμα I.8.53. Θεωρούμε την εκθετική συνάρτηση η οποία μπορεί να οριστεί ως

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}. \tag{I.13}$$

Παρατηρούμε ότι $a_n = n!$ οπότε $\lim \frac{a_{n+1}}{a_n} = \lim \frac{(n+1)!}{n!} = \lim n = \infty$. Συνεπώς η ακτίνα σύγκλισης είναι άπειρη και η σειρά συγκλίνει για κάθε $x \in \mathbb{C}$.

Θεωρούμε τώρα την γεωμετρική σειρά

$$g(x) = \sum_{n=0}^{\infty} x^n.$$

Εδώ $a_n = 1$, οπότε η ακτίνα σύγκλισης $R = 1$ και η σειρά συγκλίνει για $x \in \mathbb{C}$, $|x| = 1$. Αυτό αντανακλά το γεγονός ότι η γεωμετρική σειρά αθροίζεται στην $g(x) = \frac{1}{1-x}$ η οποία απειρίζεται για $x = 1$.

Στην πρόταση I.8.40 έχουμε εκφράσει κάθε πολυώνυμο ως ένα πολυωνυμικό ανάπτυγμα με την βοήθεια των παραγώγων. Μία παρόμοια θεωρία έχουμε για μια κλάση συναρτήσεων τις οποίες ονομάσουμε αναλυτικές.

Θεώρημα I.8.54. *θεωρούμε μια συνάρτηση $f : \mathbb{F} \longrightarrow \mathbb{F}$, όπου $\mathbb{F} = \mathbb{R}$ ή $\mathbb{F} = \mathbb{C}$. Θα συμβολίζουμε με $f^{(n)}$ την n-στη παράγωγο της συνάρτησης f. Υποθέτουμε ότι η συνάρτηση f είναι άπειρες φορές παραγωγίσιμη σε μία περιοχή του z_0. Σχηματίζουμε την τυπική σειρά στην μεταβλητή $z - z_0$*

$$f = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n \in \mathbb{F}\left[[(z - z_0)]\right].$$

Υπολογίζουμε την ακτίνα σύγκλισης $R \in \mathbb{R}$ σύμφωνα με την (I.12). Αν $R > 0$ τότε η f ορίζει μια συνάρτηση

$$\begin{aligned} \{z \in \mathbb{F} : |z - z_0| < R\} &\longrightarrow \mathbb{F} \\ z &\longmapsto \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n \end{aligned}$$

Αν $R = \infty$ τότε ορίζεται συνάρτηση

$$f : \mathbb{F} \longrightarrow \mathbb{F}$$
$$z \longmapsto \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n$$

Η παραπάνω συνάρτηση είναι άπειρες φορές παραγωγίσιμη και μάλιστα

$$f^{(n)}(z) = D^{(n)}(z).$$

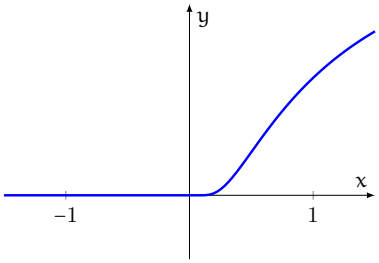
Οι συναρτήσεις που ορίστηκαν παραπάνω με την βοήθεια της άπειρης άθροισης ταυτίζονται με την αρχική συνάρτηση σε κατάλληλη περιοχή του z_0.

Παρατήρηση Ι.8.55. Τα πολυώνυμα στο $\mathbb{F}$ είναι άπειρες φορές παραγωγίσιμα. Στην πραγματικότητα ένα πολυώνυμο βαθμού n μετά από $n+1$ παραγωγίσεις μηδενίζεται οπότε δεν τίθεται θέμα σύγκλισης.

Παρατήρηση Ι.8.56. Δεν είναι όλες οι απειροδιαφορίσιμες συναρτήσεις $\mathbb{F} \to \mathbb{F}$ αναλυτικές. Κλασικό παράδειγμα είναι η συνάρτηση $f(x) : \mathbb{R} \to \mathbb{R}$ η οποία ορίζεται ως

$$f(x) = \begin{cases} e^{-\frac{1}{x}} & \text{αν } x > 0 \\ 0 & \text{αν } x \leq 0. \end{cases} \tag{I.14}$$

Η οποία έχει παραγώγους κάθε τάξης και μάλιστα $f^{(n)}(0) = 0$. Η συνάρτηση αυτή δεν είναι



Σχήμα Ι.16: Η απειροδιαφορίσιμη αλλά όχι αναλυτική συνάρτηση $f(x)$ της εξίσωσης (Ι.14).

αναλυτική γιατί τότε θα είχε ένα ανάπτυγμα στο 0 της μορφής

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!}x^n = \sum_{n=0}^{\infty} \frac{0}{n!}x^n = 0$$

δηλαδή θα έπρεπε να είναι η σταθερή μηδενική συνάρτηση, που δεν είναι.

Παράδειγμα Ι.8.57. Έχουμε ήδη ορίσει την εκθετική συνάρτηση με την βοήθεια δυναμοσειράς. Με οποιοδήποτε άλλο τρόπο και να ορίσουμε την εκθετική συνάρτηση μπορούμε να καταλήξουμε στην δυναμοσειρά της εξίσωσης (Ι.13) αρκεί να μπορούμε με βάση τον εναλλακτικό ορισμό της εκθετικής να μπορούμε να δείξουμε ότι κάθε παράγωγος της εκθετικής υπολογισμένη στο 0 δίνει την τιμή 1.

Μερικές ακόμα συναρτήσεις που εκφράζονται με την βοήθεια δυναμοσειρων είναι οι

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$
$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

όπως μπορούμε να υπολογίσουμε από τις $\sin^{(n)}(0)$ και $\cos^{(n)}(0)$. Επίσης και οι δύο παραπάνω σειρές έχουν άπειρη ακτίνα σύγκλισης. Τέλος, συγκρίνοντας τις παραπάνω εκφράσεις με αυτή του e^x καταλήγουμε στο ότι για $x \in \mathbb{R}$ έχουμε

$$e^{ix} = \cos(x) + i\sin(x).$$

Παρατήρηση I.8.58. Υπάρχουν συγγραφείς που ορίζουν τις συναρτήσεις ημιτόνου και συνημιτόνου με βάση την παραπάνω έκφραση:

$$\sin(x) = \frac{e^{ix} - e^{-ix}}{2i} \qquad \cos(x) = \frac{e^{ix} + e^{-ix}}{2}, \text{ για } x \in \mathbb{R}.$$

Παρατήρηση I.8.59. Ισχύει ότι

$$e^{x+y} = e^x e^y.$$

Πράγματι,

$$\begin{aligned} e^{x+y} &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \sum_{a+b=n} \binom{n}{a} x^a y^b \\ &= \sum_{n=0}^{\infty} \frac{n!}{n!} \sum_{a+b=n} \binom{n}{a} \frac{x^a}{a!} \frac{y^b}{b!} = \left(\sum_{a=0}^{\infty} \frac{x^a}{a!}\right)\left(\sum_{b=0}^{\infty} \frac{x^b}{b!}\right) \\ &= e^x e^y. \end{aligned}$$

Από την παραπάνω ιδιότητα μπορούμε να αποδείξουμε τριγωνομετρικούς τύπους, για παράδειγμα για $x, y \in \mathbb{R}$

$$\big(\cos(x) + i\sin(x)\big)\big(\cos(y) + i\sin(y)\big) = e^{ix}e^{iy} = e^{i(x+y)} = (\cos(x+y) + i\sin(x+y))$$

από όπου έχουμε συγκρίνοντας μιγαδικό και πραγματικό μέρος ότι

$$\begin{aligned} \cos(x+y) &= \cos(x)\cos(y) - \sin(x)\sin(y) \\ \sin(x+y) &= \sin(x)\cos(y) + \cos(x)\sin(y) \end{aligned}$$

Παρατήρηση I.8.60. Αθροίζοντας μερικούς μόνο όρους μιας σειράς Taylor έχουμε μια πολυωνυμική προσέγγιση της συνάρτησης. Στο σχήμα I.17 απεικονίζονται η συνάρτηση $\sin(x)$ μαζί με τις διαδοχικές προσεγγίσεις

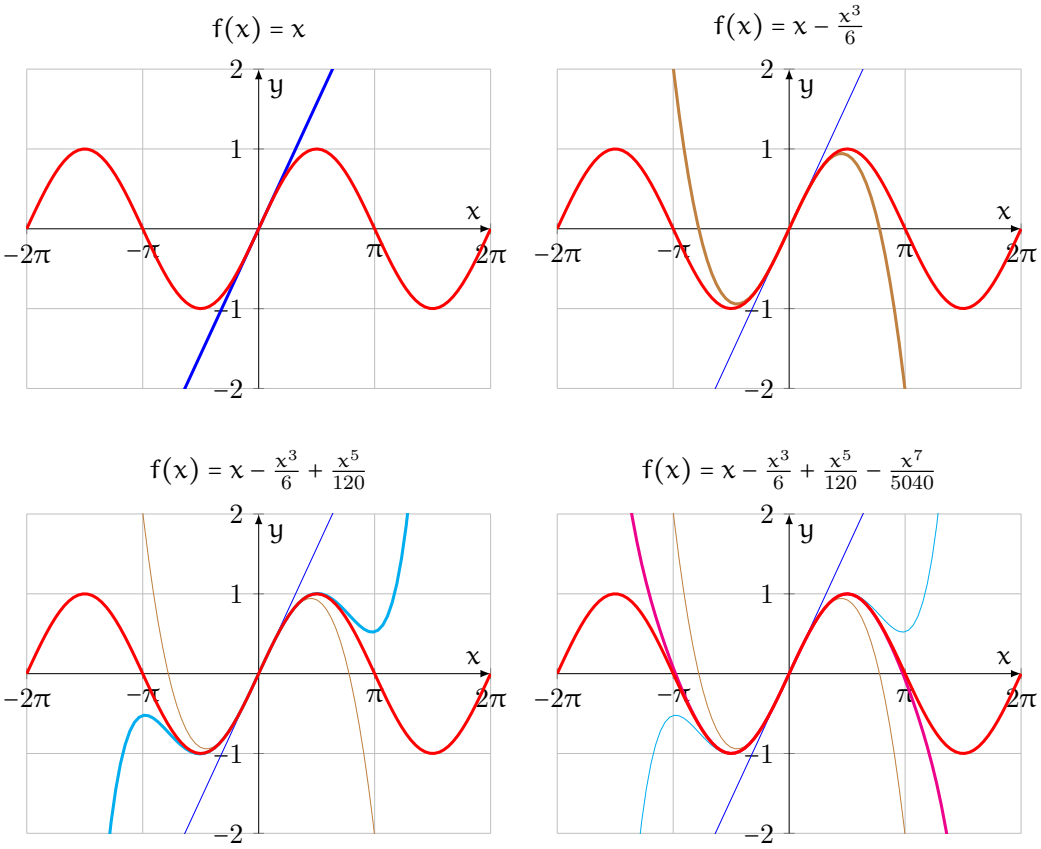
$$x, \quad x - \frac{x^3}{6}, \quad x - \frac{x^2}{6} + \frac{x^5}{120}, \quad x - \frac{x^2}{6} + \frac{x^5}{120} - \frac{x^7}{5040}.$$

I.8.9 Η μιγαδική λογαριθμική συνάρτηση

Αναλυτική προσέγγιση

Ορισμός I.8.61. Ορίζουμε την σειρά του λογαρίθμου γύρω από το 1 δηλαδή στην μεταβλητή $x - 1$:

$$\log(x) = \sum_{k=1}^{\infty} \frac{(x-1)^k}{k}(-1)^{k+1}. \tag{I.15}$$



Σχήμα Ι.17: Πολυωνυμικές προσεγγίσεις της $\sin(x)$ όσο περισσότερους πολυωνυμικούς όρους αθροίζουμε τόσο καλύτερη είναι η προσέγγιση της συνάρτησης του ημιτόνου.

Πρόταση Ι.8.62. *Όπως ορίστηκε ο λογάριθμος ισχύει ότι*

$$\log(e^x) = x$$

Απόδειξη. Υπολογίζουμε την ποσότητα:

$$\begin{aligned}
\log(e^x) &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}(e^x-1)^n && \text{(Ι.16)}\\
&= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \sum_{k=0}^{n} \binom{n}{k}(-1)^{n-k} e^{kx}\\
&= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \sum_{k=0}^{n} \binom{n}{k}(-1)^{n-k} \sum_{m=0}^{\infty} \frac{k^m x^m}{m!}\\
&= -\sum_{m=0}^{\infty} \frac{x^m}{m!} \sum_{n=1}^{\infty} \frac{1}{n} \sum_{k=0}^{n} \binom{n}{k}(-1)^k k^m\\
&= -\sum_{m=0}^{\infty} \frac{x^m}{m!} a_m && \text{(1)}
\end{aligned}$$

όπου έχουμε θέσει

$$a_m = \sum_{n=1}^{\infty} \frac{1}{n} \sum_{k=0}^{n} \binom{n}{k}(-1)^k k^m. \qquad \text{(Ι.17)}$$

Στην παραπάνω έκφραση ότι $k \geq 1$ εφαρμόζουμε την ταυτότητα

$$\frac{1}{n}\binom{n}{k} = \frac{1}{k}\binom{n-1}{k-1}$$

ενώ για τους όρους με $k = 0$ στην (I.17) παρατηρούμε ότι είναι μηδενικοί αφού θεωρούμε a_m με $m \geq 1$. Συνεπώς έχουμε

$$\begin{aligned} a_m &= \sum_{k=1}^{m} (-1)^k k^m \sum_{n=k}^{m} \frac{1}{k}\binom{n-1}{k-1} \\ &= \sum_{k=1}^{m} (-1)^k k^{m-1} \sum_{n=k}^{m} \binom{n-1}{k-1} \end{aligned}$$

Εφαρμόζουμε τώρα την ταυτότητα (άσκηση **??**)

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}$$

για να πάρουμε

$$a_m = \sum_{k=1}^{m} (-1)^k k^{m-1} \binom{m}{k}.$$

Στην τελευταία εφαρμόζουμε την ταυτότητα (άσκηση **??**)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} k^m = 0 \text{ για } m, n \in \mathbb{Z}, 0 \leq m < n. \tag{I.18}$$

οπότε έχουμε

$$a_m = \left(\sum_{k=0}^{m} (-1)^k k^{m-1} \binom{m}{k} \right) - 0^{m-1}$$

όπου για $m - 1$ έχουμε κάνει την σύμβαση ότι $0^0 = 1$. Για παράδειγμα στο ανάπτυγμα του εκθετικού

$$e^{kx} = \sum_m k^m x^m / m!$$

ο $m = 0$ όρος θεωρείται ίσος με 1 ακόμα και όταν $k = 0$. Συνεπώς

$$0^{m-1} = \begin{cases} 0 & \text{αν } m \neq 1 \\ 1 & \text{αν } m = 1 \end{cases}$$

Οπότε εφαρμόζουμε και πάλι την εξίσωση (I.18), οι προϋποθέσεις ικανοποιούνται αφού $m < m-1$ για να πάρουμε ότι

$$a_m = -0^{m-1}.$$

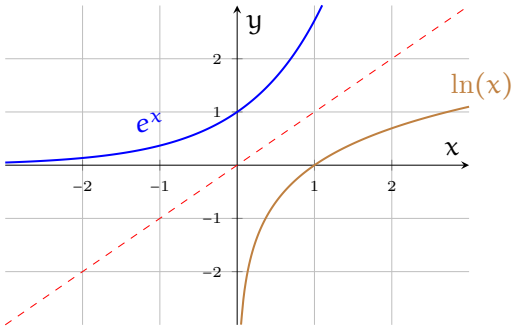
Συνεπώς η (1) καταλήγει στο ότι

$$\log(e^x) = x.$$

□

Γεωμετρική προσέγγιση

Παρατηρούμε ότι η εκθετική συνάρτηση είναι 1-1 και επί από το $\mathbb{R} \to \mathbb{R}^*$, συνεπώς έχει αντίστροφη $\ln(x) : \mathbb{R}^* \to \mathbb{R}$, η οποία έχει γράφημα συμμετρικό ως προς την διαγώνιο, δείτε την εικόνα I.18.



Σχήμα Ι.18: Η εκθετική πραγματική συνάρτηση και η αντίστροφη της λογαριθμική

Μπορούμε να ορίσουμε την συνάρτηση $\ln : \mathbb{R}^* \to \mathbb{R}$ την οποίο ορίζουμε για $|x| < 1$ με βάση την εξίσωση Ι.15 γράφοντας την στην μορφή

$$\ln(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n. \tag{Ι.19}$$

Την συνάρτηση αυτή την επεκτείνουμε για $x > 1$ κάνοντας χρήση της συναρτησιακής εξίσωσης[3]

$$\ln(x) + \ln(y) = \ln(xy) \tag{Ι.20}$$

η οποία προκύπτει αντιστρέφοντας την σχέση $e^{x+y} = e^x e^y$. Από την (Ι.20) μπορούμε να ορίσουμε την $\ln(x)$ για $x > 1$ ως εξής: Παρατηρούμε ότι $(1+x)\left(1 - \frac{x}{1+x}\right) = 1$, οπότε

$$\ln(1+x) = -\ln\left(1 - \frac{x}{1+x}\right)$$

και αν $x > 1$ τότε $\frac{x}{1+x} < 1$.

Για την τιμή $x = -1$ η συνάρτηση $\ln(1+x)$ δεν μπορεί να οριστεί με κανένα τρόπο, ενώ για την τιμή $x = 1$ καταλήγουμε στον υπολογισμό του

$$\ln(2) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n}.$$

Παρατηρούμε ότι το άπειρο άθροισμα στο δεξί μέρος της παραπάνω ισότητας υπάρχει. Πράγματι αν θεωρήσουμε τα μερικά αθροίσματα

$$S_{2m+1} = \sum_{n=1}^{2m+1} \frac{(-1)^n}{n}$$

παρατηρούμε ότι

$$S_{2(m+1)+1} = S_{2m+1} - \frac{1}{2m+2} + \frac{1}{2m+3} \le S_{2m+1}$$

και

$$S_{2(m+1)} = S_{2m} + \frac{1}{2m+1} - \frac{1}{2m+2} \ge S_{2m}$$

Συνεπώς η ακολουθία S_{2m+1} είναι φθίνουσα ενώ η ακολουθία S_{2m} είναι αύξουσα. Συνεπώς έχουμε ότι

$$1 - \frac{1}{2} = S_2 \le S_{2m} \le S_{2m+1} \le S_1 = a_1$$

[3] Ο συγγραφέας ελπίζει ότι ο αναγνώστης θα εμβαθύνει στις σπουδές του κάποια στιγμή θα δει μια παρόμοια επέκταση συνάρτησης για την ζ-συνάρτηση του Riemann.

άρα σύμφωνα με την άσκηση **??** η ακολουθίες των άρτιων και περιττών αθροισμάτων συγκλίνουν και οι δύο. Τέλος συγκλίνουν στον ίδιο όριο αφού

$$\lim_{m\to\infty}(S_{2m+1}-S_{2m})=\lim_{m\to\infty}\frac{1}{2m+1}=0.$$

Ο μιγαδικός λογάριθμος. Παρατηρούμε ότι για ένα μιγαδικό w $e^w\neq 0$ αφού $1=e^0=e^{(w-w)}=e^we^{-w}$. Ένας μιγαδικός λογάριθμος του $z\in\mathbb{C}$ είναι ένας $w\in\mathbb{C}$ ώστε $e^w=z$. Υποθέτουμε ότι ο

$$z=re^{i\theta}=r(\cos(\theta)+i\sin(\theta)),$$

όπου $r,\theta\in\mathbb{R}$, $r>0$. Συνεπώς το σύνολο των αριθμών $w\in\mathbb{C}$, ώστε $e^w=z$ είναι το σύνολο

$$\ln r+i(\theta+2\pi k),k\in\mathbb{Z}, \tag{I.21}$$

Δηλαδή υπάρχουν περισσότερες από μία μιγαδικές τιμές οι οποίες απεικονίζονται στον z. Μάλιστα το σύνολο των τιμών αυτών όπως περιγράφονται από την εξίσωση (I.21) είναι μια τροχιά της δράσης της ομάδας $2\pi i\mathbb{Z}$ όπως αυτή περιγράφηκε στο παράδειγμα I.8.36. Η δε συνάρτηση $exp:\mathbb{C}\to\mathbb{C}^*$ είναι μια ακόμα υλοποίηση του πηλίκου $\mathbb{C}/2\pi i\mathbb{Z}$.

Στο σχήμα I.19 δείχνουμε το πραγματικό κομμάτι της συνάρτησης λογαρίθμου. Παρατηρούμε ότι εξαρτάται από το μέτρο ενός μιγαδικού αριθμού, συνεπώς το γράφημα προκύπτει αν θεωρήσουμε την επιφάνεια που διαγράφει η πραγματική συνάρτηση λογαρίθμου του σχήματος I.18 γύρω από τον άξονα των y. Το μιγαδικό μέρος της συνάρτησης λογαρίθμου το οποίο απεικονίζεται στο δεξιό κομμάτι του σχήματος I.19 δεν είναι συνάρτηση με βάση τον ορισμό που έχουμε δώσει, όπου απαιτήσαμε μια τιμή του συνόλου της αφετηρίας να πηγαίνει σε μια και μοναδική τιμή του συνόλου τιμών. Μπορούμε να αντιμετωπίσουμε το θέμα με την θεωρία των καλυπτικών συναρτήσεων επιφανειών Riemann (κεφάλαια V,VI [19]), μια κάπως προχωρημένη θεωρία, ή μπορεί απλά να πούμε ότι

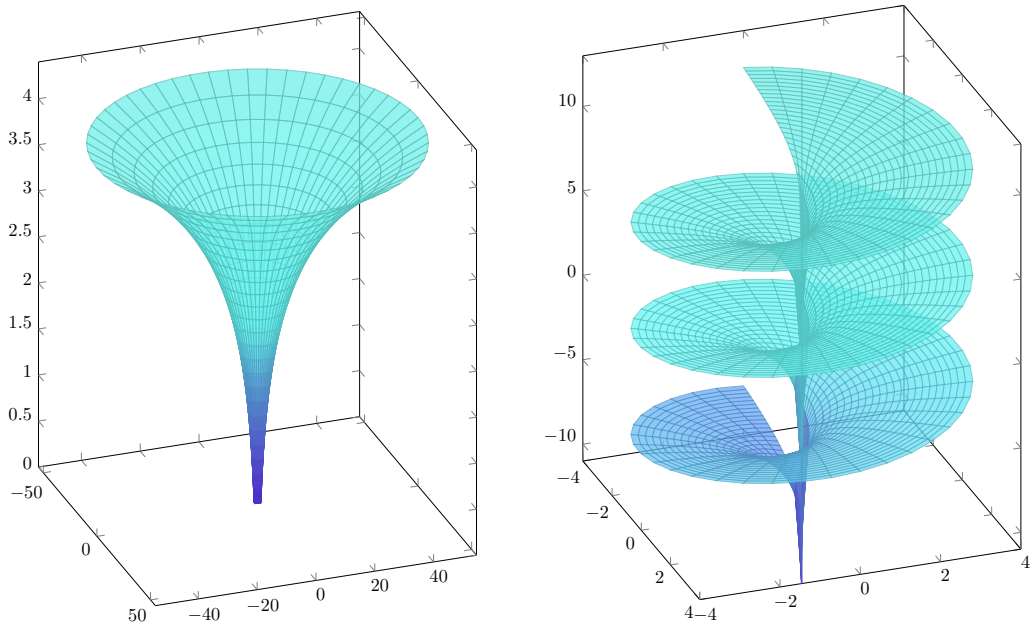
$$\log(z)=\ln r+i\theta,\ \text{όπου}\ 0\leq\theta<2\pi.$$

Ασκήσεις

Άσκηση I.23 Αποδείξτε ότι $\cos^2(t)+\sin^2(t)=1$.

Άσκηση I.24 Αποδείξτε ότι για $a\in\mathbb{R}$ ισχύει

$$\sum_{\nu=0}^{n}\cos(\nu a)=\frac{\cos\left(\frac{na}{2}\right)\sin\left(\frac{(n+1)a}{2}\right)}{\sin\left(\frac{a}{2}\right)}.$$



Σχήμα Ι.19: Αριστερά αποτυπώνεται η γραφική παράσταση του πραγματικού μέρος της συνάρτησης λογαρίθμου και δεξιά του φανταστικού μέρους. Παρατηρήστε την ιδιομορφία στο 0 που παρουσιάζει το πραγματικό μέρος της συνάρτησης λογαρίθμου.