Κεφάλαιο 0

Προκαταρκτικές Έννοιες: Σύνολα και Αριθμοί

Στο παρόν εισαγωγικό Κεφάλαιο, υπενθυμίζουμε, κατά κύριο λόγο χωρίς αποδείξεις, βασικές γνώσεις από: τη στοιχειώδη θεωρία συνόλων και απεικονίσεων, την αριθμητική των φυσικών αριθμών, συμπεριλαμβανομένης της Αρχής Μαθηματικής Επαγωγής και των ισοδυνάμων της, την διαιρετότητα των ακεραίων αριθμών, και τις στοιχειώδεις ιδιότητες των μιγαδικών αριθμών. Επίσης εισάγουμε συμβολισμό ο οποίος θα είναι εν χρήσει καθ' όλη τη διάρκεια των σημειώσεων.

0.1 Σύνολα

Στη βάση των σύγχρονων Μαθηματικών βρίσκεται η έννοια του συνόλου. Στις παρούσες σημειώσεις δεν θα προσπαθήσουμε να ορίσουμε αυστηρά την έννοια του συνόλου, η οποία είναι πρωταρχική έννοια, αλλά θα ακολουθήσουμε τον μη αυστηρό ορισμό σύμφωνα με τον οποίο ένα **σύνολο** είναι μια συλλογή καλά ορισμένων και διακεκριμένων αντικειμένων, τα οποία μπορεί να σχετίζονται ή να μην σχετίζονται μεταξύ τους. Υποθέτουμε ότι ο αναγνώστης έχει μια στοιχειώδη οικειότητα με τα συνόλα και τις βασικές ιδιοτήτες τους, κάποιες από τις οποίες θα επαναλάβουμε εδώ χάριν ευκολίας του αναγνώστη και για να σταθεροποιήσουμε συμβολισμό ο οποίος θα είναι εν χρήσει καθ' όλη τη διάρκεια του κειμένου που ακολουθεί. Ιδιαίτερα θεωρούμε γνωστές τις έννοιες της συνεπαγωγής «$\Longrightarrow$» ή «$\Longleftarrow$», της έννοιας της ισοδυναμίας «$\Longleftrightarrow$», της έννοιας του ποσοδείκτη *για κάθε* «$\forall$», και της έννοιας του *υπάρχει* «$\exists$», μεταξύ μαθηματικών αντικειμένων ή μαθηματικών προτάσεων.

0.1.1 Σύνολα Αριθμών

Από τώρα και στο εξής θα χρησιμοποιούμε τα εξής οικεία σύμβολα:

$$\mathbb{N} = \{1, 2, \cdots, n, \cdots\}, \qquad \mathbb{N}_0 = \{0, 1, 2, \cdots, n, \cdots\}, \qquad \mathbb{N}_n = \{1, 2, \cdots, n\}$$

$$\mathbb{Z} = \{\cdots, -n, \cdots, -1, 0, 1, \cdots, n, \cdots, \}, \qquad \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

για τα σύνολα: $\mathbb{N}$ των φυσικών αριθμών, $\mathbb{N}_0$ των φυσικών αριθμών μαζί με το 0, $\mathbb{N}_n$ των n πρώτων φυσικών αριθμών, $\mathbb{Z}$ των ακεραίων αριθμών, και $\mathbb{Q}$ των ρητών αριθμών.

Επιπρόσθετα συμβολίζουμε με $\mathbb{R}$ το σύνολο των πραγματικών αριθμών και με $\mathbb{C}$ το σύνολο των μιγαδικών αριθμών, και θεωρούμε γνωστές τις βασικές στοιχειώδεις ιδιότητες των συνόλων αριθμών: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$.

0.1.2 Βασικές Έννοιες

Έστω X ένα σύνολο, το οποίο αποτελείται από αντικείμενα $a, b, c, \cdots$. Θα γράφουμε $a \in X$, υποδηλώνοντας ότι το αντικείμενο a είναι στοιχείο του συνόλου X ή ότι το αντικείμενο a ανήκει στο σύνολο X. Αν ένα

αντικείμενο a δεν ανήκει στο σύνολο X, θα γράφουμε $a \notin X$. Δύο σύνολα X και Y είναι ίσα, και τότε θα γράφουμε $X = Y$, αν κάθε στοιχείο του X είναι και στοιχείο του Y και κάθε στοιχείο του Y είναι και στοιχείο του X, δηλαδή αν: $\forall x \in X \Longrightarrow x \in Y$ και $\forall y \in Y \Longrightarrow y \in X$. Αν τα σύνολα X και Y δεν είναι ίσα, θα γράφουμε $X \neq Y$. Ένα σύνολο Y είναι **υποσύνολο** του συνόλου X, και τότε θα γράφουμε $Y \subseteq X$ ή $Y \subsetneqq X$ (σπανιότερα $X \supseteq Y$ ή $X \supsetneqq Y$), αν κάθε στοιχείο y του Y είναι και στοιχείο του X, δηλαδή αν: $y \in Y \Longrightarrow y \in X$. Αν το σύνολο Y είναι υποσύνολο του X και $Y \neq X$, θα λέμε ότι το Y είναι **γνήσιο υποσύνολο** του X και θα γράφουμε $Y \subset X$ ή $Y \subsetneq X$ ή $Y \subsetneqq X$. Σύμφωνα με αυτή την ορολογία, θα έχουμε: $X = Y$ αν και μόνο αν $Y \subseteq X$ και $X \subseteq Y$. Το **κενό σύνολο** είναι το σύνολο το οποίο δεν περιέχει κανένα στοιχείο, συμβολίζεται με $\emptyset$ και είναι υποσύνολο κάθε συνόλου. Ένα σύνολο X καλείται *μη κενό*, αν περιέχει τουλάχιστον ένα στοιχείο, και τότε θα γράφουμε $X \neq \emptyset$. Ένα σύνολο μπορεί να καθοριστεί με πολλούς τρόπους, για παράδειγμα με αναγραφή των στοιχείων του (συνήθως όταν περιέχει πεπερασμένο πλήθος στοιχείων) ή με χρήση κάποιας ιδιότητας (ή συνόλου ιδιοτήτων) την οποία ικανοποιούν τα στοιχεία του συνόλου. Έτσι, αν το σύνολο X αποτελείται από ένα πεπερασμένο πλήθος στοιχείων, έστω $x_1, x_2, \cdots, x_n$, τότε θα γράφουμε:

$$X = \{x_1, x_2, \cdots, x_n\}$$

Παρόμοια, αν P είναι μια ιδιότητα η οποία αφορά κάποια μαθηματικά ή μη αντικείμενα, τα οποία συνήθως είναι στοιχεία ενός συνόλου A, τότε το σύνολο όλων των αντικειμένων του συνόλου A, τα οποία ικανοποιούν την ιδιότητα P, θα συμβολίζεται με

$$X = \{x \in A \mid \text{το } x \text{ ικανοποιεί την ιδιότητα } P\}$$

Αν τα αντικείμενα τα οποία ικανοποιούν την ιδιότητα P δεν είναι στοιχεία κάποιου μεγαλύτερου συνόλου, τότε θα γράφουμε $X = \{x \mid \text{το } x \text{ ικανοποιεί την ιδιότητα } P\}$. Για παράδειγμα, αν $\mathbb{N} = \{1, 2, \cdots, n, n+1, \cdots\}$ είναι το σύνολο των θετικών ακεραίων ή φυσικών αριθμών, τότε το σύνολο το οποίο αποτελείται από όλους τους φυσικούς αριθμούς οι οποίοι είναι το πολύ ίσοι με 5 είναι $X = \{1, 2, 3, 4, 5\}$. Αν X είναι το σύνολο το οποίο αποτελείται από όλους τους θετικούς ακέραιους αριθμούς της μορφής $2n$, όπου n είναι τυχών θετικός αριθμός, τότε $X = \{a \in \mathbb{N} \mid \text{ο } a \text{ είναι άρτιος}\}$. Αν $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ είναι το σύνολο των ακεραίων αριθμών, τότε το σύνολο των θετικών ακεραίων ή φυσικών αριθμών είναι: $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\} = \{1, 2, \cdots, n, \cdots\}$.

0.1.3 Πράξεις και Κατασκευές Συνόλων

Αν X είναι σύνολο, τότε το **δυναμοσύνολο** του συνόλου X ορίζεται να είναι το σύνολο όλων των υποσυνόλων του συνόλου X, και συμβολίζεται με $\mathscr{P}(X)$:

$$\mathscr{P}(X) = \{A \mid A \subseteq X\}$$

Το δυναμοσύνολο $\mathscr{P}(X)$ περιέχει πάντοτε ως στοιχεία του το κενό σύνολο $\emptyset$ και το σύνολο X.

Έστω ότι X είναι ένα σύνολο και ότι A και B είναι δύο υποσύνολα του X. Η **τομή** $A \cap B$ των υποσυνόλων A και B ορίζεται να είναι το σύνολο όλων των στοιχείων του X τα οποία ανήκουν στο A και στο B:

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

Τα υποσύνολα A και B καλούνται **ξένα** αν $A \cap B = \emptyset$. Η **ένωση** $A \cup B$ των υποσυνόλων A και B ορίζεται να είναι το σύνολο όλων των στοιχείων του X τα οποία ανήκουν είτε στο A είτε στο B:

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

Η ένωση $A \cup B$ των υποσυνόλων A και B καλείται **ξένη ένωση**, αν: $A \cap B = \emptyset$.

Για την τομή και την ένωση υποσυνόλων ενός συνόλου ισχύουν οι εξής σχέσεις γνωστές ως Νόμοι του De Morgan.

Πρόταση 0.1.1 (Νόμοι του De Morgan). [1] *Αν A, B, και C είναι υποσύνολα ενός συνόλου X, τότε:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{και} \quad A \cup (B \cap C) = A \cup B) \cap (A \cup C)$$

[1] Augustus De Morgan (27 Ιουνίου 1806 - 18 Μαρτίου 1871) [https://en.wikipedia.org/wiki/Augustus_De_Morgan]: Βρετανός μαθηματικός και θεωρητικός της Λογικής. Γνωστός για τους νόμους που φέρουν το όνομά του.

Έστω ότι A και B είναι δύο υποσύνολα ενός συνόλου X. Η **διαφορά** $A \setminus B$ **των συνόλων** A και B ορίζεται να είναι το σύνολο των στοιχείων του A τα οποία δεν ανήκουν στο B:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

Αν $B \subseteq A$, τότε η διαφορά $A \setminus B$ καλείται το **συμπλήρωμα** του B στο A.

Έστω I ένα σύνολο με στοιχεία $i, j, k, \cdots$. Έστω $\mathscr{A}$ μια συλλογή ή οικογένεια συνόλων, δηλαδή ένα σύνολο $\mathscr{A}$ τα στοιχεία του οποίου είναι επίσης σύνολα. Το σύνολο I καλείται **σύνολο δεικτών** για την οικογένεια συνόλων $\mathscr{A}$, αν για κάθε στοιχείο $i \in I$ υπάρχει ένα σύνολο A_i το οποίο ανήκει στην οικογένεια $\mathscr{A}$. Τότε θα γράφουμε $\mathscr{A} = \{A_i\}_{i \in I}$. Αν το σύνολο δεικτών I για την οικογένεια συνόλων $\mathscr{A}$ είναι πεπερασμένο, για παράδειγμα αν $I = \{1, 2, \cdots, n\}$, τότε $\mathscr{A} = \{A_i\}_{i \in I} = \{A_1, A_2, \cdots, A_n\}$. Για παράδειγμα, δύο σύνολα A_1 και A_2 αποτελούν τα στοιχεία μιας οικογένειας συνόλων $\{A_1, A_2\}$ όπου $I = \{1, 2\}$. Όπως και στην περίπτωση δύο υποσυνόλων ενός συνόλου, έτσι και στην περίπτωση μιας οικογένειας υποσυνόλων $\mathscr{A} = \{A_i\}_{i \in I}$ ενός συνόλου X, όπου I είναι ένα μη κενό σύνολο δεικτών, μπορούμε να ορίσουμε την έννοια της τομής και ένωσης των συνόλων της οικογένειας, ως εξής. Η **τομή** $\cap_{i \in I} A_i$ **της οικογένειας συνόλων** $\mathscr{A}$ ορίζεται να είναι το σύνολο

$$\bigcap_{i \in I} A_i = \{x \in X \mid x \in A_i,\ \forall i \in I\}$$

Η **ένωση** $\cup_{i \in I} A_i$ **της οικογένειας συνόλων** $\mathscr{A}$ ορίζεται να είναι το σύνολο

$$\bigcup_{i \in I} A_i = \{x \in X \mid \exists i \in I : x \in A_i\}$$

Η ένωση $\cup_{i \in I} A_i$ της οικογένειας υποσυνόλων $\mathscr{A} = \{A_i\}_{i \in I}$ ενός συνόλου X καλείται **ξένη ένωση**, αν για κάθε $i, j \in I$: $i \neq j \Longrightarrow A_i \cap A_j = \emptyset$.

Αν το σύνολο I είναι πεπερασμένο, έστω για παράδειγμα $I = \{1, 2, \cdots, n\}$, τότε θα γράφουμε:

$$\bigcap_{i \in I} A_i = \bigcap_{i=1}^{n} A_i = A_1 \bigcap A_2 \bigcap \cdots \bigcap A_n \quad \text{και} \quad \bigcup_{i \in I} A_i = \bigcup_{i=1}^{n} A_i = A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n$$

Παρόμοια μπορουμε να ορίσουμε την τομή $\cap_{A \in \mathscr{K}} A$ και την ένωση $\cup_{A \in \mathscr{K}} A$ μιας οικογένειας υποσυνόλων $\mathscr{K} \subseteq \mathscr{P}(X)$ ενός συνόλου X ως εξής:

$$\bigcap_{A \in \mathscr{K}} A = \{x \in X \mid \forall A \in \mathscr{K} :\ x \in A\} \quad \text{και} \quad \bigcup_{A \in \mathscr{K}} A = \{x \in X \mid \exists A \in \mathscr{K} :\ x \in A\}$$

Έστω A και B δύο (μη κενά) σύνολα. Το (**καρτεσιανό**) **γινόμενο** $A \times B$ των συνόλων A και B ορίζεται να είναι το σύνολο όλων των διατεταγμένων ζευγών (a, b), όπου $a \in A$ και $b \in B$:

$$A \times B = \{(a, b) \mid a \in A \text{ και } b \in B\}$$

και όπου δύο διατεταγμένα ζεύγη $(a, b), (c, d) \in A \times B$ θεωρούνται ίσα, $(a, b) = (c, d)$, αν: $a = c$ και $b = d$.

Έτσι, για παράδειγμα, αν $A = \{1, 2, 3\}$ και $B = \{a, b\}$, τότε $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Γενικεύοντας, αν $A_1, A_2, \cdots, A_n$ είναι n το πλήθος σύνολα, τότε το (**καρτεσιανό**) **γινόμενο** $\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n$ των συνόλων A_i, $1 \leq i \leq n$, ορίζεται να είναι το σύνολο όλων των διατεταγμένων n-άδων $(a_1, a_2, \cdots, a_n)$, όπου $a_i \in A_i$, $1 \leq i \leq n$:

$$\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i,\ 1 \leq i \leq n\}$$

και όπου δύο διατεταγμένες n-άδες $(a_1, a_2, \cdots, a_n)$, $(a'_1, a'_2, \cdots, a'_n) \in A \times B$ θεωρούνται ίσες, $(a_1, a_2, \cdots, a_n) = (a'_1, a'_2, \cdots, a'_n)$, αν: $a_i = a'_i$, $1 \leq i \leq n$.

0.2 Απεικονίσεις

Αν X είναι ένα μη κενό σύνολο, τότε μια **(διμελής) σχέση επί του** X είναι ένα υποσύνολο του καρτεσιανού γινομένου $X \times X$. Έστω X, Y δύο μη κενά σύνολα. Γενικεύοντας την έννοια της σχέσης επί ενός συνόλου, ορίζουμε μια **σχέση από το** X **στο** Y, ή μια *αντιστοιχία από το* X *στο* Y, να είναι ένα υποσύνολο του καρτεσιανού γινομένου $X \times Y$. Θα μας απασχολήσουν κυρίως οι ακόλουθες ειδικού τύπου σχέσεις από ένα σύνολο X σε ένα σύνολο Y:

Μια **απεικόνιση** $\mathscr{R}$ **από το** X **στο** Y είναι μια σχέση $\mathscr{R}$ από το X στο Y η οποία ικανοποιεί τις ακόλουθες ιδιότητες:

1. $\forall x \in X,\ \exists y \in Y\colon \quad (x,y) \in \mathscr{R}$.

2. $(x,y) \in \mathscr{R}$ και $(x,y') \in \mathscr{R} \implies y = y'$.

Δηλαδή, για κάθε $x \in X$ υπάρχει ακριβώς ένα στοιχείο $y \in Y$, έτσι ώστε $(x,y) \in \mathscr{R}$. Ισοδύναμα:

$$\forall x \in X,\ \exists y \in Y\colon\ (x,y) \in \mathscr{R} \quad \text{και} \quad (x,y_1),\ (x,y_2) \in \mathscr{R} \implies y_1 = y_2$$

Συνήθως μια απεικόνιση από το X στο σύνολο Y θα συμβολίζεται με ένα από τα παρακάτω σύμβολα:

$$f,\ g,\ h,\ \varphi,\ \psi,\ \cdots$$

Έστω $f \subseteq X \times Y$ μια απεικόνιση από το σύνολο X στο σύνολο Y. Τότε για κάθε $x \in X$, το μοναδικό, σύμφωνα με τον παραπάνω ορισμό, στοιχείο $y \in Y$, για το οποίο ισχύει $(x,y) \in f$, συμβολίζεται με $f(x) = y$, και η απεικόνιση f θα συμβολίζεται ως εξής:

$$f\colon X \longrightarrow Y,\quad x \longmapsto f(x)$$

Από τώρα και στο εξής θα χρησιμοποιούμε τον παραπάνω οικείο συμβολισμό για τις απεικονίσεις.

Έστω $f\colon X \longrightarrow Y$ μια απεικόνιση, και $A \subseteq X$ και $B \subseteq Y$ δύο υποσύνολα. Υπενθυμίζουμε ότι το υποσύνολο του Y

$$f(A) = \big\{y \in Y \mid \exists x \in A\colon y = f(x)\big\} = \big\{f(x) \in Y \mid x \in A\big\}$$

καλείται η **εικόνα** του A μέσω της f, και το υποσύνολο του X

$$f^{-1}(B) = \big\{x \in X \mid f(x) \in B\big\}$$

καλείται η **αντίστροφη εικόνα** του B μέσω της f. Ειδικότερα, θέτοντας $A = X$, έχουμε την **εικόνα** της f:

$$\mathsf{Im}(f) = f(X)$$

• ΠΟΤΕ ΔΥΟ ΑΠΕΙΚΟΝΙΣΕΙΣ ΕΙΝΑΙ ΙΣΕΣ; Επειδή ορίσαμε τις απεικονίσεις ως υποσύνολα καρτεσιανών γινομένων, δηλαδή ως τριάδες (X,Y,f), όπου $f \subseteq X \times Y$, διαπιστώνουμε ότι δύο απεικονίσεις (X,Y,f) και (X',Y',f'), δηλαδή $f\colon X \longrightarrow Y$ και $f'\colon X' \longrightarrow Y'$, είναι ίσες, και θα γράφουμε $f = f'$, αν και μόνο αν $(X,Y,f) = (X',Y',f')$, δηλαδή αν και μόνο αν $X = X', Y = Y'$ και τα υποσύνολα $f \subseteq X \times Y$ και $f' \subseteq X \times Y$ είναι ίσα. Το τελευταίο ιδιαίτερα σημαίνει ότι $f(x) = f'(x),\ \forall x \in X$. Επομένως, δύο απεικονίσεις $f, f'\colon X \longrightarrow Y$ είναι ίσες αν και μόνο αν $f(x) = f'(x),\ \forall x \in X$.

Τονίζουμε ιδιαίτερα ότι δύο απεικονίσεις $f\colon X \longrightarrow Y$ και $f'\colon Z \longrightarrow W$, όπου $X \neq Z$ ή $Y \neq W$, δεν είναι ποτέ ίσες. Για παράδειγμα, οι απεικονίσεις $f\colon \mathbb{N} \longrightarrow \mathbb{N},\ f(n) = 3n+5$, και $f'\colon \mathbb{N} \longrightarrow \mathbb{Z},\ f'(n) = 3n+5$ δεν είναι ίσες, μολονότι $f(n) = f'(n)$, για κάθε στοιχείο $n \in \mathbb{N}$.

Παράδειγμα 0.2.1. Για κάθε μη κενό σύνολο X, μπορούμε να θεωρήσουμε την **ταυτοτική** απεικόνιση

$$\mathsf{Id}_X\colon X \longrightarrow X,\ \ \mathsf{Id}_X(x) = x$$

η οποία ως υποσύνολο του $X \times X$ είναι η «διαγώνιος» $\mathsf{Id}_X = \big\{(x,x) \in X \times X \mid x \in X\big\}$. $\quad\surd$

Παράδειγμα 0.2.2. Έστω $S \subseteq X$ ένα υποσύνολο του συνόλου X. Τότε ορίζεται η **απεικόνιση έγκλεισης**

$$\iota_S \colon S \longrightarrow X, \quad \iota_S(s) = s$$

του υποσυνόλου S στο X. Παρατηρούμε ότι, αν και οι απεικονίσεις ι_S και Id_S ικανοποιούν τη σχέση $\iota_S(s) = s = \mathsf{Id}_S(s)$, $\forall s \in S$, δεν είναι ίσες. $\surd$

Παράδειγμα 0.2.3. Έστω X ένα μη κενό σύνολο, και $A \subseteq X$ ένα υποσύνολό του. Αν θέσουμε $\mathbf{2} = \{0,1\}$, τότε η **χαρακτηριστική συνάρτηση** του A ορίζεται να είναι η απεικόνιση

$$\chi_A \,:\, X \longrightarrow \mathbf{2}, \quad \chi_A(a) = \begin{cases} 1, & a \in A \\ 0, & a \notin A \end{cases} \quad \surd$$

Παράδειγμα 0.2.4. Έστω $f \colon X \longrightarrow Y$ μια απεικόνιση μεταξύ συνόλων. Αν $A \subseteq X$, είναι ένα μη κενό υποσύνολο του X, τότε ορίζεται η απεικόνιση

$$f|_A \colon A \longrightarrow Y, \quad f|_A(a) = f(a)$$

η οποία καλείται ο **περιορισμός της** f **στο υποσύνολο** A. Προφανώς $f|_A = f \circ \iota_A$. $\surd$

Κλείνουμε την παρούσα υποενότητα με παραδείγματα απεικονίσεων οι οποίες προκύπτουν με χρήση καρτεσιανών γινομένων συνόλων. Οι απεικονίσεις οι οποίες ορίζονται παρακάτω χαρακτηρίζονται μοναδικά από μια ιδιότητα.

Παράδειγμα 0.2.5. Έστω $\prod_{k=1}^{n} X_k := X_1 \times X_2 \times \cdots \times X_n$ το καρτεσιανό γινόμενο μιας πεπερασμένης οικογένειας $\{X_k\}_{k=1}^{n}$ μη κενών συνόλων. Τότε, για κάθε δείκτη $k = 1,2,\cdots,n$, ορίζεται η k-**οστή απεικόνιση-προβολής**

$$\pi_k \,:\, \prod_{k=1}^{n} X_k \;\longrightarrow\; X_k, \quad \pi_k(x_1, x_2, \cdots, x_n) = x_k$$

Η οικογένεια $\{\pi_k\}_{k=1}^{n}$ των απεικονίσεων-προβολών, ικανοποιεί την ακόλουθη ιδιότητα: *Αν A είναι ένα μη κενό σύνολο και $f_k \colon A \longrightarrow X_k$ είναι απεικονίσεις, $1 \le k \le n$, τότε υπάρχει μοναδική απεικόνιση $f \colon A \longrightarrow \prod_{k=1}^{n} X_k$, έτσι ώστε: $\pi_k \circ f = f_k$, $1 \le k \le n$.* Πράγματι οριζουμε μια απεικόνιση

$$f \colon A \longrightarrow \prod_{k=1}^{n} X_k, \quad f(a) = \big(f_1(a), f_2(a), \cdots, f_n(a)\big)$$

και τότε, $\forall k = 1,2,\cdots,n$:

$$\forall a \in A: \qquad (\pi_k \circ f)(a) = \pi_k(f(a)) = \pi_k\big(f_1(a), f_2(a), \cdots, f_n(a)\big) = f_k(a)$$

Άρα πράγματι $\pi_k \circ f = f_k$, $1 \le k \le n$. Έστω ότι $g \colon A \longrightarrow \prod_{k=1}^{n} X_k$ είναι μια άλλη απεικόνιση για την οποία ισχύει ότι $\pi_k \circ g = f_k$, $1 \le k \le n$. Για κάθε στοιχείο $a \in A$, θέτοντας $g(a) = (x_1, x_2, \cdots, x_n)$, θα έχουμε:

$$\pi_k(g(a)) = \pi_k(x_1, x_2, \cdots, x_n) \quad \Longrightarrow \quad f_k(a) = x_k, \quad 1 \le k \le n \quad \Longrightarrow \quad g(a) = \big(f_1(a), f_2(a), \cdots, f_n(a)\big), \quad \forall a \in A$$

Επομένως $g = f$. $\surd$

Παράδειγμα 0.2.6. Έστω $f_k \colon X_k \longrightarrow Y_k$, $1 \le k \le n$, μια οικογένεια απεικονίσεων. Τότε ορίζεται η **απεικόνιση-γινόμενο** $\prod_{k=1}^{n} f_k := f_1 \times f_2 \times \cdots \times f_k \colon \prod_{k=1}^{n} X_k \;\longrightarrow\; \prod_{k=1}^{n} Y_k$, ως εξής:

$$\prod_{k=1}^{n} f_k \,:\, \prod_{k=1}^{n} X_k \;\longrightarrow\; \prod_{k=1}^{n} Y_k, \quad \big(\prod_{k=1}^{n} f_k\big)(x_1, x_2, \cdots, x_n) = (f_1(x_1), f_2(x_2), \cdots, f_n(x_n))$$

Η απεικόνιση $\prod_{k=1}^n \colon \prod_{k=1}^n X_k \longrightarrow \prod_{k=1}^n Y_k$ ικανοποιεί τις σχέσεις $\pi_k^Y \circ \prod_{k=1}^n f_k = f_k \circ \pi_k^X$, $1 \le k \le n$, όπου $\pi_k^X \colon \prod_{k=1}^n X_k \longrightarrow X_k$ και $\pi_k^Y \colon \prod_{k=1}^n Y_k \longrightarrow U_k$ είναι οι αντίστοιχες απεικονίσεις προβολές, όπως στο Παράδειγμα 0.2.5. Πράγματι, για κάθε στοιχείο $x = (x_1, \cdots, x_n) \in \prod_{k=1}^n X_k$, και για κάθε $k = 1, 2, \cdots, n$, θα έχουμε:

$$(\pi_k^Y \circ \prod_{k=1}^n f_k)(x) = \pi_k^Y\big((\prod_{k=1}^n f_k)(x_1, \cdots, x_n)\big) = \pi_k^Y(f_1(x_1), \cdots, f_n(x_n)) = f_k(x_k) = f_k(\pi_k^X(x_1, \cdots, x_n) = (f_k \circ \pi_k^X)(x)$$

από όπου έπεται ότι: $\pi_k^Y \circ \prod_{k=1}^n f_k = f_k \circ \pi_k^X$, $1 \le k \le n$. Η απεικόνιση-γινόμενο $\prod_{k=1}^n f_k$ είναι η μοναδική η οποία ικανοποιεί τις παραπάνω σχέσεις διότι, αν $g \colon \prod_{k=1}^n X_k \longrightarrow \prod_{k=1}^n Y_k$ είναι μια άλλη απεικόνιση για την οποία ισχύει ότι: $\pi_k^Y \circ g = f_k \circ \pi_k^X$, $1 \le k \le n$, τότε για κάθε στοιχείο $x = (x_1, \cdots, x_n \in \prod_{k=1}^n X_k$ θα έχουμε:

αν $g(x) = (y_1, \cdots, y_n)$, τότε $\pi_k(g(x)) = \pi_k(y_1, \cdots, y_n) \implies f_k \pi_k^X(x) = y_k, \implies f_k(x_k) = y_k, \quad 1 \le k \le n$

δηλαδή $g(x_1, \cdots, x_n = (f_1(x_1, \cdots, f_n(x_n))$, και άρα $g = \prod_{k=1}^n f_k$. $\quad \surd$

Έστω $\mathscr{A} = \{A_i\}_{i \in I}$ μια οικογένεια συνόλων, όπου I είναι ένα σύνολο δεικτών. Μια I-**άδα στοιχείων** των συνόλων A_i, $i \in I$, είναι μια απεικόνιση $f \colon I \longrightarrow \cup_{i \in I} A_i$, έτσι ώστε $f(i) \in A_i$. Συνήθως μια I-άδα στοιχείων f συμβολίζεται με αναγραφή των τιμών της $f(i) := a_i \in A_i$ ως στοιχείων μιας ακολουθίας $(a_i)_{i \in I}$, όπου $a_i \in A_i$, $\forall i \in I$. Για παράδειγμα, αν $I = \{1, 2, 3\}$, και $f \colon I \longrightarrow A_1 \cup A_2 \cup A_3$ είναι μια I-άδα στοιχείων, τότε, θέτοντας $f(1) = a_1$, $f(2) = a_2$, και $f(3) = a_3$, μπορούμε να γράψουμε ισοδύναμα την f ως (a_1, a_2, a_3), δηλαδή ως μια τριάδα στοιχείων. Αν $I = \{1, 2, \cdots, n\}$, τότε μια I-άδα στοιχείων είναι απλώς μια n-άδα στοιχείων.

Το (**καρτεσιανό**) **γινόμενο** $\prod_{i \in I} A_i$ της οικογένειας συνόλων $\mathscr{A} = \{A_i\}_{i \in I}$, όπου I είναι ένα σύνολο δεικτών, ορίζεται να είναι το σύνολο όλων των I-άδων στοιχείων των συνόλων A_i, $i \in I$:

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} \mid a_i \in A_i, \ \forall i \in I\}$$

0.2.1 Η Άλγεβρα των Απεικονίσεων

Υπενθυμίζουμε ότι, αν $f \colon X \longrightarrow Y$ και $g \colon W \longrightarrow Z$ είναι απεικονίσεις και $Y = W$, τότε (και μόνο τότε) ορίζεται η «*σύνθεση*» των απεικονίσεων f και g ως το ακόλουθο υποσύνολο του $X \times Z$:

$$g \circ f = \{(x, z) \in X \times Z \mid (f(x), z) \in g \subseteq Y \times Z\}$$

Με άλλα λόγια $g \circ f$ είναι η απεικόνιση

$$g \circ f \colon X \longrightarrow Z, \quad (g \circ f)(x) = g(f(x))$$

Υπενθυμίζουμε επίσης ότι, αν $f \colon X \longrightarrow Y$, $g \colon Y \longrightarrow Z$, και $h \colon Z \longrightarrow W$ είναι απεικονίσεις, τότε ορίζονται οι συνθέσεις $h \circ (g \circ f)$ και $(h \circ g) \circ f$ και ισχύει

$$\text{Αν} \quad X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W \quad \text{τότε} \quad h \circ (g \circ f) = (h \circ g) \circ f \qquad \text{(προσεταιριστική ιδιότητα σύνθεσης)}$$

Πράγματι οι συνθέσεις $g \circ f$, $h \circ (g \circ f)$, και $h \circ g$, $(h \circ g) \circ f$ ορίζονται και $\forall x \in X$:

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

Παρατηρούμε ότι:

$$\text{για κάθε απεικόνιση} \quad f \colon X \longrightarrow Y \quad \text{ισχύει ότι:} \quad \mathsf{Id}_Y \circ f = f \quad \& \quad f \circ \mathsf{Id}_X = f$$

Παρατήρηση 0.2.7. Αν $f,g\colon X\longrightarrow X$ είναι απεικονίσεις επί ενός συνόλου X, έτσι ώστε οι συνθέσεις $f\circ g$ και $g\circ f$ ορίζονται, γενικά οι απεικονίσεις $f\circ g$ και $g\circ f$ δεν είναι ίσες. Το μικρότερο σύνολο X στο οποίο μπορούμε να δούμε ότι $f\circ g\neq g\circ f$, είναι να θεωρήσουμε ένα σύνολο X με δύο στοιχεία: $X=\{a,b\}$. Τότε ορίζουμε απεικόνιση $f\colon X\longrightarrow X$, ως εξής: $f(a)=b$, $f(b)=b$, και απεικόνιση $g\colon X\longrightarrow X$, ως εξής: $g(a)=a$, $g(b)=a$. Θα έχουμε $(f\circ g)(a)=f(g(a))=f(a)=b$ και $(g\circ f)(a)=g(f(a))=g(b)=a$. Επομένως $(f\circ g)(a)\neq(g\circ f)(a)$, και άρα $f\circ g\neq g\circ f$.

Αν το σύνολο $X=\{a,b,\cdots\}$ έχει παραπάνω από δύο στοιχεία, τότε, ορίζοντας απεικονίσεις $f,g\colon X\longrightarrow X$ να έχουν τιμές στα στοιχεία a και b όπως παραπάνω, και θέτοντας $f(x)=x=g(x)$, $\forall x\in X\setminus\{a,b\}$, αποκτούμε απεικονίσεις f, g επί του X έτσι ώστε $f\circ g\neq g\circ f$. Προφανώς, αν το σύνολο X έχει ένα στοιχείο $X=\{a\}$, τότε $f\circ g=g\circ f$ διότι η μοναδική απεικόνιση $f\colon X\longrightarrow X$ είναι η ταυτοτική $f=\mathsf{Id}_X$. ▲

Έστω $f\colon X\longrightarrow Y$ μια απεικόνιση. Παραπάνω ορίσαμε την αντίστροφη εικόνα $f^{-1}(B)$ κάθε υποσυνόλου του X να είναι το υποσύνολο $\{x\in X\mid f(x)\in B\}$. Ιδιαίτερα έχουμε το υποσύνολο $f^{-1}(Y)=\{x\in X\mid f(x)\in Y\}$. Παρατηρούμε ότι υπάρχουν τουλάχιστον δύο προβλήματα αν προσπαθήσουμε να ορίσουμε «απεικόνιση» $f^{-1}\colon Y\longrightarrow X$ ως εξής: $f^{-1}(y)=x$, όπου $f(x)=y$. Πράγματι: (α) για δεδομένο στοιχείο $y\in Y$, μπορεί να μην υπάρχει στοιχείο $x\in X$ έτσι ώστε $f(x)=y$, δηλαδή μπορεί $f^{-1}(\{y\})=\emptyset$, και (β) αν για δεδομένο $y\in Y$, έχουμε $f^{-1}(y)\neq\emptyset$, μπορεί να υπάρχουν διακεκριμένα στοιχεία $x_1,x_2\in f^{-1}(\{y\})$, και τότε θα είχαμε $f^{-1}(y)=x_1\neq x_2=f^{-1}(y)$. Τα προβλήματα αυτά παύουν να υπάρχουν αν η απεικόνιση f είναι (α) «επί» και (β) η απεικόνιση f είναι «1-1», με τις ακόλουθες έννοιες:

1. Η f καλείται «**απεικόνιση 1-1**» αν: $\forall x,y\in X$, $f(x)=f(y)\Longrightarrow x=y$.
2. Η f καλείται «**απεικόνιση επί**», αν: $\mathsf{Im}(f)=Y$, δηλαδή: $\forall y\in Y$, $\exists x\in X$: $f(x)=y$.
3. Η f καλείται «**αντιστρέψιμη απεικόνιση**», αν υπάρχει απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε:

$$g\circ f=\mathsf{Id}_X\qquad\&\qquad f\circ g=\mathsf{Id}_Y \tag{†}$$

Πρόταση 0.2.8. *Μια απεικόνιση $f\colon X\longrightarrow Y$ είναι «1-1» και «επί» αν και μόνο αν η f είναι αντιστρέψιμη.*
Αν $g,h\colon Y\longrightarrow X$ είναι δύο απεικόνισεις έτσι ώστε: $g\circ f=\mathsf{Id}_X=h\circ f$ και $f\circ g=\mathsf{Id}_Y=f\circ h$, τότε $g=h$.

Απόδειξη. «$\Longrightarrow$» Έστω ότι η $f\colon X\longrightarrow Y$ είναι «1-1» και «επί». Ορίζουμε μια απεικόνιση $g\colon Y\longrightarrow X$, ως εξής. Για κάθε $y\in Y$, επειδή η f είναι «επί», υπάρχει ένα στοιχείο $x\in X$ έτσι ώστε $f(x)=y$. Το στοιχείο αυτό x είνα μοναδικό διότι αν $f(x)=y$ και $f(x')=y$, τότε $f(x)=f(x')$ και επομένως $x=x'$ διότι η f είναι «1-1». Ορίζουμε $g(y)=x$, όπου x είναι το μοναδικό στοιχείο $x\in X$ έτσι ώστε $f(x)=y$. Δείχνουμε ότι: $(g\circ f)(x)=x$, $\forall x\in X$ και $(f\circ g)(y)=y$, $\forall y\in Y$. Πράγματι $(g\circ f)(x)=g(f(x))$ είναι το μοναδικό στοιχείο x' του X έτσι ώστε $f(x')=f(x)$, από όπου $x'=x$ διότι η f είναι «1-1». Άρα $g(f(x))=x$. Από την άλλη πλευρά, επειδή $g(y)$ είναι το μοναδικό στοιχείο του X έτσι ώστε $f(x)=y$, θα έχουμε $f(g(y))=f(x)=y$. Επομένως $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$, και άρα η f είναι αντιστρέψιμη.

«$\Longleftarrow$» Έστω οτι η απεικόνιση f είναι αντιστρέψιμη, και άρα υπάρχει απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$. Έστω $f(x)=f(x')$. Τότε $g(f(x))=g(f(x'))\Longrightarrow(g\circ f)(x)=(g\circ f)(x')\Longrightarrow\mathsf{Id}_X(x)=\mathsf{Id}_X(x')\Longrightarrow x=x'$ και άρα η f είναι «1-1». Από τη σχέση $g\circ f=\mathsf{Id}_X$ βλέπουμε ότι για κάθε $x\in X$ έχουμε $g(f(x))=x$, το οποίο σημαίνει ότι η g είναι «επί».

Τέλος, έστω $h\colon Y\longrightarrow X$ μια άλλη απεικόνιση έτσι ώστε $h\circ f=\mathsf{Id}_X$ και $f\circ h=\mathsf{Id}_Y$. Τότε:

$$h\circ f=\mathsf{Id}_X\implies(h\circ f)\circ g=\mathsf{Id}_X\circ g\implies h\circ(f\circ g)=g\implies h\circ\mathsf{Id}_Y=g\implies h=g$$ ■

Παρατήρηση 0.2.9. Αν $f\colon X\longrightarrow Y$ και $g\colon Y\longrightarrow X$ είναι απεικονίσεις και ισχύει ότι $g\circ f=\mathsf{Id}_X$, τότε από την απόδειξη της Πρότασης 0.2.8 έπεται ότι η f είναι «1-1» και η g είναι «επί». ▲

Αν η απεικόνιση $f\colon X\longrightarrow Y$ είναι «1-1» και «επί», ισοδύναμα η f είναι αντιστρέψιμη, σύμφωνα με την Πρόταση 0.2.8 υπάρχει μοναδική απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$. Η απεικόνιση g καλείται η **αντίστροφη απεικόνιση** της f και συμβολίζεται με $g=f^{-1}$.

Πόρισμα 0.2.10. *Έστω ότι $f\colon X \longrightarrow Y$ είναι μια αντιστρέψιμη απεικόνιση. Τότε η αντίστροφη απεικόνιση $f^{-1}\colon Y \longrightarrow X$ είναι επίσης αντιστρέψιμη αεπικόνιση και ισχύει: $(f^{-1})^{-1} = f$.*

Απόδειξη. Επειδή η f είναι αντιστρέψιμη, έπεται ότι υπάρχει η αντίστροφή της $f^{-1}\colon Y \longrightarrow X$ και ισχύει:

$$f^{-1} \circ f = \mathsf{Id}_X \quad \& \quad f \circ f^{-1} = \mathsf{Id}_Y$$

Οι παραπάνω σχέσεις δείχνουν ότι η f^{-1} είναι αντιστρέψιμη και η αντίστροφή της είναι η $(f^{-1})^{-1} = f$. ■

Παράδειγμα 0.2.11. Έστω ότι $X = \{x, y, z\}$ είναι ένα σύνολο με τρία στοιχεία, και έστω $Y = \{1, 2, 3\}$. Θεωρούμε την απεικόνιση $f\colon X \longrightarrow Y$ ως εξής: $f(x) = 2$, $f(y) = 3$ και $f(z) = 1$. Τότε προφανώς η f είναι «1-1» και «επί» και άρα η f είναι αντιστρέψιμη. Η αντίστροφή της είναι η απεικόνιση $f^{-1}\colon X \longrightarrow Y$, η οποία ορίζεται ως εξής: $f^{-1}(1) = z$, $f^{-1}(2) = x$, και $f^{-1}(3) = y$. √

Πρόταση 0.2.12. *Έστω ότι $f\colon X \longrightarrow Y$ και $g\colon Y \longrightarrow Z$ είναι απεικονίσεις.*

1. *Αν οι απεικονίσεις f, g είναι «1-1», τότε η απεικόνιση $g \circ f$ είναι «1-1». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «1-1», τότε η απεικόνιση f είναι «1-1».*

2. *Αν οι απεικονίσεις f, g είναι «επί», τότε η απεικόνιση $g \circ f$ είναι «επί». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «επί», τότε η απεικόνιση g είναι «επί».*

3. *Αν οι απεικονίσεις f, g είναι αντιστρέψιμες, τότε η απεικόνιση $g \circ f$ είναι αντιστρέψιμη και ισχύει ότι:*

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

Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι αντιστρέψιμη. τότε η f είναι «1-1» και η g είναι «επί».

Απόδειξη. 1. Έστω ότι οι απεικονίσεις f, g είναι «1-1», και έστω $x, y \in X$ έτσι ώστε: $(g \circ f)(x) = (g \circ f)(y)$. Τότε $g(f(x)) = g(f(y))$, και επομένως $f(x) = f(y)$ διότι η g είναι «1-1». Επειδή η f είναι επίσης «1-1», θα έχουμε $x = y$, και άρα η $g \circ f$ είναι «1-1». Αντίστροφα, αν τα στοιχεία $x, y \in X$ είναι τέτοια ώστε $f(x) = f(y)$, τότε θα έχουμε $g(f(x)) = g(f(y))$, δηλαδή $(g \circ f)(x) = (g \circ f)(y)$. Επομένως, αν η απεικόνιση $g \circ f$ είναι «1-1», τότε θα έχουμε $x = y$, και άρα η f είναι «1-1».

2. Έστω ότι οι απεικονίσεις f, g είναι «επί», και έστω ένα στοιχείο $z \in Z$. Επειδή η g είναι «επί», έπεται ότι υπάρχει στοιχείο $y \in Y$ έτσι ώστε $g(y) = z$, και επειδή η f είναι «επί», έπεται ότι υπάρχει στοιχείο $x \in Y$ έτσι ώστε $f(x) = y$. Τότε $(g \circ f)(x) = g(f(x)) = g(y) = z$ και άρα η $g \circ f$ είναι «επί». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «επί», και $z \in Z$, τότε υπάρχει $x \in X$ έτσι ώστε $(g \circ f)(x) = g(f(x)) = y$, και επομένως η g είναι «επί».

3. Έστω ότι οι απεικονίσεις f, g είναι αντιστρέψιμες. Τότε από την Πρόταση 0.2.8 έπεται ότι οι f, g είναι απεικονίσεις «1-1» και «επί». Από τα μέρη 1. και 2. έπεται τότε ότι η σύνθεση $g \circ f$ είναι «1-1» και «επί», και επομένως πάλι από την Πρόταση 0.2.8 η απεικόνιση $g \circ f$ είναι αντιστρέψιμη, και άρα υπάρχει η αντίστροφή της $(g \circ f)^{-1}$. Επιπλέον, χρησιμοποιώντας την προσεταιριστική ιδιότητα της σύνθεσης απεικονίσεων, θα έχουμε:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = ((g \circ f^{-1}) \circ f) \circ g^{-1} = (g \circ (f^{-1} \circ f)) \circ g^{-1} = (g \circ \mathsf{Id}_X) \circ g^{-1} = g \circ g^{-1} = \mathsf{Id}_Y$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = ((f^{-1} \circ g^{-1}) \circ g) \circ f = (f^{-1} \circ (g^{-1} \circ g)) \circ f = (f^{-1} \circ \mathsf{Id}_X) \circ f = f^{-1} \circ f = \mathsf{Id}_X$$

Λόγω της μοναδικότητας της αντίστροφης απεικόνισης, βλέπε την Πρόταση 0.2.8, θα έχουμε: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Τέλος αν η απεικόνιση $g \circ f$ είναι αντιστρέψιμη, τότε όπως παραπάνω η $g \circ f$ είναι «1-1» και «επί» και τότε από τα μέρη 1. και 2. έπεται ότι η f είναι «1-1» και η g είναι επί. ■

Παρατήρηση 0.2.13. Παρατηρούμε ότι η σύνθεση απεικονίσεων $f, g, h, \cdots : X \longrightarrow X$, όπου X είναι ένα μη κενό σύνολο, ορίζεται πάντα. Ιδιαίτερα, για κάθε απεικόνιση $f : X \longrightarrow X$, και για κάθε θετικό ακέραιο n, ορίζεται επαγωγικά η απεικόνιση

$$f^n := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ φορές}} : X \longrightarrow X, \quad x \longmapsto f^n(x)$$

ως εξής. Αν $n = 1$, τότε $f^1 = f$. Αν $n = 2$, τότε $f^2 = f \circ f$. Αν $n \geq 3$ και έχει οριστεί επαγωγικά η απεικόνιση f^{n-1}, τότε ορίζουμε $f^n = f^{n-1} \circ f$.

Από την άλλη πλευρά, ορίζουμε $f^0 = \mathrm{Id}_X$. Αν επιπλέον *η απεικόνιση f είναι αντιστρέψιμη*, οπότε ορίζεται η αντίστροφή της $f^{-1} : X \longrightarrow X$, τότε μπορούμε να ορίσουμε αρνητικές ακέραιες δυνάμεις f^{-n}, όπου $n \geq 1$, της f, ως εξής:

$$f^{-n} : X \longrightarrow X, \quad f^{-n} = (f^{-1})^n \quad \blacktriangle$$

Άσκηση 0.2.14. *Έστω $f_k : X_k \longrightarrow Y_k$, $1 \leq k \leq n$, μια οικογένεια απεικονίσεων μεταξύ μη-κενών συνόλων, και έστω η απεικόνιση-γινόμενο*

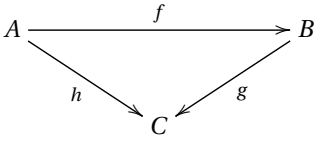
$$\prod_{k=1}^{n} f_k : \prod_{k=1}^{n} X_k \longrightarrow \prod_{k=1}^{n} Y_k, \quad (\prod_{k=1}^{n} f_k)(x_1, x_2, \cdots, x_n) = (f_1(x_1), f_2(x_2), \cdots, f_n(x_n))$$

όπως στο παράδειγμα 0.2.6. Να δειχθεί ότι η απεικόνιση $\prod_{k=1}^{n} f_k$ είναι «1-1», αντίστοιχα «επί», αν και μόνο αν οι απεικονίσεις f_k, $1 \leq k \leq n$ είναι «1-1», αντίστοιχα «επί». Αν οι απεικονίσεις f_k, $1 \leq k \leq n$ είναι «1-1» και «επί», να βρεθεί η αντίστροφη $(\prod_{k=1}^{n} f_k)^{-1}$ της απεικόνισης-γινόμενο $\prod_{k=1}^{n} f_k$.

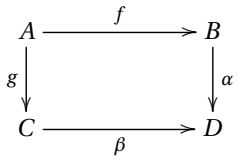
Συμβολισμός 0.2.15 (Ειδικού Τύπου Απεικονίσεις και Μεταθετικά Διαγράμματα)**.** Αν μια απεικόνιση $f : A \longrightarrow B$ είναι «1-1», «επί», ή «1-1» και «επί», τότε συχνά θα συμβολίζουμε αντίστοιχα

$$A \overset{f}{\rightarrowtail} B, \qquad A \overset{f}{\twoheadrightarrow} B, \qquad f : A \overset{\cong}{\longrightarrow} B$$

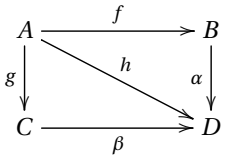
Συχνά η ισότητα μεταξύ (συνθέσεων) απεικονίσεων παριστάται μέσω μεταθετικών διαγραμμάτων. Ένα **μεταθετικό διάγραμμα** *συνόλων και απεικονίσεων* είναι ένα διάγραμμα το οποίο αποτελείται από κορυφές, οι οποίες αντιστοιχούν σε σύνολα και προσανατολισμένες ακμές μεταξύ των κορυφών, οι οποίες αντιστοιχούν σε απεικονίσεις μεταξύ συνόλων, έτσι ώστε όλες οι τεθλασμένες γραμμές οι οποίες σχηματίζονται από τις ακμές του διαγράμματος και οι οποίες έχουν την ίδια αρχή και το ίδιο τέλος δίνουν, μέσω της σύνθεσης, την ίδια απεικόνιση. Για παράδειγμα, αν $f : A \longrightarrow B$ και $g : B \longrightarrow C$ και $h : A \longrightarrow C$ είναι απεικονίσεις μεταξύ συνόλων, τότε ισχύει ότι: $h = g \circ f$ αν και μόνο αν το ακόλουθο διάγραμμα είναι μεταθετικό.



Παρόμοια, αν $f : A \longrightarrow B$ και $\alpha : B \longrightarrow D$ και $g : A \longrightarrow C$, και $\beta : C \longrightarrow D$ είναι απεικονίσεις μεταξύ συνόλων, τότε ισχύει ότι: $\alpha \circ f = \beta \circ g$ αν και μόνο αν το ακόλουθο διάγραμμα είναι μεταθετικό:



Για παράδειγμα, το διάγραμμα απεικονίσεων μεταξύ συνόλων



είναι μεταθετικό αν: $\alpha \circ f = h$ και $\beta \circ g = h$ (και τότε προφανως θα έχουμε και $\alpha \circ f = \beta \circ g$). ▲

0.2.2 Πεπερασμένα και Άπειρα Σύνολα

Υπενθυμίζουμε κάποια βασικά στοιχεία που αφορούν πεπερασμένα και άπειρα σύνολα.

Για κάθε φυσικό αριθμό n, θεωρούμε το σύνολο

$$\mathbb{N}_n = \{1, 2, \cdots, n\}$$

Ένα σύνολο X **έχει πλήθος στοιχείων ίσο με** n, αν υπάρχει μια «1-1» και «επί» απεικόνιση $f: X \longrightarrow \mathbb{N}_n$. Τότε θα γράφουμε

$$|X| = \#X = \mathsf{card}(X) = n$$

Ένα μη κενό σύνολο X καλείται **πεπερασμένο**, και τότε θα γράφουμε $|X| < \infty$, αν, με την παραπάνω έννοια, έχει πλήθος στοιχείων ίσο με n, για κάποιον φυσικό αριθμό n. Το μη-κενό σύνολο X καλείται **άπειρο** αν δεν είναι πεπερασμένο, και τότε θα γράφουμε $|X| = \infty$. Τέλος, ορίζουμε το πλήθος των στοιχείων του κενού συνόλου $\emptyset$ να είναι ίσο με 0. Η επόμενη Παρατήρηση δείχνει ότι οι παραπάνω ορισμοί ειναι «καλοί», δηλαδή δεν περιέχουν αντιφάσεις.

Παρατήρηση 0.2.16. Αν $f: X \longrightarrow \mathbb{N}_n$ και $g: X \longrightarrow \mathbb{N}_m$ είναι «1-1» και «επί» απεικονίσεις, τότε $n = m$.

Πράγματι τότε οι απεικονίσεις f, g είναι αντιστρέψιμες και άρα ορίζεται η απεικόνιση $h = g \circ f^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ η οποία, σύμφωνα με την Πρόταση 0.2.12 και το Πόρισμα 0.2.10, είναι «1-1» και «επί» και άρα είναι αντιστρέψιμη. Επειδή η h είναι «1-1», έπεται ότι τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι διαφορετικά στοιχεία του $\mathbb{N}_m$ και επομένως $n \leq m$. Παρόμοια, επειδή η h^{-1} είναι «1-1», έπεται ότι τα στοιχεία $h^{-1}(1), h^{-1}(2), \cdots, h^{-1}(m)$ είναι διαφορετικά στοιχεία του $\mathbb{N}_n$ και επομένως $m \leq n$. Άρα $n = m$. ▲

Έστω ότι X και Y είναι δύο μη-κενά σύνολα.

1. Το σύνολο X **έχει το πολύ τόσα στοιχεία όσα έχει το σύνολο** Y, και τότε γράφουμε: $|X| \leq |Y|$, αν υπάρχει μια «1-1» απεικόνιση $f: X \longrightarrow Y$.

2. Το σύνολο X **έχει τουλάχιστον όσα στοιχεία έχει το σύνολο** Y, και τότε γράφουμε: $|X| \geq |Y|$, αν υπάρχει μια απεικόνιση «επί» $f: X \longrightarrow Y$.

3. Τα σύνολα X και Y **έχουν το ίδιο πλήθος στοιχείων**, και τότε γράφουμε: $|X| = |Y|$, αν υπάρχει μια «1-1» και «επί» απεικόνιση $f: X \longrightarrow Y$. Διαφορετικά θα γράφουμε $|X| \neq |Y|$.

4. Θα γράφουμε $|X| < |Y|$, αν $|X| \leq |Y|$ και $|X| \neq |Y|$, και θα λέμε ότι το X έχει λιγότερα στοιχεία από όσα έχει το Y. Ισοδύναμα αυτό ισχύει αν υπάρχει «1-1» απεικόνιση $X \longrightarrow Y$ αλλά δεν υπάρχει «επί» απεικόνιση $X \longrightarrow Y$. Παρόμοια θα γράφουμε $|X| > |Y|$, αν $|X| \geq |Y|$ και $|X| \neq |Y|$, και θα λέμε ότι το X έχει περισσότερα στοιχεία από όσα έχει το Y. Ισοδύναμα αυτό ισχύει αν υπάρχει «επί» απεικόνιση $X \longrightarrow Y$, αλλά δεν υπάρχει «1-1» απεικόνιση $X \longrightarrow Y$.

5. Το σύνολο X καλείται **αριθμήσιμο** αν έχει το ίδιο πλήθος στοιχείων με το σύνολο $\mathbb{N}$ των θετικών ακεραίων. Διαφορετικά το σύνολο X καλείται **μη αριθμήσιμο**.

Επισημαίνουμε ότι γράφοντας $|X| \leq |Y|$ δεν συμβολίζουμε μια σχέση ανισότητας μεταξύ αριθμών αλλά το γεγονός ότι υπάρχει «1-1» απεικόνιση από το σύνολο X στο σύνολο Y. Παρόμοια για τους συμβολισμούς $|X| \geq |Y|$ και $|X| = |Y|$.

Πρόταση 0.2.17. *Έστω ότι X και Y είναι δύο πεπερασμένα σύνολα, και έστω ότι $|X| = n$ και $|Y| = m$.*

1. *Υπάρχει «1-1» απεικόνιση $f: X \longrightarrow Y \iff n \leq m$.*
2. *Υπάρχει «επί» απεικόνιση $f: X \longrightarrow Y \iff n \geq m$.*
3. *Αν $|X| = |Y|$, τότε μια απεικόνιση $f: X \longrightarrow Y$ είναι αντιστρέψιμη αν και μόνο αν είτε η f είναι «1-1» είτε η f είναι «επί».*
4. *Αν $|X| \neq |Y|$, τότε για κάθε «επί» απεικόνιση $f: X \longrightarrow Y$ υπάρχει τουλάχιστον ένα ζεύγος (x_1, x_2) στοιχείων του X έτσι ώστε $x_1 \neq x_2$ και $f(x_1) = f(x_2)$*[2].

Απόδειξη. Επειδή $|X| = n$, έπεται ότι υπάρχει «1-1» και «επί» απεικόνιση $\alpha: X \longrightarrow \mathbb{N}_n$, και επειδή $|Y| = m$, έπεται ότι υπάρχει «1-1» και «επί» απεικόνιση $\beta: X \longrightarrow \mathbb{N}_m$. Ιδιαίτερα τότε υπάρχουν οι απεικονίσεις α^{-1} και β^{-1} οι οποίες είναι επίσης «1-1» και «επί».

1. Αν υπάρχει «1-1» απεικόνιση $f: X \longrightarrow Y$, τότε η σύνθεση $h := \beta \circ f \circ \alpha^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ είναι προφανώς μια «1-1» απεικόνιση, και τότε τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι ανά δύο διαφορετικά στοιχεία του συνόλου $\mathbb{N}_m$. Επομένως $n \leq m$. Αντίστροφα, αν $n \leq m$, τότε $\mathbb{N}_m = \mathbb{N}_n \cup \{n+1, \cdots, m\}$ και προφανώς η απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_m$, $h(k) = k$, $\forall k = 1, \cdots, n$, είναι «1-1». Η σύνθεση $\beta^{-1} \circ h \circ \alpha: X \longrightarrow Y$ είναι, σύμφωνα με την Πρόταση 0.2.12, μια απεικόνιση «1-1».

2. Έστω ότι υπάρχει μια «επί» απεικόνιση $f: X \longrightarrow Y$. Τότε σύμφωνα με την Πρόταση 0.2.12, η απεικόνιση $h := \beta \circ f \circ \alpha^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ είναι «επί». Επομένως, για κάθε $k \in \mathbb{N}_m$, υπάρχει τουλάχιστον ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Τότε όμως $m \leq n$. Αντίστροφα, αν $m \leq n$, τότε $\mathbb{N}_n = \mathbb{N}_m \cup \{m+1, \cdots, n\}$ και προφανώς η απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_m$, $h(k) = k$, αν $1 \leq k \leq m$ και $h(k) = 1$, αν $m+1 \leq k \leq n$, είναι «επί». Τότε, σύμφωνα με την Πρόταση 0.2.12, η απεικόνιση $f := \beta^{-1} \circ h \circ \alpha: X \longrightarrow Y$ είναι «επί».

3. Υποθέτουμε ότι $n = m$, και έστω $f: X \longrightarrow Y$ μια απεικόνιση. Αν η f είναι «1-1», τότε όπως στο μέρος 1. υπάρχει μια «1-1» απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_n$ και επομένως τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι ανά δύο διαφορετικά. Τότε, $\mathbb{N}_n = \{h(1), \cdots, h(n)\}$ και άρα η h είναι «επί». Αν η f είναι «επί», τότε όπως στο μέρος 2. υπάρχει μια «επί» απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_n$ και άρα για κάθε $k \in \mathbb{N}_n$ υπάρχει τουλάχιστον ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Αν για δεδομένο k έχουμε $h(l_1) = k = h(l_2)$, τότε αναγκαστικά $l_1 = l_2$ διότι διαφορετικά το σύνολο $\mathbb{N}_n$ θα περιείχε τουλάχιστον $n+1$ στοιχεία. Άρα, για κάθε $k \in \mathbb{N}_n$, υπάρχει ακριβώς ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Τότε προφανώς η h είναι «1-1».

4. Προκύπτει άμεσα από το μέρος 3. ∎

Παράδειγμα 0.2.18. Έστω X ένα μη-κενό σύνολο. Θεωρούμε το σύνολο $\mathbf{2} = \{0, 1\}$, και έστω

$$\mathbf{2}^X := \{f: X \longrightarrow \mathbf{2} \mid f : \text{απεικόνιση}\}$$

Επίσης θεωρούμε το *δυναμοσύνολο* $\mathscr{P}(X)$ του X, δηλαδή το σύνολο όλων των υποσυνόλων του X. Θα δείξουμε ότι:

$$|X| \ < \ |\mathbf{2}^X| \ = \ |\mathscr{P}(X)|$$

(α) Ορίζουμε απεικόνιση

$$\Omega: X \longrightarrow \mathbf{2}^X, \quad \Omega(a) = \chi_{\{a\}}$$

όπου $\chi_{\{a\}}$ είναι η χαρακτηριστική συνάρτηση του μονοσυνόλου $\{a\}$, βλέπε Παράδειγμα 0.2.3. Αν $\Omega(a) = \Omega(b)$, τότε $\chi_{\{a\}} = \chi_{\{b\}}$ και επομένως $\chi_{\{a\}}(a) = \chi_{\{b\}}(a)$, από όπου έπεται ότι $1 = \begin{cases} 1, \text{ αν } b = a \\ 0, \text{ αν } b \neq a \end{cases}$. Άρα θα έχουμε $a = b$, και επομένως η απεικόνιση Ω είναι «1-1». Η απεικόνιση Ω δεν είναι «επί» διότι, επειδή $X \neq \emptyset$, έπεται ότι το X

[2] Αυτός ο ισχυρισμός είναι η μαθηματική διατύπωση της θεμελιώδους αρχής απαρίθμησης γνωστής ως «*Αρχή του Περιστερώνα*»: Αν $n = |X|$ περιστέρια τοποθετηθούν σε $m = |Y| < n$ φωλιές, τότε σε τουλάχιστον μία φωλιά υπάρχουν τουλάχιστον δύο περιστέρια. Η αυστηρή διατύπωση αυτής της αρχής είναι η εξής: *Έστω X και Y δύο πεπερασμένα σύνολα, και $f: X \longrightarrow Y$ μια απεικόνιση. Τότε: (α) αν $|X| > |Y|$, τότε η f δεν είναι «1-1», και (β) αν $|X| < |Y|$, τότε η f δεν είναι «επί».*

περιέχει τουλάχιστον ένα στοιχείο, έστω το a. Τότε ορίζονται οι απεικονίσεις $f\colon X \longrightarrow \mathbf{2}$, $f(a)=0$, και $f(x)=1$, $\forall x \neq a$, και $g\colon X \longrightarrow \mathbf{2}$, $g(a)=0$, και $g(x)=1$, $\forall x \neq a$. Αν η απεικόνιση Ω είναι «επί», τότε υπάρχει στοιχείο $b \in X$ έτσι ώστε $\Omega(b) = \chi_{\{b\}} = f$, και επομένως $\chi_{\{b\}}(a) = f(a)$, δηλαδή: $\begin{cases} 1, \text{ αν } b=a \\ 0, \text{ αν } b \neq a \end{cases} = \begin{cases} 0, \text{ αν } b=a \\ 1, \text{ αν } b \neq a \end{cases}$, το οποίο είναι άτοπο. Άρα η Ω δεν είναι «επί» και επομένως: $|X| < |\mathbf{2}^X|$.

(β) Γενικότερα θα δείξουμε ότι δεν υπάρχει «1-1» και «επί» απεικόνιση $f\colon X \longrightarrow \mathscr{P}(X)$. Πράγματι, αν υπάρχει μια τέτοια απεικόνιση, τότε για κάθε στοιχείο $x \in X$, το $f(x)$ είναι ένα υποσύνολο του X και επομένως είτε $x \in f(x)$ ή $x \notin f(x)$. Θεωρούμε το υποσύνολο $S = \{x \in X \mid x \notin f(x)\}$. Επειδή η f είναι «επί», έπεται ότι υπάρχει $y \in X$ έτσι ώστε $f(y) = S$. Τότε είτε $y \in S$ ή $y \notin S$. Όμως $y \in S = f(y)$ σημαίνει ότι $y \notin f(y)$ και $y \notin S = f(y)$ σημαίνει ότι $y \in f(y)$. Και οι δύο περιπτώσεις μάς οδηγούν σε άτοπο και επομένως δεν υπάρχει «1-1» και «επί» απεικόνιση $: X \longrightarrow \mathscr{P}(X)$.

(γ) Θεωρούμε απεικονίσεις

$$\Phi\colon \mathscr{P}(X) \longrightarrow \mathbf{2}^X, \quad \Phi(A) = \chi_A \qquad \text{και} \qquad \Psi\colon \mathbf{2}^X \longrightarrow \mathscr{P}(X), \quad \Psi(f) = f^{-1}(\{1\})$$

Θα δείξουμε ότι η Φ είναι αντιστρέψιμη με αντίστροφη την Ψ. Για κάθε υποσύνολο $A \subseteq X$, έχουμε:

$$\Psi\Phi(A) = \Psi(\chi_A) = \chi_A^{-1}(\{1\}) = \left\{x \in X \mid x \in \chi_A^{-1}(x)\right\} = \left\{x \in X \mid \chi_A(x) = 1\right\} = \left\{x \in X \mid x \in A\right\} = A$$

Δηλαδή $\Psi\Phi = \mathsf{Id}_{\mathscr{P}(X)}$. Για κάθε απεικόνιση $f\colon X \longrightarrow \mathbf{2}$, έχουμε:

$$\Phi\Psi(f) = \Phi(f^{-1}(\{1\})) = \chi_{f^{-1}(\{1\})} \quad \text{και} \quad \forall x \in X\colon \ \chi_{f^{-1}(\{1\})}(x) = \begin{cases} 1, \text{ αν } x \in f^{-1}(\{1\}) \\ 0, \text{ αν } x \notin f^{-1}(\{1\}) \end{cases} = \begin{cases} 1, \text{ αν } f(x) = 1 \\ 0, \text{ αν } f(x) = 0 \end{cases} = f(x)$$

Επομένως $\chi_{f^{-1}(\{1\})}(x) = f(x)$, $\forall x \in X$, και άρα $\chi_{f^{-1}(\{1\})} = f$, δηλαδή $\Phi\Psi(f) = f$. Επειδή η απεικόνιση f ήταν τυχαία, έπεται ότι $\Phi\Psi = \mathsf{Id}_{\mathbf{2}^X}$. Έτσι η απεικόνιση Φ είναι αντιστρέψιμη με αντίστροφη την απεικόνιση Ψ, και επομένως $|\mathbf{2}^X| = |\mathscr{P}(X)|$. $\surd$

Ο συμβολισμός $\mathbf{2}^X$ για ένα σύνολο X προέρχεται από το Παράδειγμα 0.2.18 σε συνδυασμό με την ακόλουθη παρατήρηση.

Παρατήρηση 0.2.19. Για κάθε σύνολο X ισχύει ότι:

$$|X| < \infty \quad \Longrightarrow \quad |\mathscr{P}(X)| = 2^{|X|}$$

Αν $X = \emptyset$, τότε $|X| = 0$ και το $\mathscr{P}(X)$ περιέχει μόνο το στοιχείο $\emptyset$. Άρα $|\mathscr{P}(\emptyset)| = 1 = 2^0 = 2^{|\emptyset|}$. Αν $|X| = 1$, τότε $X = \{a\}$ και $\mathscr{P}(X) = \{\emptyset, \{a\}\}$ και επομένως $|\mathscr{P}(X)| = 2 = 2^1 = 2^{|X|}$. Υποθέτουμε ότι $|\mathscr{P}(X)| = 2^{|X|}$, για κάθε σύνολο με $|X| = n$, όπου $n \geq 2$. Έστω $|X| = n+1$, και έστω $a \in X$. Θεωρούμε το σύνολο $Y = X \setminus \{a\}$ για το οποίο έχουμε $|Y| = n$. Αν S είναι ένα υποσύνολο του X, τότε είτε $a \in S$ ή $a \notin S$. Στην τελευταία περίπτωση, θα έχουμε προφανώς ότι $S \subseteq Y$. Επομένως τα υποσύνολα του X συμπίπτουν με τα υποσύνολα S του Y, τα οποία από την Επαγωγική Υπόθεση σε πλήθος είναι $|\mathscr{P}(Y)| = 2^{|Y|} = 2^n$, μαζί με τα υποσύνολα $S \cup \{a\}$ του X, για κάθε υποσύνολο S του Y, και τα οποία σε πλήθος είναι όσα και τα υποσύνολα του Y, δηλαδή είναι 2^n. Έτσι το πλήθος των υποσυνόλων του $\mathscr{P}(X)$ είναι $2^n + 2^n = 2 \cdot 2^n = 2^{n+1} = 2^{|X|}$. Από την Αρχή Μαθηματικής Επαγωγής, έπεται ότι $|\mathscr{P}(X)| = 2^{|X|}$, για κάθε πεπερασμένο σύνολο X. ▲

Παράδειγμα 0.2.20.

1. $|\mathbb{N}| = |\mathbb{Z}|$, διότι, όπως μπορεί να δειχθεί εύκολα, η απεικόνιση

$$f\colon \mathbb{N} \longrightarrow \mathbb{Z}, \quad f(n) = (-1)^n \left[\frac{n}{2}\right]$$

είναι «1-1» και «επί», όπου $\left[\frac{n}{2}\right]$ συμβολίζει τον μεγαλύτερο ακέραιο ο οποίος δεν υπερβαίνει τον $\frac{n}{2}$.

2. $|\mathbb{Z}| = |2\mathbb{Z}|$, όπου $2\mathbb{Z} = \{2n \in \mathbb{Z} \mid n \in \mathbb{Z}\}$ είναι το σύνολο των αρτίων ακεραίων, διότι όπως μπορεί να δειχθεί εύκολα η απεικόνιση

$$f\colon \mathbb{Z} \longrightarrow 2\mathbb{Z}, \quad f(n) = 2n$$

είναι «1-1» και «επί».

3. $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$, διότι όπως μπορεί να δειχθεί εύκολα η απεικόνιση

$$f:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N},\quad f(n,m)=\frac{(m+n-2)(m+n-1)}{2}+n$$

είναι «1-1» και «επί».

4. Αποδεικνύεται παρόμοια ότι $|\mathbb{N}| = |\mathbb{Q}|$, και άρα το σύνολο $\mathbb{Q}$ είναι αριθμήσιμο. Όμως τα σύνολα $\mathbb{R}$ και $\mathbb{C}$ είναι άπειρα μη αριθμήσιμα και έχουν το ίδιο πλήθος στοιχείων. $\surd$

Υποθέτουμε ότι X και Y είναι δύο σύνολα, όχι απαραίτητα πεπερασμένα. Αν $|X| \le |Y|$, δηλαδή αν υπάρχει «1-1» απεικόνιση $: X \longrightarrow Y$, και αν $|Y| \le |X|$, δηλαδή αν υπάρχει «1-1» απεικόνιση $: Y \longrightarrow X$, τότε το ακόλουθο αποτέλεσμα το οποίο οφείλεται στους Schröder-Bernstein πιστοποιεί ότι τα σύνολα X και Y έχουν το ίδιο πλήθος στοιχείων, δηλαδή υπάρχει «1-1» και «επί» απεικόνιση $X \longrightarrow Y$.

Πρόταση 0.2.21 (Schröder-Bernstein)**.** [3] [4] *Αν X και Y είναι δύο σύνολα, τότε:*

$$|X| \le |Y| \quad \textit{και} \quad |Y| \le |X| \qquad \Longleftrightarrow \qquad |X| = |Y|$$

0.3 Ακέραιοι Αριθμοί

Στην παρούσα ενότητα, θα υπενθυμίσουμε βασικές έννοιες από την αριθμητική και τη διαιρετότητα των ακεραίων αριθμών. Επίσης θα αναλύσουμε εν συντομία την Αρχή της Μαθηματικής Επαγωγής, καθώς και διάφορες αποδεικτικές μεθόδους, οι οποίες θα χρησιμοποιηθούν στη συνέχεια του κειμένου.

0.3.1 Το σύνολο των Φυσικών Αριθμών και η Αρχή Μαθηματικής Επαγωγής

Θεωρούμε γνωστές τις στοιχειώδεις ιδιότητες του συνόλου[5] των θετικών ακεραίων ή φυσικών αριθμών

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

καθώς και του συνόλου $\mathbb{N}_0 = \mathbb{N}\cup\{0\} = \{0, 1, 2, \cdots, n, \cdots\}$ των μη αρνητικών ακεραίων. Το σύνολο $\mathbb{N}_0$ προκύπτει ως επέκταση του συνόλου $\mathbb{N}$ έτσι ώστε, για κάθε $n \in \mathbb{N}$, η εξίσωση $n + x = n$ να έχει λύση.

Στη μελέτη της δομής και των βασικών ιδιοτήτων του συνόλου $\mathbb{N}$ των φυσικών αριθμών, αλλά και σε σημαντικές αποδεικτικές μεθόδους, θεμελιώδη ρόλο διαδραματίζουν διάφορες αρχές αξιωματικού χαρακτήρα. Οι σημαντικότερες από αυτές τις αρχές είναι οι εξής. Πριν περάσουμε στην διατύπωσή τους, υπενθυμίζουμε ότι, αν S είναι ένα μη κενό υποσύνολο του συνόλου $\mathbb{N}$ των φυσικών αριθμών, τότε ένα *ελάχιστο*, αντίστοιχα *μέγιστο*, στοιχείο του S είναι ένα στοιχείο $x \in S$, έτσι ώστε, για κάθε $s \in S$: $x \le s$, αντίστοιχα $s \le x$. Ένα ελάχιστο, αντίστοιχα μέγιστο, στοιχείο του S συμβολίζεται με $\min S$, αντίστοιχα $\max S$.

---

[3] Felix Bernstein (24 Φεβρουαρίου 1878 - 3 Δεκεμβρίου 1956) [https://en.wikipedia.org/wiki/Felix_Bernstein_(mathematician)]: Γερμανός μαθηματικός, γνωστός για την απόδειξη του Θεωρήματος Schröder-Bernstein.

[4] Friedrich Wilhelm Karl Ernst Schröder (25 Νοεμβρίου 1841 - 16 Ιουνίου 1902) [https://en.wikipedia.org/wiki/Felix_Bernstein_(mathematician)]: Γερμανός μαθηματικός με συμβολή στην Μαθηματική Λογική.

[5] Το σύνολο των φυσικών αριθμών μπορεί να οριστεί αξιωματικά, ξεκινώντας από ένα μη κενό σύνολο $\mathbb{N}$, ένα διακεκριμένο στοιχείο $1 \in \mathbb{N}$, και μια απεικόνιση

$$\mathsf{s}:\mathbb{N}\longrightarrow\mathbb{N},\quad n\longmapsto \mathsf{s}(n)$$

η οποία ικανοποιεί τα **αξιώματα του Peano**:

1. $\forall n \in \mathbb{N}$: $1 \neq \mathsf{s}(n)$.
2. Η απεικόνιση s είναι «1-1».
3. Αν $A \subseteq \mathbb{N}$ είναι ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:

   (α') $1 \in A$.

   (β') $n \in A \Longrightarrow \mathsf{s}(n) \in A$.

   τότε $A = \mathbb{N}$.

(ΑΚΔ) Αρχη Καλης Διαταξης: Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.

(ΑΜΕ)$_1$ Αρχη Μαθηματικης Επαγωγης$_1$: Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:

(α) $1 \in S$.

(β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.

Τότε: $S = \mathbb{N}$.

(ΑΜΕ)$_2$ Αρχη Μαθηματικης Επαγωγης$_2$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(1)$ είναι αληθής.

(β) $\forall k \in \mathbb{N}$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

(ΑΜ) Αρχη Μεγιστου: Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.

Θα δείξουμε ότι οι παραπάνω αρχές είναι μεταξύ τους ισοδύναμες.

Θεώρημα 0.3.1. *Οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *(ΑΚΔ): Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.*
2. *(ΑΜΕ)$_1$: Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:*

   (α) $1 \in S$.

   (β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.

   Τότε: $S = \mathbb{N}$.
3. *(ΑΜΕ)$_2$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:*

   (α) *Η πρόταση $P(1)$ είναι αληθής.*

   (β) $\forall k \in \mathbb{N}$: *η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.*

   Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.
4. *(ΑΜ): Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.*

Απόδειξη. • (ΑΚΔ) $\implies$ (ΑΜΕ)$_1$ Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω S ένα υποσύνολο του $\mathbb{N}$ έτσι ώστε $1 \in S$, και $k \in S \implies k+1 \in S$.

Υποθέτουμε ότι $S \neq \mathbb{N}$. Τότε το σύνολο $\mathbb{N} \setminus S$ είναι μη κενό. Επόμενως από την αρχή καλής διάταξης έπεται ότι το $\mathbb{N} \setminus S$ έχει ελάχιστο στοιχείο:

$$\ell = \min(\mathbb{N} \setminus S), \quad \text{δηλαδή} \quad \ell \in \mathbb{N} \setminus S \quad \text{και} \quad \ell \leq x, \ \ \forall x \in \mathbb{N} \setminus S$$

Αν $\ell = 1$, τότε $1 \in \mathbb{N} \setminus S$ το οποίο είναι άτοπο, διότι από την υπόθεση έχουμε $1 \in S$. Άρα $\ell > 1$ και επομένως $1 \leq \ell - 1 < \ell$.

Τότε το στοιχείο $\ell - 1$ θα ανήκει στο S, διότι διαφορετικά $\ell - 1 \in \mathbb{N} \setminus S$, κάτι το οποίο είναι άτοπο διότι $\ell - 1 < \ell$ και το ℓ είναι το ελάχιστο στοιχείο του $\mathbb{N} \setminus S$. Απο την ιδιότητα (β) του συνόλου S θα έχουμε τότε: $1 \in S$, και $\ell - 1 \in S \implies \ell \in S$. Αυτό όμως είναι άτοπο διότι εκ κατασκευής $\ell \in \mathbb{N} \setminus S$, δηλαδή $\ell \notin S$.

Στο άτοπο καταλήξαμε υποθέτοντας ότι $S \neq \mathbb{N}$. Επομένως θα έχουμε $S = \mathbb{N}$, και άρα ισχύει η πρώτη εκδοχή της Αρχής Μαθηματικής Επαγωγής.

• $(\text{ΑΜΕ})_1 \implies (\text{ΑΜΕ})_2$ Υποθέτουμε ότι ισχύει η πρώτη εκδοχή της Αρχής Μαθηματικής Επαγωγής και έστω η πρόταση $P(n)$, $n \in \mathbb{N}$, για την οποία ικανοποιούνται οι συνθήκες του μέρους **3**. Θεωρούμε το ακόλουθο σύνολο

$$S = \{n \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής}\}$$

Προφανώς τότε για το υποσύνολο S ικανοποιούνται οι συνθήκες (α) και (β) του μέρους **2**. Επομένως θα έχουμε ότι $S = \mathbb{N}$, το οποίο σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$. Άρα ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής.

• $(\text{ΑΜΕ})_2 \implies (\text{ΑΚΔ})$ Υποθέτουμε ότι ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής και έστω $S \subseteq \mathbb{N}$ ένα μη κενό υποσύνολο του $\mathbb{N}$.

Υποθέτουμε ότι το S δεν έχει ελάχιστο στοιχείο. Για κάθε $n \in \mathbb{N}$, θεωρούμε την πρόταση

$$P(n): \text{ για κάθε } k \in \mathbb{N} \text{ έτσι ώστε } 1 \le k \le n, \text{ ισχύει ότι: } k \notin S$$

Η πρόταση $P(1)$, δηλαδή ο ισχυρισμός ότι $1 \notin S$, είναι αληθής. Πράγματι, αν $1 \in S$, τότε προφανώς το 1 είναι ελάχιστο στοιχείο του S, κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο.

Υποθέτουμε ότι η πρόταση $P(n)$ είναι αληθής, δηλαδή κανένας από τους αριθμούς $1, 2, \cdots, n$ δεν ανήκει στο S. Αν το $n+1$ ανήκει στο S, τότε επειδή $k \notin S$, όπου $1 \le k \le n$, έπεται άμεσα ότι το $n+1$ είναι ελάχιστο στοιχείο του S, κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο. Άρα θα έχουμε ότι $n+1 \notin S$. Αυτό όμως σημαίνει ότι η πρόταση $P(n+1)$ είναι αληθής.

Από την δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής έπεται τότε ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$, και επομένως $\forall n \in \mathbb{N}$, $1 \le k \le n \implies k \notin S$. Με άλλα λόγια, $\forall n \in \mathbb{N}$, $n \notin S$. Αυτό όμως, επειδή $S \subseteq \mathbb{N}$, σημαίνει ότι $S = \emptyset$, κάτι το οποίο είναι άτοπο από την αρχική μας υπόθεση.

Στο άτοπο καταλήξαμε υποθέτοντας ότι το μη κενό υποσύνολο S του $\mathbb{N}$ δεν έχει ελάχιστο στοιχείο. Άρα το S έχει ελάχιστο στοιχείο και επομένως ισχύει η Αρχή Καλής Διάταξης.

– Έτσι έχουμε δείξει ότι οι τρεις πρώτες αρχές (ΑΚΔ), $(\text{ΑΜΕ})_1$, $(\text{ΑΜΕ})_2$ είναι ισοδύναμες. Ολοκληρώνουμε την απόδειξη δείχνοντας ότι: $(\text{ΑΚΔ}) \implies (\text{ΑΜ}) \implies (\text{ΑΜΕ})_2$.

• $(\text{ΑΚΔ}) \implies (\text{ΑΜ})$ Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω $T \subseteq \mathbb{N}$ ένα μη-κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Έστω $b \in \mathbb{N}$ ένα άνω φράγμα του T, δηλαδή:

$$b \in \mathbb{N} \text{ και } t \le b, \ \forall t \in T$$

Ορίζουμε ένα νέο σύνολο, το σύνολο όλων των άνω φραγμάτων του T στο $\mathbb{N}$:

$$S = \{s \in \mathbb{N} \mid t < s, \ \forall t \in T\}$$

Το σύνολο S είναι μη κενό διότι $\forall t \in T$: $t \le b < b+1$, και άρα $b+1 \in S$.

Από την Αρχή Καλής Διάταξης, έπεται ότι το σύνολο S έχει ελάχιστο στοιχείο, έστω ότι αυτό είναι το s_0:

$$s_0 = \min S, \quad \text{δηλαδή } s_0 \in S \text{ και } s_0 \le s, \ \forall s \in S$$

Από τον ορισμό του συνόλου S, έπεται ότι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \le t_0$. Πράγματι, αν $s_0 - 1 > t$, $\forall t \in T$, τότε θα είχαμε ότι $s_0 - 1 \in S$, κάτι το οποίο είναι άτοπο διότι $s_0 - 1 < s_0$ και το s_0 είναι ένα ελάχιστο στοιχείο του S.

Άρα πράγματι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \le t_0$. Επειδή όμως έχουμε και $t_0 < s_0$, έπεται ότι θα έχουμε $s_0 - 1 = t_0 \in T$. Ισχυριζόμαστε ότι:

$$t_0 = \max T, \quad \text{δηλαδή το } t_0 \text{ είναι μέγιστο στοιχείο του } T$$

Πράγματι, το t_0 ανήκει εκ κατασκευής στο T και επιπλέον επειδή από τον ορισμό του συνόλου S έχουμε $t < s_0$, $\forall t \in T$, έπεται ότι $t \le s_0 - 1 = t_0$, $\forall t \in T$. Δηλαδή $t_0 = \max T$.

• $(\text{ΑΜ}) \implies (\text{ΑΜΕ})_2$ Υποθέτουμε ότι ισχύει η Αρχή Μεγίστου, και έστω $P(n)$ μια πρόταση η οποία εξαρτάται από το $n \in \mathbb{N}$, για την οποία ισχύει ότι η $P(1)$ είναι αληθής, και για κάθε φυσικό αριθμό n: $P(n)$ είναι αληθής $\implies$ $P(n+1)$ είναι αληθής.

Έστω ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Ορίζουμε τότε ένα σύνολο T ως εξής:

$$T = \{t \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής } \forall n \in \mathbb{N}: \ 1 \leq n \leq t\}$$

Επειδή η πρόταση $P(1)$ είναι αληθής, έπεται ότι $1 \in T$ και άρα $T \neq \emptyset$. Επιπρόσθετα, ο φυσικός αριθμός m είναι προφανώς ένα άνω φράγμα για το σύνολο T. Πράγματι αν $k \in \mathbb{N}$ και $m \leq k$, τότε $k \notin T$, διότι διαφορετικά, αν $k \in T$, τότε θα είχαμε ότι η $P(m)$ είναι αληθής, κάτι το οποίο δεν ισχύει.

Έτσι το T είναι ένα μη κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Επομένως από την Αρχή Μεγίστου, το σύνολο T έχει ένα μέγιστο στοιχείο, έστω ότι αυτό είναι το t_0:

$$t_0 = \max T, \ \text{δηλαδή} \ \ t_0 \in T \ \ \text{και} \ \ t \leq t_0, \ \forall t \in T$$

Από τον ορισμό του συνόλου T θα έχουμε ότι η πρόταση $P(t_0)$ είναι αληθής. Τότε από την υπόθεση θα έχουμε ότι και η πρόταση $P(t_0+1)$ είναι αληθής. Αυτό όμως σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$ έτσι ώστε: $1 \leq n \leq t_0+1$, και επομένως ο αριθμός t_0+1 ανήκει στο σύνολο T. Αυτό όμως είναι άτοπο διότι $t_0 < t_0+1$ και το t_0 είναι μέγιστο στοιχείο του T.

Στο άτοπο καταλήξαμε υποθέτοντας ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Άρα η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$, και επομένως ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής. ■

Σχόλιο 0.3.2. Από τώρα και στο εξής θα υποθέτουμε ότι ισχύει μια και επομένως και οποιαδήποτε από τις υπόλοιπες, από τις αρχές του παραπάνω Θεωρήματος. Κάθεμια από τις παραπάνω αρχές είναι ισοδύναμη με την αξιωματική θεμελίωση του συνόλου $\mathbb{N}$ των φυσικών αριθμών, η οποία πιστοποιεί την ύπαρξη ενός συνόλου $\mathbb{N}$ το οποίο ικανοποιεί την Αρχή Μαθηματικής Επαγωγής. √

Εναλλακτικές Μορφές Μαθηματικής Επαγωγής. Είδαμε μέχρι τώρα δύο (ισοδύναμες) μορφές της Αρχής Μαθηματικής Επαγωγής, τις $(\text{ΑΜΕ})_1$ και $(\text{ΑΜΕ})_2$. Θα δούμε κάποιες ακόμα χρήσιμες μορφές της Αρχής Μαθηματικής Επαγωγής.

$(\text{ΑΜΕ})_3$ Αρχη Μαθηματικης Επαγωγης$_3$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(1)$ είναι αληθής.

(β) $\forall k \in \mathbb{N}$, $1 \leq k < n$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(n)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

$(\text{ΑΜΕ})_4$ Αρχη Μαθηματικης Επαγωγης$_4$: Έστω ότι n_0 είναι ένας φυσικός αριθμός, και $P(n)$ είναι μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, όπου $n \geq n_0$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(n_0)$ είναι αληθής.

(β) Είτε $\forall k \in \mathbb{N}$, $n_0 \leq k < n$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(n)$ είναι αληθής, είτε $\forall k \in \mathbb{N}$, $k \geq n_0$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \geq n_0$.

Υπενθυμίζουμε ότι στο σύνολο $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ των μη αρνητικών ακεραίων ορίζονται οι συνήθεις πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» φυσικών αριθμών, οι οποίες ικανοποιούν τις ακόλουθες ιδιότητες, $\forall x, y, z \in \mathbb{N}$:

1. $(x+y)+z = x+(y+z)$ (Προσεταιριστικότητα της πρόσθεσης)
2. $x+y = y+x$ (Μεταθετικότητα της πρόσθεσης)
3. $x+0 = x = 0+x$ (Ύπαρξη ουδετέρου στοιχείου ως προς την πρόσθεση)

4. $x+y=x+z \implies y=z$ (Νόμος διαγραφής ως προς την πρόσθεση)
5. $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ (Προσεταιριστικότητα του πολλαπλασιασμού)
6. $x\cdot y = y\cdot x$ (Μεταθετικότητα του πολλαπλασιασμού)
7. $x\cdot 1 = x = 1\cdot x$ (Ύπαρξη ουδετέρου στοιχείου ως προς τον πολλαπλασιασμό)
8. $x\cdot y = x\cdot z$ και $x\neq 0 \implies y=z$ (Νόμος διαγραφής ως προς τον πολλαπλασιασμό)
9. $x\cdot(y+z) = x\cdot y + x\cdot z$ και $(x+y)\cdot z = x\cdot z + y\cdot z$ (Επιμεριστικότητα του πολλαπλασιασμού ως προς την πρόσθεση)

Το σύνολο $\mathbb{N}_0$ των μη αρνητικών ακεραίων είναι εφοδιασμένο με τη συνήθη σχέση διάταξης «≤»:

$$b\leq a \iff \text{υπάρχει } c\in\mathbb{N}_0 : \ a=b+c$$

δηλαδή ο μη αρνητικός ακέραιος a είναι *μεγαλύτερος ή ίσος* από τον μη αρνητικό ακέραιο b, ισοδύναμα ο b είναι *μικρότερος ή ίσος* από τον a, αν η εξίσωση $a=b+x$ έχει λύση στο σύνολο $\mathbb{N}_0$. Θα γράφουμε επίσης $a\geq b$, και αν $b\leq a$ και $a\neq b$ θα γράφουμε $b<a$ ή $a>b$.

Για την σχέση διάταξης ≤ στο σύνολο $\mathbb{N}_0$ ισχύουν οι ακόλουθες οικείες ιδιότητες, $\forall x,y,z\in\mathbb{N}_0$:

1. $y\leq x$ και $x\leq y \implies x=y$ (Αντισυμμετρία)
2. $x\leq y$ και $y\leq z \implies x\leq z$ (Μεταβατικότητα)
3. Είτε $x\leq y$ είτε $y\leq x$ (Διχοτομία)
4. $y\leq x \implies y+z\leq x+z$ (Συμβατότητα ως προς την πρόσθεση)
5. $y\leq x \implies y\cdot z\leq x\cdot z$ (Συμβατότητα ως προς τον πολλαπλασιασμό)
6. $y\leq x$ και $z\leq w \implies y+z\leq x+w$ και $y\cdot z\leq x\cdot w$.

0.3.2 Διαιρετότητα Ακεραίων

Συμβολίζουμε με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών:

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

το οποίο είναι ξένη ένωση $-\mathbb{N}\cup\{0\}\cup\mathbb{N}$ του συνόλου $-\mathbb{N}=\{\cdots,-3,-2,-1\}$ των αρνητικών ακεραίων αριθμών, του μηδενός 0, και του συνόλου $\mathbb{N}$ των θετικών ακεραίων αριθμών. Το σύνολο $\mathbb{Z}$ προκύπτει ως επέκταση του συνόλου $\mathbb{N}_0$ έτσι ώστε, $\forall n\in\mathbb{N}_0$, η εξίσωση $n+x=0$ να έχει λύση.

Ένας ακέραιος b **διαιρεί** τον ακέραιο a ή ο ακέραιος a είναι **πολλαπλάσιο** του ακεραίου b, αν υπάρχει ακέραιος c έτσι ώστε $a=bc$. Αν $b\mid a$, τότε ο ακέραιος b καλείται **διαιρέτης** του a και θα γράφουμε $b\mid a$. Ο ακέραιος b καλείται γνήσιος διαιρέτης του a αν $b\neq\pm a$ και $b\neq\pm 1$. Αν ο ακέραιος b δεν διαιρεί τον ακέραιο a θα γράφουμε $b\nmid a$. Οι βασικές ιδιότητες διαιρετότητας ακεραίων περιγράφονται στην ακόλουθη Πρόταση.

Πρόταση 0.3.3. *Έστω $a,b,c\in\mathbb{Z}$.*

1. *(i) $a\mid a$, (ii) $1\mid a$, (iii) $a\mid 0$, και (iv) $0\mid b \iff b=0$.*
2. *$a\mid b \iff -a\mid b \iff a\mid -b \iff -a\mid -b \iff |a|\mid|b|$.*
3. *$a\mid b$ και $b\mid c \implies a\mid c$.*
4. *$a\mid b$ και $c\mid d \implies ac\mid bd$.*
5. *$a\mid b$ και $a\mid c \implies a\mid bx+cy$, $\forall x,y\in\mathbb{Z}$.*

6. $a \mid b \quad \text{και} \quad b \neq 0 \implies |a| \leq |b|$.

7. $a \mid b \quad \text{και} \quad b \mid a \implies |a| = |b|$.

Θεώρημα 0.3.4 (Ευκλείδεια Διαίρεση)**.** *Αν a, b είναι ακέραιοι, και $b \neq 0$, τότε υπάρχει μοναδικό ζεύγος ακεραίων q, r έτσι ώστε:*

$$a = bq + r, \qquad 0 \leq r < |b|$$

Υπενθυμίζουμε ότι ο θετικός ακέραιος $p > 1$ καλείται **πρώτος** αν ο p δεν έχει γνήσιους θετικούς διαιρέτες. Ο θετικός ακέραιος a καλείται **σύνθετος** αν $a = bc$, για κάποιους θετικούς ακέραιους b, c, όπου $1 < b, c < a$. Οι πρώτοι αριθμοί αποτελούν θεμελιώδη έννοια στα Μαθηματικά και ικανοποιούν σημαντικές ιδιότητες

Πρόταση 0.3.5. *Έστω $a, b \in \mathbb{Z}$ και p είναι ένας πρώτος αριθμός έτσι ώστε: $p \mid ab$. Τότε είτε $p \mid a$ είτε $p \mid b$.*

Θεώρημα 0.3.6 (Θεμελιώδες Θεώρημα της Αριθμητικής)**.** *Κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί ως γινόμενο $a = p_1 p_2 \cdots p_n$ πρώτων αριθμών $p_1, p_2, \cdots, p_n$ με μοναδικό τρόπο: αν $a = q_1 q_2 \cdots q_m$, όπου οι θετικοί ακέραιοι $q_1, q_2, \cdots, q_m$ είναι πρώτοι, τότε $n = m$ και υπάρχει μια αναδιάταξη των πρώτων p_i και q_j, όπου $1 \leq i, j \leq n$, έτσι ώστε: $p_i = q_i$, $1 \leq i \leq n$.*

Σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής, κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί με μοναδικό τρόπο ως γινόμενο

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \tag{1}$$

όπου οι $p_1, p_2, \cdots, p_k$ είναι διακεκριμμένοι πρώτοι αριθμοί με $p_1 < p_2 < \cdots < p_k$, και $a_i \geq 1$, $1 \leq i \leq k$. Η παράσταση (1) καλείται η **πρωτογενής ανάλυση** του a. Η πρωτογενής ανάλυσης ενός θετικού ακεραίου $a > 1$ μπορεί να επεκταθεί στην πρωτογενή ανάλυση κάθε ακεραίου $a \neq 0, \pm 1$: $a = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

Όπως προκύπτει εύκολα από την πρωτογενή ανάλυση (1) ενός θετικού ακεραίου $a > 1$, ένας θετικός ακέραιος d είναι διαιρέτης του a αν και μόνο αν μπορεί να γραφεί στην μορφή $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, όπου $0 \leq b_i \leq a_i$, $1 \leq i \leq k$.

Αν $n_1, n_2, \cdots, n_k$ είναι θετικοί ακέραιοι, τότε ένας **μέγιστος κοινός διαιρέτης** των $n_1, n_2, \cdots, n_k$ είναι ένας θετικός ακέραιος d ο οποίος ικανοποιεί τις ακόλουθες ιδιότητες:

1. $d \mid n_i$, $1 \leq i \leq k$.

2. Αν $\delta \in \mathbb{N}$ και $\delta \mid n_i$, $1 \leq i \leq k$, τότε $\delta \leq d$.

Παρόμοια ένα **ελάχιστο κοινό πολλαπλάσιο** των θετικών ακεραίων $n_1, n_2, \cdots, n_k$ είναι ένας θετικός ακέραιος e ο οποίος ικανοποιεί τις ακόλουθες ιδιότητες:

1. $n_i \mid e$, $1 \leq i \leq k$.

2. Αν $\epsilon \in \mathbb{N}$ και $n_i \mid \epsilon$, $1 \leq i \leq k$, τότε $e \leq \epsilon$.

Ο μέγιστος κοινός διαιρέτης, αντίστοιχα το ελάχιστο κοινό πολλαπλάσιο, θετικών ακεραίων a_i, $1 \leq i \leq k$, υπάρχει πάντα, είναι μοναδικός, αντίστοιχα μοναδικό, και συμβολίζεται με $(a_1, a_2, \cdots, a_k)$ ή $\text{ΜΚΔ}(a_1, a_2, \cdots, a_k)$, αντίστοιχα $[a_1, a_2, \cdots, a_k]$ ή $\text{ΕΚΠ}(a_1, a_2, \cdots, a_k)$. Οι θετικοί ακέραιοι $a_1, a_2, \cdots, a_k$ καλούνται **πρώτοι μεταξύ τους**, αντίστοιχα **πρώτοι μεταξύ τους ανά δύο**, αν $(a_1, a_2, \cdots, a_k) = 1$, αντίστοιχα αν $(a_i, a_j) = 1$, $1 \leq i \neq j \leq n$.

Πρόταση 0.3.7. *Έστω $a, b \in \mathbb{N}$.*

1. *Αν $\delta \in \mathbb{N}$ και $\delta \mid a$ και $\delta \mid b$, τότε $\delta \mid (a, b)$.*

2. *Αν $\epsilon \in \mathbb{N}$ και $a \mid \epsilon$ και $b \mid \epsilon$, τότε $[a, b] \mid \epsilon$.*

3. *Υπάρχουν ακέραιοι x και y έτσι ώστε: $(a, b) = ax + by$. Αντίστροφα, αν $ax + by = 1$, τότε $(a, b) = 1$.*

4. *Αν* $a \mid bc$ *και* $(a,b) = 1$, *τότε* $a \mid c$.

5. $$(a,b)[a,b] = ab$$

6. *Οι θετικοί ακέραιοι* a *και* b *μπορούν να γραφούν ως γινόμενο μη-αρνητικών δυνάμεων των ίδιων διακεκριμένων πρώτων αριθμών* $p_1, p_2, \cdots, p_k$*:*

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{και} \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}, \quad \text{όπου} \quad a_i, b_i \geq 0, \quad 1 \leq i \leq k$$

και τότε:

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\min\{a_k,b_k\}}$$
$$[a,b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdots p_k^{\max\{a_k,b_k\}}$$

Οι ισχυρισμοί της παραπάνω Πρότασης γενικεύονται εύκολα για πεπερασμένο πλήθος θετικών ακεραίων $a_1, a_2, \cdots, a_k$.

0.4 Μιγαδικοί Αριθμοί

Επεκτάσεις του συνόλου των ακεραίων αριθμών αποτελούν με σειρά γενικότητας:

1. Το σύνολο $\mathbb{Q}$ των ρητών αριθμών:
$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$$
όπου μπορούμε να υποθέσουμε ότι $(a,b) = 1$. Το σύνολο $\mathbb{Q}$ προκύπτει ως επέκταση του συνόλου $\mathbb{Z}$ των ακεραίων, έτσι ώστε εξισώσεις της μορφής $bx = a$, $a, b \in \mathbb{Z}$, $b \neq 0$, να έχουν λύση.

2. Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών το οποίο προκύπτει ως επέκταση του συνόλου $\mathbb{Q}$ των ρητών αριθμών, έτσι ώστε εξισώσεις της μορφής $x^2 = 2$ να έχουν λύση.

3. Το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών το οποίο προκύπτει ως επέκταση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών, έτσι ώστε εξισώσεις της μορφής $x^2 + 1 = 0$ να έχουν λύση.

Θεωρούμε γνωστή τη θεμελίωση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών. Το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών μπορεί να οριστεί κατά πολλούς (ισοδύναμους) τρόπους, κάποιους από αυτούς θα δούμε και σε επόμενα κεφάλαια. Άτυπα μπορούμε να πούμε ότι ένας μιγαδικός αριθμός είναι της μορφής $a + bi$, όπου οι a, b είναι πραγματικοί αριθμοί, και ικανοποιούνται οι εξής κανόνες ισότητας, πρόσθεσης «+» και πολλαπλασιασμού «·»:

(i) $a + bi = c + di$, όπου $a, b, c, d \in \mathbb{R}$, αν και μόνο αν $a = c$ και $b = d$.

(ii) $(a + bi) + (c + di) = (a + c) + (b + d)i$ και $(a + bi) - (c + di) = (a + c) - (b + d)i$.

(iii) $(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)i$.

Αυστηρότερα, θεωρούμε το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$ του συνόλου $\mathbb{R}$ των πραγματικών αριθμών με τον εαυτό του, στο οποίο ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·», ως εξής:

$$(a,b) + (c,d) = (a + c, b + d) \quad \text{και} \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc)$$

Θέτοντας $1 = (1,0)$ και $i = (0,1)$, και ορίζοντας $r(a,b) = (ra, rb)$, $\forall r \in \mathbb{R}$, θα έχουμε:

$$i^2 = -1 \quad \text{και} \quad (a,b) = a(1,0) + b(0,1) = a1 + bi \quad \text{και} \quad 1 \cdot (a,b) = (a,b) = (a,b) \cdot 1$$

Συνήθως παραλείπουμε το σύμβολο $1 = (1,0)$ στην γραφή $(a,b) = a1 + bi$. Έτσι το ζεύγος $(a,b) \in \mathbb{R} \times \mathbb{R}$ μπορεί να γραφεί ως $z = a + bi$ και καλείται **μιγαδικός αριθμός** με *πραγματικό μέρος* τον πραγματικό αριθμό a και *φανταστικό μέρος* τον πραγματικό αριθμό b. Ο μιγαδικός αριθμός i καλείται **φανταστική μονάδα**. Το σύνολο όλων των μιγαδικών αριθμών συμβολίζεται με $\mathbb{C}$, και ως σύνολο ταυτίζεται με το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$, το οποίο θεωρούμε πάντα εφοδιασμένο με τις πράξεις πρόσθεσης και πολλαπλασιασμού, όπως αυτές περιγράφονται με βάση τους παραπάνω συμβολισμούς, από τις σχέσεις (i), (ii), και (iii). Χάριν ευκολίας στον συμβολισμό, ακολουθούμε τις εξής συμβάσεις: $0 + 0i = 0$ και $a + 0i = a$.

Για τις παραπάνω πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» μιγαδικών αριθμών ικανοποιούνται οι ακόλουθες ιδιότητες, $\forall x, y, z \in \mathbb{C}$:

1. $(x + y) + z = x + (y + z)$ (Προσεταιριστικότητα της πρόσθεσης)
2. $x + y = y + x$ (Μεταθετικότητα της πρόσθεσης)
3. $x + 0 = x = 0 + x$ (Ύπαρξη ουδετέρου στοιχείου ως προς την πρόσθεση)
4. Για κάθε $x \in \mathbb{Z}$, $x + (-x) = 0 = (-x) + x$ (Ύπαρξη αντιθέτου στοιχείου ως προς την πρόσθεση)
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Προσεταιριστικότητα του πολλαπλασιασμού)
6. $x \cdot y = y \cdot x$ (Μεταθετικότητα του πολλαπλασιασμού)
7. $x \cdot (y + z) = x \cdot y + x \cdot z$ και $(x + y) \cdot z = x \cdot z + y \cdot z$ (Επιμεριστικότητα του πολλαπλασιασμού ως προς την πρόσθεση)
8. $x \cdot 1 = x = 1 \cdot x$ (Ύπαρξη ουδετέρου στοιχείου ως προς τον πολλαπλασιασμό)

Από τις παραπάνω ιδιότητες έπονται άμεσα οι εξής νόμοι διαγραφής:

$$x + y = x + z \implies y = z \qquad \text{(Νόμος διαγραφής ως προς την πρόσθεση)}$$

$$x \cdot y = x \cdot z \text{ και } x \neq 0 \implies y = z \quad \text{(Νόμος διαγραφής ως προς τον πολλαπλασιασμό)}$$

Αν $z = a + bi$ είναι ένας μιγαδικός αριθμός, τότε ο *συζυγής* του z είναι ο μιγαδικός αριθμός $\overline{z} = a - bi$, και έτσι ορίζεται η απεικόνιση συζυγίας

$$\bar{}: \mathbb{C} \longrightarrow \mathbb{C}, \quad z = a + bi \longmapsto \overline{z} = a - bi$$

η οποία ικανοποιεί τις ακόλουθες ιδιότητες, $\forall z, w \in \mathbb{C}$:

(α) $\overline{\overline{z}} = z$.

(β) $\overline{z \pm w} = \overline{z} \pm \overline{w}$.

(γ) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

(δ) $z \cdot \overline{z} \in \mathbb{R}$. Επιπλέον $z \cdot \overline{z} \geq 0$ και $z \cdot \overline{z} = 0$ αν και μόνο αν $z = 0$.

Το *μέτρο* του μιγαδικού αριθμού $z = a + bi$ ορίζεται να είναι ο μη-αρνητικός πραγματικός αριθμός

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

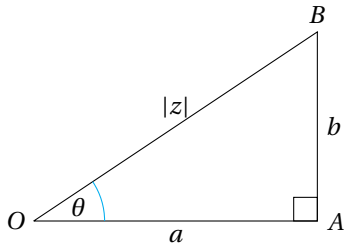
Τότε εύκολα βλέπουμε ότι $\forall z, w \in \mathbb{C}$:

$$|z| \in \mathbb{R}, \quad |z| \geq 0 \quad \text{και} \quad |z| = 0 \iff z = 0, \qquad |z \cdot w| = |z| \cdot |w|$$

Παρατηρούμε ότι, αν z είναι ένας μη-μηδενικός μιγαδικός αριθμός, τότε ορίζεται ο μιγαδικός αριθμός $\frac{\overline{z}}{|z|^2}$ και ισχύει ότι $z \cdot \frac{\overline{z}}{|z|^2} = \frac{|z|}{|z|^2} = 1$. Επομένως:

9. Για κάθε $0 \neq x \in \mathbb{C}$, υπάρχει μιγαδικός αριθμός y έτσι ώστε $x \cdot y = 1 = y \cdot x$ (Ύπαρξη αντιστρόφου στοιχείου ως προς τον πολλαπλασιασμό)

Επιστρέφοντας προσωρινά στην μορφή ενός μιγαδικού αριθμού $z = a + bi$ ως ζεύγους $z = (a, b)$ και άρα ως σημείου του επιπέδου $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, ο μη αρνητικός αριθμός $|z| = \sqrt{a^2 + b^2}$ είναι η απόσταση του σημείου του επιπέδου με συντεταγμένες (a, b) από την αρχή των αξόνων με συντεταγμένες $(0, 0)$. Στο ορθογώνιο τρίγωνο OBA το οποίο σχηματίζεται στο επίπεδο $\mathbb{R}^2$ από την αρχή των αξόνων $O = (0, 0)$, από το σημείο $B = (a, b)$, και το σημείο $A = (a, 0)$, έστω θ η γωνία την οποία σχηματίζουν οι πλευρές OB και OA:



Τότε θα έχουμε την *πολική μορφή* του μιγαδικού αριθμού $z = a + bi$:

$$a = |z| \cos\theta, \qquad b = |z| \sin\theta, \quad \text{και} \quad z = |z|\big(\cos\theta + i \sin\theta\big)$$

Η πολική μορφή ενός μιγαδικού αριθμού είναι χρήσιμη στον προσδιορισμό της n-οστής δύναμης ενός μιγαδικού αριθμού, όπως πιστοποιεί το ακόλουθο Θεώρημα.

Θεώρημα 0.4.1 (Θεώρημα De Moivre). [6] *Αν $z = a + bi = r(\cos\theta + i \sin\theta)$, όπου $r = |z|$, τότε, $\forall n \geq 1$:*

$$z^n = (a + bi)^n = [r(\cos\theta + i \sin\theta)]^n = r^n(\cos n\theta + i \sin n\theta)$$

Χρησιμοποιώντας τον τύπο του Euler $e^{ix} = \cos x + i \sin x$, $\forall x \in \mathbb{R}$, μπορούμε επίσης να γράψουμε:

$$z = re^{i\theta} = r(\cos\theta + i \sin\theta)$$

Ένας μιγαδικός αριθμός z καλείται **n-οστή ρίζα της μονάδας** αν $z^n = 1$. Το σύνολο όλων των n-οστών ριζών της μονάδας συμβολίζεται με

$$\mathsf{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

Αν $z = r(\cos\theta + i \sin\theta) \in \mathsf{U}_n$ είναι μια n-οστή ρίζα της μονάδας, όπου $r = |z|$, τότε $|z^n| = |z|^n = 1$ και άρα επειδή ο πραγματικός αριθμός $|z|$ είναι μη αρνητικός θα έχουμε $r = |z| = 1$. Επιπλέον

$$z^n = 1 \implies \cos n\theta + i \sin n\theta = 1 \implies \cos n\theta = 1 \text{ και } \sin n\theta = 0 \implies \theta = \frac{2k\pi}{n}, \quad k \in \mathbb{Z}$$

Ιδιαίτερα έπεται ότι

$$\text{αν} \quad \omega_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}, \quad \text{τότε} \quad \omega_n^n = 1$$

Μια n-οστή ρίζα της μονάδας z καλείται **πρωταρχική n-οστή ρίζα της μονάδας**, αν $z^k \neq 1$ για κάθε θετικό ακέραιο $k < n$.

Ισχυρισμός: Ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας και, αν ω είναι μια πρωταρχική n-οστή ρίζα της μονάδας, τότε υπάρχει μια ισότητα συνόλων:

$$\mathsf{U}_n = \{\omega^k \in \mathbb{C} \mid k \in \mathbb{Z}\} = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$$

[6] Abraham de Moivre (26 Μαίου 1667 - 27 Νοεμβρίου 1754) [https://en.wikipedia.org/wiki/Abraham_de_Moivre]: Γάλλος μαθηματικός με συμβολή στην τριγωνομετρία, στους μιγαδικούς αριθμούς, και στη Θεωρία Πιθανοτήτων. Γνωστός κυρίως για το παρόν Θεώρημα που φέρει το όνομά του.

Πράγματι από την Ευκλείδεια Διαίρεση του ακεραίου k με το n: $k = nq + r$, $0 \leq r < n$, έπεται ότι

$$\omega^k = \omega^{nq+r} = (\omega^n)^q \cdot \omega^r = \omega^r$$

Επιπλέον τα στοιχεία $1, \omega, \omega^2, \cdots, \omega^{n-1}$ είναι ανά δύο διαφορετικά διότι αν $\omega^k = \omega^l$, όπου $0 \leq k, l \leq n-1$ και όπου χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $l \leq k$, τότε $\omega^{k-l} = 1$ και αυτό είναι άτοπο διότι $k - l < n$ και ο αριθμός ω είναι μια n-στή ρίζα της μονάδας.

Ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μοναδας διότι, αν $\omega_n^k = 1$, όπου $k < n$, τότε όπως παραπάνω θα έχουμε $\frac{2\pi}{n} = \frac{2l\pi}{n}$, για κάποιον ακέραιο l και επομένως $k = nl$, δηλαδή $n \mid k$ και άρα $n \leq k$ το οποίο είναι άτοπο. Επομένως ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας.

Επομένως κάθε άλλη n-οστή ρίζα της μονάδας είναι ένας εκ των μιγαδικών αριθμών

$$\mathsf{U}_n = \{\omega_n^0 = 1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\}$$