1. Τα θεμελιώδη αριθμητικά συστήματα

Με τον όρο θεμελιώδη αριθμητικά συστήματα εννοούμε τα σύνολα $\mathbb{N}$ των φυσικών αριθμών, $\mathbb{Z}$ των ακεραίων, $\mathbb{Q}$ των ρητών και $\mathbb{R}$ των πραγματικών. Από αυτά, το σύνολο $\mathbb{N}$ είναι πρωτογενές ενώ οι ακέραιοι και οι ρητοί είναι παράγωγα των φυσικών και των ακεραίων αντίστοιχα με σχετικά απλή διαδικασία. Τέλος οι πραγματικοί αριθμοί προκύπτουν από τους ρητούς κατά μη τετριμένο τρόπο. Στο κεφάλαιο αυτό θα ορίσουμε τα θεμελιώδη συστήματα και θα συζητήσουμε κάποιες από τις βασικές ιδιότητές τους. Οι αριθμοί αποτελούν τον "ακρογωνιαίο λίθο" των μαθηματικών αλλά και όλων των επιστημών που το περιεχόμενό τους βασίζεται σε ποσοτικούς προσδιορισμούς. Η σαφής γνώση της δομής τους αποτελεί απαραίτητη προυπόθεση για ενασχόληση με οποιοδήποτε κλάδο των μαθηματικών.

2. Οι φυσικοί αριθμοί

Το σύνολο $\mathbb{N}$ των φυσικών αριθμών είναι αναμφίβολα το απλούστερο από τα αριθμητικά συστήματα. Οι φυσικοί αριθμοί είναι τα πρώτα μαθηματικά αντικείμενα που έγιναν αντιληπτά από τον άνθρωπο στη διαδικασία της εξέλιξής του. Έχουν διακριτή δομή κατανοητή από τον οποιοδήποτε. Για παράδειγμα είναι σαφές ότι αν βρισκόμαστε στον φυσικό αριθμό m τότε μπορούμε να μεταβούμε στον $m+1$ και μεταξύ τους δεν υπάρχει κανένας φυσικός. Επίσης καταλαβαίνουμε πως μπορούμε να προσθέσουμε και να πολλαπλασιάσουμε φυσικούς αριθμούς και τέλος ότι αν μας δοθούν δύο φυσικοί αριθμοί τότε είτε είναι ίσοι είτε ο ένας είναι μεγαλύτερος από τον άλλο. Συνοψίζοντας τα παραπάνω μπορούμε να πούμε ότι το σύνολο των φυσικών αριθμών είναι ένα σύνολο $\mathbb{N}$ εφοδιασμένο με δύο πράξεις " $+$ "," $\cdot$ " και μια διάταξη " $<$ " που ικανοποιούν κάποιες προφανείς ιδιότητες. Το ερώτημα που τίθεται είναι το ακόλουθο. Μεταξύ όλων των ιδιοτήτων των φυσικών αριθμών ποιες είναι οι ελάχιστες δυνατές που αν υποθέσουμε ότι ισχύουν σε ένα σύνολο $\mathbf{N}$ τότε το $\mathbf{N}$ υποχρεωτικά ταυτίζεται με το σύνολο των φυσικών αριθμών; Οι ελάχιστες αυτές ιδιότητες εντοπίστηκαν μετά το 1850 από διάφορους μαθηματικούς, ανεξάρτητα, και έχει επικρατήσει να ονομάζονται "Αξιώματα Peano" παρά το γεγονός ότι ο Peano δεν ήταν ο πρώτος που τα όρισε!

Το σύνολο των φυσικών αριθμών, όπως θα οριστεί στο παρόν κείμενο δε θα περιλαμβάνει το μηδεν. Ορισμένοι συγγραφεις θεωρούν το μηδέν σα στοιχείο των φυσικών αριθμών. Κανένας από τους δύο ορισμούς δε θεωρείται λάθος και η παρουσία ή όχι του μηδενός δεν επιρρεάζει την ευρύτερη δομή του συνόλου.

3. Τα αξιώματα του Peano

Αξιωματα 0.1. *(Peano). Το σύνολο $\mathbb{N}$ των φυσικών αριθμών είναι ένα σύνολο τέτοιο ώστε υπάρχει μια απεικόνιση $s : \mathbb{N} \to \mathbb{N}$ με τις εξής ιδιότητες:*

(i.) *Υπάρχει ένα στοιχείο $1 \in \mathbb{N}$.*
(ii.) *Για κάθε $n \in \mathbb{N}$, $s(n) \neq 1$.*
(iii.) *Η s είναι αμφιμονοσήμαντη (1-1).*
(iv.) *Εάν $U \subset \mathbb{N}$ τέτοιο ώστε $1 \in U$ και για κάθε $n \in \mathbb{N}$, $s(n) \in U$, τότε $U = \mathbb{N}$. (Αρχή της Μαθηματικής Επαγωγής).*

Ας παρατηρήσουμε ότι οι βασικές ιδιότητες του $\mathbb{N}$, δηλαδή οι πράξεις και η διάταξη απουσιάζουν πλήρως από τις παραπάνω ιδιότητες. Το κυρίαρχο στοιχείο των αξιωμάτων είναι η συνάρτηση s (συνάρτηση επομένου), όπου όταν θα ορίσουμε τις πράξεις το $s(n) = n+1$. Πρέπει επίσης να τονιστεί ότι οι φυσικοί αριθμοί δεν απλά το σύνολο $\mathbb{N}$. Το σημαντικότερο στοιχείο τους είναι η δομή τους που περιγράφεται, σε επίπεδο αξιωμάτων από την συνάρτηση s και την αρχή της επαγωγής, ενώ σε μεταγενέστερο στάδιο θα περιγράφεται από τις πράξεις και τη διάταξη. Το πλέον ενδιαφέρον από τα αξιώματα είναι αυτό της Αρχής της Μαθηματικής Επαγωγής. Θα παίξει καθοριστικό ρόλο τόσο στον ορισμό των πράξεων όσο και στον ορισμό της διάταξης. Θα μπορούσε να θεωρηθεί ότι είναι μια θεμελιώδης αρχή "διαχείρισης του απείρου". Σαν άμεση συνέπεια έχει τη μαθηματική επαγωγή σαν αποδειχτική διαδικασία. Ακριβέστερα ισχύει το ακόλουθο:

Πρόταση 0.2. *Έστω $P(n)$ μια μαθηματική πρόταση που διατυπώνεται για κάθε $n \in \mathbb{N}$. Υποθέτουμε τα ακόλουθα:*

(i.) *Η $P(1)$ ισχύει.*

(ii.) *Αν ισχύει η $P(n)$ τότε αποδεικνύεται ότι ισχύει η $P(s(n))$.*

Τότε συμπεραίνουμε ότι για κάθε $n \in \mathbb{N}$ ισχύει η $P(n)$. Δηλαδή το σύνολο $\{n \in \mathbb{N} :$ η $P(n)$ ισχύει$\}$ ισούται με το $\mathbb{N}$.

Η απόδειξη της πρότασης είναι άμεση συνέπεια του αξιώματος (iv.), παρατηρώντας ότι το σύνολο $\{n \in \mathbb{N} :$ η $P(n)$ ισχύει$\}$ ικανοποιεί τις υποθέσεις του (iv.) και άρα ταυτίζεται με το $\mathbb{N}$.

Αξίζει να παρατηρήσουμε ότι η προηγούμενη πρόταση έχει μεταμαθηματικό περιεχόμενο. Ουσιαστικά αφορά τον τρόπο που αποδεικνύουμε ιδιότητες των φυσικών αριθμών (και όχι μόνο). Βεβαίως το ότι το αξίωμα (iv.) συνεπάγεται την πρόταση 0.2 είναι σχεδόν φανερό. Το αντίστροφο δε συμβαίνει. Δηλαδή αν δεχτούμε ότι ισχύει η πρόταση 0.2 τότε το αξίωμα (iv.) δεν είναι συνέπεια αυτής. Θα δούμε παρακάτω ότι το αξίωμα (iv.) είναι συνέπεια μιας πολύ φυσιολογικής ιδιότητας της διάταξης στο $\mathbb{N}$.

Πρόταση 0.3. *Για κάθε $n \in \mathbb{N}$ με $n \neq 1$ υπάρχει $m \in \mathbb{N}$ τέτοιο ώστε $s(m) = n$.*

Απόδειξη. Θα κάνουμε χρήση της μαθηματικής επαγωγής. Θα θέσουμε

$$U = \{n \in \mathbb{N} : \text{ υπάρχει } m \in \mathbb{N} \text{ ώστε } s(m) = n\}$$

και θα δείξουμε ότι $U \cup \{1\} = \mathbb{N}$.

Πράγματι $1 \in U \cup \{1\}$. Αν το $n \in U \cup \{1\}$ τότε για $m = n \in \mathbb{N}$ έχουμε ότι $s(n) = s(m)$ και επομένως $s(n) \in U$. Άρα $s(n) \in U \cup \{1\}$. Από μαθηματική επαγωγή έχουμε ότι $U \cup \{1\} = \mathbb{N}$. Επομένως για κάθε $n \in \mathbb{N}$ με $n \neq 1$ έχουμε ότι $n \in U$ και συνεπώς, από τον ορισμό του U, υπάρχει $m \in \mathbb{N}$ τέτοιο ώστε $n = s(m)$. □

Τα αξιώματα του Peano εξασφαλίζουν ότι ουσιαστικά υπάρχει ένα μόνο ζεύγος $(\mathbb{N}, s)$ που τα ικανοποιεί. Με αυτό εννοούμε ότι αν (N', s') είναι ένα άλλο ζεύγος που ικανοποιεί τα αξιώματα του Peano τότε υπάρχει $\Phi : \mathbb{N} \to N'$ 1-1 και επί ώστε $s'(\Phi(n)) = \Phi(s(n))$. Αυτό σημαίνει ότι μια ιδιότητα ισχύει στο $(\mathbb{N}, s)$ αν και μόνο αν ισχύει στο (N', s') και υπό αυτήν την έννοια το ζεύγος $(\mathbb{N}, s)$ είναι μοναδικό. Η απόδειξη αυτής της ιδιότητας δίνεται στην επόμενη πρόταση.

Πρόταση 0.4. *Υπάρχει μοναδικό ζεύγος $(\mathbb{N}, s)$ που ικανοποιεί τα αξιώματα Peano.*

Περιγραφή Απόδειξης. Έστω ζεύγη $(\mathbb{N}, s)$ και (N', s') που ικανοποιούν τα αξιώματα του Peano. Επομένως υπάρχουν $1 \in \mathbb{N}$ και $1' \in N'$. Η Φ ορίζεται με επαγωγή. Ορίζουμε $\Phi(1) = 1'$ και αν το $\Phi(n)$ έχει οριστεί, θέτουμε $\Phi(s(n)) = s'(\Phi(n))$. Η αρχή της μαθηματικής επαγωγής είναι αυτή που θα μας εξασφαλίσει ότι το σύνολο $\{n \in \mathbb{N} :$ το $\Phi(n)$ έχει οριστεί$\}$

είναι το σύνολο $\mathbb{N}$ καθώς επίσης ότι η Φ είναι 1-1 και επί. Προφανώς για κάθε $n \in \mathbb{N}$, $\Phi(s(n)) = s'(\Phi(n))$. □

4. Αναδρομικοί ορισμοί

Ο προσεκτικός, αλλά όχι με αρκετή εμπειρία αναγνώστης, θα παρατηρήσει ότι η απόδειξη της προηγούμενης πρότασης είναι αρκετά πλήρης, γεγονός που δε δικαιολογεί τον όρο "περιγραφή της απόδειξης" που διατυπώνεται στην αρχή της. Αν εξετάσουμε προσεκτικά το περιεχόμενο της απόδειξης θα συμφωνίσουμε ότι το βασικό στοιχείο της είναι ο ορισμός της συνάρτησης $Q : (\mathbb{N}, s) \to (N', s')$. Ο ορισμός της Q γίνεται επαγωγικά (ή με αναδρομή) και το σημείο που πρέπει να επισημανθεί είναι ότι ο επαγωγικός ορισμός δεν είναι απλή συνέπεια της Μαθηματικής Επαγωγής. Εκτός αυτής χρησιμοποιεί και στοιχεία από τη θεωρία συνόλων. Η δυνατότητα να ολοκληρώνουμε ορισμούς νέων μαθηματικών αντικειμένων μέσω αναδρομής είναι το περιεχόμενο του Θεωρήματος της Αναδρομής που είναι το ακόλουθο:

Θεωρημα 0.5 (Αναδρομής). *Έστω A σύνολο, $h : A \to A$ συνάρτηση και $a \in A$. Τότε υπάρχει συνάρτηση $\Phi : \mathbb{N} \to A$ ώστε*

(i) $\Phi(1) = a$.
(ii) *Για κάθε $n \in \mathbb{N}$, $\Phi(s(n)) = h(\Phi(n))$.*

Ο ενδιαφερόμενος αναγνώστης μπορεί να βρει την απόδειξη του Θεωρήματος σε βιβλία Θεωρίας Συνόλων. Για παράδειγμα περιέχεται στο εξαιρετικό κείμενο του Γ. Μοσχοβάκη "Σημειώσεις στη Συνολοθεωρία".

Αξίζει να παρατηρήσει κανείς ότι η πρόταση 0.4 που διασφαλίζει τη μοναδικότητα του ζεύγους $(\mathbb{N}, s)$ είναι άμεση συνέπεια του Θεωρήματος της Αναδρομής. Αρκεί να θέσει κανείς όπου $A = N'$, $h = s'$ και $a = 1'$.

5. Οι πραξεις στο $\mathbb{N}$

Όταν λέμε ότι ένα σύνολο A είναι εφοδιασμένο με μια πράξη "$*$" εννοούμε την ύπαρξη μιας συνάρτησης $* : A \times A \to A$ ώστε $*(a, b) = a * b$. Θα ορίσουμε τώρα τις δύο θεμελιώδεις πράξεις στο $\mathbb{N}$, δηλαδή την πρόσθεση "$+$" και τον πολλαπλασιασμό "$\cdot$". Δεδομένου ότι οι πράξεις είναι συναρτήσεις ο ακριβής ορισμός τους απαιτεί τη χρήση του Θεωρήματος Αναδρομής που έχουμε ήδη αναφέρει. Στον ορισμό που αναφέρεται αυτό παραλείπεται.

Ορισμος 0.6. (Πρόσθεση) Ορίζουμε μια πράξη $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, την οποία καλούμε πρόσθεση, με τις εξής ιδιότητες:

i. Για κάθε $n \in \mathbb{N}$, $n + 1 = s(n)$.
ii. Για κάθε $(n, m) \in \mathbb{N} \times \mathbb{N}$, $n + s(m) = s(n + m)$.

Ενώ για κάθε $(n, m) \in \mathbb{N} \times \mathbb{N}$ χρησιμοποιώντας την Αρχή της Μαθηματικής Επαγωγής έχουμε ορίσει το $n + m$, εν τούτοις ο ορισμός της πρόσθεσης σαν συνάρτηση απαιτεί το Θεώρημα της Αναδρομής και αυτό το βήμα το παραλείπουμε.

Ορισμος 0.7. (Πολλαπλασιασμός) Ορίζουμε μια πράξη $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, την οποία καλούμε πολλαπλασιασμό, με τις εξής ιδιότητες:

i. Για κάθε $n \in \mathbb{N}$, $n \cdot 1 = n$.
ii. Για κάθε $(n, m) \in \mathbb{N} \times \mathbb{N}$, $n \cdot s(m) = n \cdot m + n$.

Πρόταση 0.8. *Εάν $n, m, k \in \mathbb{N}$, τότε*

α. i. $n + (m + k) = (n + m) + k$ *(προσεταιριστική ιδιότητα).*
ii. $n + m = m + n$ *(μεταθετική ιδιότητα).*
iii. *Εάν* $n + m = n + k$, *τότε* $m = k$ *(νόμος διαγραφής).*

β. i. $n(mk) = (nm)k$ *(προσεταιριστική ιδιότητα).*
ii. $nm = mn$ *(μεταθετική ιδιότητα).*
iii. *Εάν* $nm = nk$, *τότε* $m = k$ *(νόμος διαγραφής).*

γ. $(n + m)k = nk + mk$ *(επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση).*

Απόδειξη. Αποδεικνύουμε μόνο την α.i. Έστω U το σύνολο όλων των $k \in \mathbb{N}$ για τα οποία

$$n + (m + k) = (n + m) + k$$

για όλα τα $n, m \in \mathbb{N}$. Λόγω του ορισμού 0.6 έχουμε

$$n + (m + 1) = n + s(m) = s(n + m) = (m + n) + 1$$

Άρα $1 \in U$. Έστω $k \in U$, τότε πάλι λογω του ορισμού 0.6 έχουμε

$$n + (m + s(k)) = n + s(m + k) = s(n + (m + k)) = s((n + m) + k) = (n + m) + s(k)$$

Άρα $s(k) \in U$ και λόγω του αξιώματος 0.1 (iv.) $U = \mathbb{N}$, και η ιδιότητα έχει αποδειχθεί.

Οι υπόλοιπες ιδιότητες αποδεικνύονται με χρήση Μαθηματικής Επαγωγής και αφήνονται στον αναγνώστη. □

6. Η διάταξη στο $\mathbb{N}$

Η διάταξη των φυσικών αριθμών είναι μια πολύ σημαντική συνιστώσα τ ης δομής τους. Η βασική ιδιότητά της είναι ότι είναι καλή διάταξη, δηλαδή ότι κάθε υποσύνολο έχει ελάχιστο στοιχείο. Αυτή η ιδιότητα που φαίνεται τελείως φυσιολογική είναι τόσο ισχυρή ώστε να μπορεί να αντικαταστήσει το αξίωμα της Μαθηματικής Επαγωγής. Το τελευταίο δείχνεται στην πρόταση 0.16.

Ορισμός 0.9. (Διάταξη) Έστω ένα σύνολο X. Ορίζουμε ως διάταξη στο X μια σχέση στο X, $R \subset X \times X$, που ικανοποιεί τις εξής ιδιότητες:

(i.) Για κάθε $x \in X$ έχουμε ότι $(x, x) \in R$. (αυτοπάθεια)
(ii.) Για κάθε $x, y \in X$ έχουμε ότι αν $(x, y) \in R$ και $(y, x) \in R$, τότε $x = y$. (αντισυμμετρικότητα)
(iii.) Για κάθε $x, y, z \in X$ τέτοια ώστε $(x, y) \in R$ και $(y, z) \in R$ έχουμε ότι $(x, z) \in R$. (μεταβατικότητα)

Συχνά συμβολίζουμε μια διάταξη με " $\leq$ " και αντί να γράφουμε $(x, y) \in \leq$ γράφουμε $x \leq y$ και θα λέμε ότι το x είναι μικρότερο ή ίσο του y. Το ζεύγος $(X, \leq)$ καλείται διατεταγμένος χώρος. Επίσης αν $x \leq y$ και $x \neq y$, γράφουμε $x < y$.

Αξίζει να παρατηρήσουμε στο σημείο αυτό ότι σε ένα διατεταγμένο χώρο $(X, \leq)$ δεν είναι πάντα σωστό ότι οποιαδήποτε δύο στοιχεία του, $x, y \in X$, είναι συγκρίσιμα, δηλαδή είτε $x \leq y$ είτε $y \leq x$. Θεωρήστε, για παράδειγμα, ένα σύνολο Y με τουλάχιστον δύο στοιχεία, $X = \mathcal{P}(Y)$ το δυναμοσύνολο του Y, δηλαδή το σύνολο που σαν στοιχεία του έχει όλα τα υποσύνολα του Y και τη σχέση διάταξης " $\leq$ " στο X, οπου $A \leq B$ αν $A \subset B$. Αν $x, y \in Y$ με $x \neq y$ και $A = \{x\}, B = \{y\}$, τότε τα A, B δεν είναι συγκρίσιμα.

Ορισμος 0.10. Ένας διατεταγμένος χώρος $(X, \leq)$ καλείται ολικά διατεταγμένος και η "$\leq$" καλείται ολική διάταξη αν οποιδήποτε δύο στοιχεία του X είναι συγκρίσιμα. Δηλαδή για κάθε $x, y \in X$ έχουμε ότι είτε $x \leq y$ είτε $y \leq x$.

Η διάταξη στο $\mathbb{N}$ θα οριστεί με τη βοήθεια της επόμενης πρότασης.

Προταση 0.11. *Έστω $n, m \in \mathbb{N}$. Τότε ακριβώς ένα από τα παρακάτω ισχύει.*

(a) $n = m$.
(b) *Υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $n = m + k$.*
(c) *Υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $m = n + k$.*

Αποδειξη. Για κάθε $n \in \mathbb{N}$ ορίζουμε $\Sigma_n = \{m \in \mathbb{N} : (a)\ n = m$ ή (b) υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $n = m + k$ ή (c) υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $m = n + k\}$ και θέτουμε επίσης $U = \{n \in \mathbb{N} : \Sigma_n = \mathbb{N}\}$. Χρησιμοποιώντας την Αρχή της μαθηματικής επαγωγής θα δείξουμε ότι $U = \mathbb{N}$.

Το $1 \in U$. Πράγματι, για κάθε $n \in \mathbb{N}$ έχουμε ότι είτε το $n = 1$, το οποίο άμεσα έπεται ότι $n \in \Sigma_1$ (περίπτωση (a)), είτε $n \neq 1$. Τότε από πρόταση 0.3 υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $n = s(k) = 1 + k \in \Sigma_1$ (περίπτωση (b)).

Ας υποθέσουμε ότι $n \in U$, δηλαδή $\Sigma_n = \mathbb{N}$. Θα δείξουμε ότι $\Sigma_{s(n)} = \mathbb{N}$, δηλαδή $s(n) \in U$. Πράγματι, για κάθε $m \in \mathbb{N}$ έχουμε ότι $m \in \Sigma_n$. Επομένως

(a) είτε $n = m$. Τότε $s(n) = s(m) = m + 1$ και συνεπώς $m \in \Sigma_{s(n)}$ (περίπτωση (b)).
(b) είτε υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $n = m + k$. Τότε $s(n) = s(m + k) = m + (k + 1)$. Συνεπώς $m \in \Sigma_{s(n)}$ (περίπτωση (b)).
(c) είτε υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $m = n + k$.
  (c′) Αν $k = 1$ τότε $m = n + 1 = s(n)$ και συνεπώς $m \in \Sigma_{s(n)}$ (περίπτωση (a)).
  (c″) Αν $k \neq 1$, από πρόταση 0.3 υπάρχει $l \in \mathbb{N}$ τέτοιο ώστε $s(l) = k$. Τότε $m = n + k = n + s(l) = n + l + 1 = (n + 1) + l = s(n) + l$. Συνεπώς $m \in \Sigma_{s(n)}$ (περίπτωση (c)).

Δηλαδή για κάθε $m \in \mathbb{N}$ έχουμε ότι $m \in \Sigma_{s(n)}$. Άρα $\Sigma_{s(n)} = \mathbb{N}$ και $s(n) \in U$. Από Αρχή της Μαθηματικής Επαγωγής έχουμε ότι $U = \mathbb{N}$. Εύκολα παρατηρεί κανείς ότι ακριβώς μία από τις παραπάνω περιπτώσεις θα ισχύει. Ειδάλλως θα υπήρχαν $n, k \in \mathbb{N}$ τέτοια ώστε $n + k = n$. Ισοδύναμα $n + k + 1 = n + 1$ και από το νόμο της διαγραφής έπεται ότι $k + 1 = s(k) = 1$ το οποίο αντιφάσκει με τα αξιώματα Peano. □

Ορισμος 0.12. (Διάταξη στο $\mathbb{N}$). Εάν $n, m \in \mathbb{N}$ και υπάρχει $k \in \mathbb{N}$ ώστε $n + k = m$, τότε λέμε ότι ο m είναι μεγαλύτερος του n (ή ισοδύναμα ο n μικρότερος του m) και συμβολίζουμε $m > n$ (ή ισοδύναμα $n < m$). Θα γράφουμε $n \leq m$ αν είτε $n = m$ είτε $n < m$.

Είναι εύκολο να ελέγξει κανείς ότι η σχέση "$\leq$" που μόλις ορίσαμε αποτελεί σχέση διάταξης στο $\mathbb{N}$ και μάλιστα σύμφωνα με την πρόταση 0.11 αποτελεί ολική διάταξη.

Η ακόλουθη πρόταση παραθέτει κάποιες βασικές ιδιότητες της διάταξης των φυσικών αριθμών που σχετίζονται με τις πράξεις. Η απόδειξή τους αφήνεται ως άσκηση στον αναγνώστη.

Προταση 0.13. *Έστω $n, m \in \mathbb{N}$.*

i. *Εάν $n < m$, τότε $n + k < m + k$, για κάθε $k \in \mathbb{N}$.*
ii. *Εάν $n < m$, τότε $nk < mk$, για κάθε $k \in \mathbb{N}$.*

Ορισμοι 0.14. Έστω $(X, \leq)$ διατεταγμένος χώρος, $A \subset X$ και $a \in A$.

(i.) Το a καλείται ελάχιστο (minimum) του A αν για κάθε $b \in A$ ισχύει ότι $a \leq b$.

(ii.) Το X καλείται καλά διατεταγμένο αν κάθε μη κενό υποσύνολό του έχει ελάχιστο στοιχείο και η $\leq$ καλείται καλή διάταξη.

Ας παρατηρήσουμε ότι κάθε καλά διατεταγμένο σύνολο είναι και ολικά διατεταγμένο. Πράγματι αν $(X, \leq)$ καλά διατεταγμένος χώρος και $x, y \in X$, τότε το σύνολο $S = \{x, y\} \subset X$ έχει ελάχιστο. Αυτό συνεπάγεται άμεσα ότι καθιστά τα δύο αυτά στοιχεία συγκρίσιμα, αφού το ελάχιστο θα είναι μικρότερο ή ίσο του άλλου.

ΘΕΩΡΗΜΑ 0.15. *Το $\mathbb{N}$ είναι καλά διατεταγμένο.*

ΑΠΟΔΕΙΞΗ. Υποθέτουμε ότι υπάρχει μη κενό $M \subset \mathbb{N}$ που δεν έχει ελάχιστο στοιχείο για να καταλήξουμε σε άτοπο, δείχνοντας ότι $M = \emptyset$. Θέτουμε $B = \{n \in \mathbb{N} : \text{για κάθε } k \leq n \text{ το } k \notin M\}$. Κάνοντας χρήση της επαγωγής θα δείξουμε ότι το $B = \mathbb{N}$ και κατεπέκταση $M = \emptyset$.
Το $1 \notin M$, διότι αν ανήκε θα αποτελούσε το ελάχιστο στοιχείο του M το οποίο έρχεται σε αντίθεση με την υπόθεση ότι το M δεν έχει ελάχιστο στοιχείο. Επομένως $1 \in B$.
Αν $n \in B$ τότε για κάθε $k \leq n$ το $k \notin M$. Επομένως $s(n) \notin M$, διότι αν άνηκε θα αποτελούσε το ελάχιστο στοιχείο του M, το οποίο οδηγεί σε άτοπο. Από επαγωγή έχουμε ότι $B = \mathbb{N}$. □

Είναι ενδιαφέρον ότι η απόδειξη της ιδιότητας της καλής διάταξης στο $\mathbb{N}$ απαιτεί την χρήση του αξιώματος της Μαθηματικής Επαγωγής. Όπως έχουμε ήδη αναφέρει στην αρχή του κεφαλαίου, αυτό είναι αναγκαίο διότι η ιδιότητα της καλής διάταξης είναι σχεδόν ισοδύναμη με την Αρχή της Μαθηματικής Επαγωγής.

ΠΡΟΤΑΣΗ 0.16. *Έστω $(N, \leq)$ ένα μη κενό καλά διατεταγμένο σύνολο, $1 = \min N$ και συνάρτηση $s : N \to N$ με τις εξής ιδιότητες:*

(i.) *Η s είναι 1-1.*

(ii.) *Για κάθε $n \in N$ με $n \neq 1$ υπάρχει $m \in N$ τέτοιο ώστε $n = s(m)$.*

(iii.) *Για κάθε $n \in N$ έχουμε ότι $n < s(n)$.*

Το ζεύγος $(N, \leq)$ ικανοποιεί τα αξιώματα Peano και πρόκειται συνεπώς για το σύνολο των φυσικών αριθμών.

ΑΠΟΔΕΙΞΗ. Καταρχάς παρατηρούμε ότι για κάθε $n \in N$, $1 \leq n < s(n)$ και συνεπώς $s(n) \neq 1$. Απομένει να δείξουμε ότι ικανοποιεί την Αρχή της Μαθηματικής Επαγωγής. Έστω $U \subset N$ τέτοιο ώστε $1 \in U$ και για κάθε $n \in U$ έχουμε ότι το $s(n) \in U$. Θα δείξουμε ότι $U = N$. Πράγματι θα υποθέσουμε ότι δεν ισχύει και θα καταλήξουμε σε άτοπο. Έστω, λοιπόν, το $V = N \setminus U \neq \emptyset$ και $n = \min V$. Επειδή $1 \in U$ έπεται ότι $n \neq 1$ και συνεπώς υπάρχει $m \in N$ τέτοιο ώστε $s(m) = n$. Επειδή $m < s(m) = n$ και n το ελάχιστο στοιχείο του V έπεται ότι $m \notin V$ και συνεπώς $m \in U$. Από την υπόθεση για το U έχουμε ότι $n = s(m) \in U$, το οποίο είναι άτοπο. □

7. Ο Ευκλείδιος Αλγόριθμος

Ο Ευκλείδιος Αλγόριθμος αφορά την εύρεση του μέγιστου κοινού διαιρέτη (μ.κ.δ.) δύο φυσικών αριθμών. Περιέχεται στα Στοιχεία του Ευκλείδη σε γεωμετρική μορφή και αφορά μια μέθοδο ελέγχου του κατά πόσο δύο ευθύγραμμα τμήματα είναι ισομετρήσιμα. Δηλαδή κατά πόσο υπάρχει ένα τρίτο ευθύγραμμο τμήμα ακέραια πολλαπλάσια του οποίου είναι τα δύο προηγούμενα. Όπως είναι γνωστό αυτή την ιδιότητα δε την έχουν όλα τα ζεύγη ευθυγράμμων τμημάτων. Για παράδειγμα η υποτείνουσα και μια κάθετη πλευρά ενός ισοσκελούς ορθογωνίου τριγώνου δεν είναι ισομετρήσιμα. Το πραγματικό όμως περιεχόμενο του Ευκλείδιου Αλγορίθμου είναι η εύρεση του μ.κ.δ. που έχουμε ήδη αναφέρει.

Ο Ευκλείδιος Αλγόριθμος περιγράφει την ακόλουθη μέθοδο. Ας υποθέσουμε ότι m, n είναι φυσικοί αριθμοί με $n < m$. Τότε $m = np_1 + v_1$ με p_1, v_1 φυσικούς αριθμούς και $v_1 < n$. Αν $v_1 = 0$ τότε η διαδικασία τερματίζεται. Διαφορετικά $n = p_2 v_1 + v_2$ με p_2, v_2 φυσικούς αριθμούς και $v_2 < v_1$. Πάλι αν $v_2 = 0$ η διαδικασία τερματίζεται. Διαφορετικά $v_1 = p_3 v_2 + v_3$ και συνεχίζουμε όπως προηγουμένως. Με τη διαδικασία αυτή ορίζουμε μια γνησίως φθίνουσα ακολουθία $n > v_1 > v_2 > \ldots > v_k$ η οποία τερματίζεται στο v_k αν και μόνο αν το $v_k = 0$. Το θεώρημα αποφαίνεται ότι αν $v_k = 0$ τότε ο μ.κ.δ. των m και n είναι ο v_{k-1}. Άρα πράγματι η διαδικασία αυτή οδηγεί στην εύρεση του μ.κ.δ. των m, n. Η απόδειξη στηρίζεται στην ακόλουθη απλή πρόταση.

Ας αρχίσουμε με κάποιους συμβολισμούς. Αν $p \in \mathbb{N}$ και $q \in \mathbb{N} \cup \{0\}$ θα γράφουμε $p|q$ αν ο p διαιρεί τον q (κάθε $p \in \mathbb{N}$ διαιρεί το 0). Επίσης για $m, n \in \mathbb{N}$ θέτουμε $\Delta(m, n) = \{p \in \mathbb{N} : p|n \text{ και } p|m\}$.

Πρόταση 0.17. *Έστω $n, m \in \mathbb{N}$ με $n < m$ και $m = np + v$ όπου $p, v \in \mathbb{N}$. Τότε $\Delta(m, n) = \Delta(n, v)$.*

Απόδειξη. Θα δείξουμε ότι $\Delta(n, v) \subset \Delta(m, n)$ και αντίστροφα. Έστω $l \in \Delta(n, v)$. Τότε $l|n$ και $l|v$. Επομένως $l|np + v$. Δηλαδή $l|m$. Αντίστροφα αν $l \in \Delta(m, n)$, τότε $l|m$ και $l|n$. Άρα $l|m - np$. Επομένως $l|v$, αφού $v = m - np$. □

Στον Ευκλείδιο Αλγόριθμο που τερματίζεται στο v_k ($v_k = 0$) η πρόταση έχει την ακόλουθη συνέπεια. $\Delta(m, n) = \Delta(n, v_1) = \Delta(v_1, v_2) = \ldots = \Delta(v_{k-2}, v_{k-1})$. Επειδή $v_{k-1}|v_{k-2}$ έπεται ότι $v_{k-1} = \max \Delta(v_{k-2}, v_{k-1}) = \max \Delta(m, n)$. Άρα v_{k-1} είναι ο μ.κ.δ. των m, n.

Παρατήρηση. Αξίζει να σημειώσουμε ότι ο τερματισμός του Ευκλείδιου Αλγόριθμου σε πεπερασμένα βήματα είναι συνέπεια της καλής διάταξης του συνόλου $\mathbb{N}$. Πράγματι μια ολική διάταξη είναι καλή αν και μόνο αν οι γνησίως φθίνουσες ακολουθίες είναι πεπερασμένες. Έτσι θεωρώντας οι αρχαίοι Έλληνες ότι ο Ευκλείδιος Αλγόριθμος τερματίζεται, ουσιαστικά δέχονταν ότι η διάταξη του $\mathbb{N}$ είναι καλή. Θα πρέπει επίσης να επισημάνουμε ότι η Μαθηματική Επαγωγή σαν αποδεικτική μέθοδος διατυπώθηκε για πρώτη φορά από τον F. Maurolicos (Φ. Μαυρόλυκος) (1494-1575) Σικελό Ελληνικής καταγωγής και εν συνεχεία από τον Pascal (1623-1662). Εντούτοις στα Στοιχεία του Ευκλείδη υπάρχουν προτάσεις που η απόδειξή του απαιτεί Μαθηματική Επαγωγή η οποία εφαρμόζεται ατελώς.

8. Ύπαρξη μοντέλου του $\mathbb{N}$

Ένα σημείο που αξίζει επίσης να σχολιάσουμε αφορά την ύπαρξη ενός συνόλου $\mathbb{N}$ εφοδιασμένου με μια συνάρτηση $s : \mathbb{N} \to \mathbb{N}$ που να ικανοποιεί τα αξιώματα του Peano. Στο ερώτημα αυτό μπορεί να διατυπωθεί ο αντίλογος σε δύο κατευθύνσεις.

Καταρχάς θα μπορούσε κάποιος να απαντήσει ότι βεβαίως και υπάρχει και είναι οι φυσικοί αριθμοί που γενιές και γενιές έχουν μεγαλώσει μαζί τους. Και αυτό ακούγεται λογικό δεδομένου ότι οι φυσικοί αριθμοί θεωρούνται το πιο στέρεο μαθηματικό οικοδόμημα. Αν συλλογιστούμε όμως τους φυσικούς αριθμούς αντιλαμβανόμαστε ότι έχουμε πλήρη γνώση ενός πολύ μικρού αρχικού διαστήματος. Για δε το υπόλοιπο μέρος τους έχουμε διαμορφώσει ένα ισχυρό πιστεύω ότι εξελίσσεται με τρόπο παρόμοιο με αυτό που παρατηρούμε στο μικρό αρχικό διάστημα του. Τα αξιώματα που παραθέσαμε στοχεύουν να ορίσουν στο $\mathbb{N}$ τη δομή που πιστεύουμε ότι πρέπει να έχει. Η απάντηση λοιπόν στο πρώτο αντίλογο είναι ότι είμαστε γνώστες ενός μικρού μέρους του $\mathbb{N}$ και το μεγαλύτερο μέρος του διαφεύγει πλήρως της εμπειρίας μας.

Ο δεύτερος αντίλογος αφορά την έκφραση "να βρούμε ένα σύνολο $\mathbb{N}$ και μια συνάρτηση $s : \mathbb{N} \to \mathbb{N}$ ώστε να ικανοποιούνται τα αξιώματα". Και η ερώτηση είναι απλή. Πως είναι δυνατόν να μπορούμε να αποδείξουμε αξιώματα; Αν αυτό συμβαίνει τότε αυτά δεν είναι αξιώματα αλλά συνέπειες αξιωμάτων!

Όλες αυτές οι παρατηρήσεις έχουν ισχυρή βάση αλήθειας. Πράγματι, οποιαδήποτε μαθηματική θεωρία βασίζεται στις θεμελιώδεις (μη ορίσιμες) έννοιες και θεμελιώδεις (μη αποδείξιμες) προτάσεις απ΄ όπου με βάση τους θεμελιώδεις νόμους της λογικής αναδεικνύεται ο επιστημονικός πλούτος. Το σημαντικό είναι ότι μια μαθηματική θεωρία μπορεί να αποτελεί μέρος μιας ευρύτερης θεωρίας της οποίας τα αξιώματα να επιτρέπουν την κατασκευή συνόλων και συναρτήσεων που να ικανοποιούν τα αξιώματα της επι μέρους θεωρίας. Για παράδειγμα τα αξιώματα Peano για το $\mathbb{N}$ μπορούν να θεωρηθούν στο ευρύτερο πλαίσιο της θεωρίας συνόλων και εκεί είναι εφικτή η κατασκευή ενός συνόλου $\mathbb{N}$ και μιας $s : \mathbb{N} \to \mathbb{N}$ ώστε να ικανοποιούνται τα αξιώματα Peano. Η απόδειξη αυτού του ισχυρισμού βρίσκεται εκτός του πλαισίου και των στόχων του μαθήματος και για το λόγο αυτό θα δεχτούμε αξιωματικά ότι υπάρχει ένα ζεύγος $(\mathbb{N}, s)$ που ικανοποιεί τα αξιώματα Peano.