ΠΩΣ ΠΡΕΠΕΙ ΝΑ ΟΡΙΖΟΝΤΑΙ ΟΙ ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ;

ΗΛΙΑΣ ΛΑΜΠΑΚΗΣ-4ο Γυμνάσιο Πύργου

Στην σελίδα 162 του σχολικού βιβλίου Μαθηματικών, (ομάδας προσανατολισμού θετικών σπουδών), Β΄ Γενικού Λυκείου βρίσκουμε τον ορισμό,

ΟΡΙΣΜΟΣ

Κάθε ακέραιος $p \neq 0, \pm 1$ λέγεται **πρώτος αριθμός** ή απλώς **πρώτος**, αν οι μόνοι θετικοί διαιρέτες του είναι οι 1 και $|p|$.

Στην σελίδα 165 του ίδιου βιβλίου, βρίσκουμε το θεώρημα,

ΘΕΩΡΗΜΑ 8

Αν ένας πρώτος p διαιρεί το γινόμενο $\alpha\beta$ δύο ακέραιων, τότε διαιρεί έναν, τουλάχιστον, από τους ακεραίους αυτούς.

Και σε πολλά άλλα σχολικά βιβλία βρίσκουμε τον πιο πάνω ορισμό σε σχέση με την έννοια των πρώτων αριθμών ως στοιχείων του συνόλου των ακεραίων.

Όμως το $\mathbb{Z}$, δεν είναι το μόνο σύνολο αριθμών στο οποίο μπορεί να αναπτυχθεί θεωρία διαιρετότητας και ως επακόλουθο αυτής θεωρία παραγοντοποιησιμότητας των στοιχείων του. Υπάρχουν πολλά σύνολα αριθμών και μάλιστα πολύ ευρύτερα του $\mathbb{Z}$, (δηλαδή περιέχουν το $\mathbb{Z}$), εφοδιασμένα με τις ίδιες πράξεις που είναι εφοδιασμένο το $\mathbb{Z}$, με τις ίδιες ιδιότητες που έχουν οι πράξεις στο $\mathbb{Z}$, τα οποία διαθέτουν πρώτους αριθμούς. Ο ορισμός όμως των πρώτων αριθμών σε αυτά τα σύνολα δεν είναι αυτός που δίνεται στην σελίδα 162 του σχολικού βιβλίου της Β΄ Λυκείου.

Ως ορισμός των πρώτων αριθμών σε αυτά τα σύνολα δίνεται η διατύπωση που αναφέρεται στην σελίδα 165 του σχολικού βιβλίου της Β΄ Λυκείου. Δηλαδή, το Θεώρημα 8 της σελίδας 165 του σχολικού βιβλίου της Β΄ Λυκείου δίνεται ως ορισμός των πρώτων αριθμών στα σύνολα αυτά με κατάλληλη βέβαια προσαρμογή σε σχέση με την φύση των στοιχείων του συνόλου ήτοι,

Ορισμός. Ένα μη μηδενικό στοιχείο p μίας ακέραιας περιοχής R καλείται πρώτο, (στοιχείο–αριθμός), αν και μόνο αν το p δεν αντιστρέφεται και $p|a\,b$ συνεπάγεται είτε $p|a$, είτε $p|b$ για $a, b \in R$.

Με τον όρο ακέραια περιοχή εννοούμε ένα σύνολο αριθμών, (στοιχείων), εφοδιασμένο με πρόσθεση και πολλαπλασιασμό οι ιδιότητες των οποίων είναι ακριβώς ίδιες με αυτές των αντίστοιχων πράξεων στο $\mathbb{Z}$. Δηλαδή, το σύνολο αυτό είναι ένας μεταθετικός δακτύλιος με μονάδα χωρίς μηδενοδιαιρέτες όπως και το $\mathbb{Z}$, (χωρίς μηδενοδιαιρέτες σημαίνει, οποτεδήποτε $a\,b = 0$ είτε $a = 0$, είτε $b = 0$).

Ο ορισμός των πρώτων αριθμών που δίνεται στα σχολικά βιβλία έλκει την καταγωγή του από την επιθυμία να τονιστεί ότι οι πρώτοι αριθμοί δεν είναι παραγοντοποιήσιμοι στο σύνολο αριθμών που ανήκουν. Όμως υπάρχουν περιπτώσεις συνόλων αριθμών που στοιχεία τους δεν είναι παραγοντοποιήσιμα αλλά για τα στοιχεία αυτά δεν ισχύει κάτι ανάλογο του Θεωρήματος 8 της σελίδας 165 του σχολικού βιβλίου Β΄ Λυκείου.

Γενικά, ότι δεν είναι παραγοντοποιήσιμο εντός ενός συνόλου αριθμών, δεν σημαίνει ότι είναι πρώτο στοιχείο, (αριθμός).

Πριν δώσουμε σχετικό παράδειγμα, ας αναφέρουμε πως νοείτε η παραγοντοποίηση σε ένα σύνολο αριθμών. Πρώτα από όλα ένα στοιχείο a είναι αντιστρέψιμο αν υπάρχει στοιχείο b ώστε $a\,b = 1$, $(b = a^{-1})$. Αυτό σημαίνει ότι τα αντιστρέψιμα στοιχεία είναι μη μηδενικά. Επίσης σημαίνει πως σε ένα σύνολο αριθμών που κάθε μη μηδενικό στοιχείο του a είναι αντιστρέψιμο μπορούμε πάντα να γράφουμε $a = a\,1 = a\,(a\,a^{-1}) = (a\,a)\,a^{-1} = b\,a^{-1}$. Άρα, κάθε μη μηδενικό στοιχείο σε ένα τέτοιο σύνολο, (ένα σώμα όπως λέγεται), παραγοντοποιείται. Επίσης, αν a, b είναι μη μηδενικά στοιχεία ενός σώματος $a = a\,(b\,b^{-1}) = (a\,b^{-1})\,b = g\,b$. Κάθε μη μηδενικό στοιχείο ενός σώματος διαιρεί όλα τα μη μηδενικά στοιχεία του σώματος.

Συμπεραίνουμε πως σε ένα σώμα δεν έχει νόημα να μιλάμε για ύπαρξη μη παραγοντοποιήσιμων στοιχείων. Όλα τα μη μηδενικά στοιχεία παραγοντοποιούνται με πολλούς τρόπους. Γι΄ αυτό περιοριζόμαστε σε σύνολα που ορισμένα στοιχεία τους μόνο είναι αντιστρέψιμα και τα υπόλοιπα από αυτά δεν είναι. Τέτοια σύνολα είναι οι ακέραιες περιοχές. Αν $a = b\,g$ σε μία ακέραια περιοχή, και το b είναι αντιστρέψιμο, τότε $g = a\,b^{-1}$ δηλαδή, $a = b\,(a\,b^{-1}) = a\,1$ και στην περίπτωση αυτή η παραγοντοποίηση είναι τετριμμένη.

Θα λέμε ότι ένα μη μηδενικό στοιχείο ακέραιας περιοχής παραγοντοποιείται με μη τετριμμένο τρόπο, (παραγοντοποιείται), αν $a = b\,g$ με b, g μη αντιστρέψιμα στοιχεία. Ένα στοιχείο ακέραιας περιοχής που δεν παραγοντοποιείται, (δηλαδή που παραγοντοποιείται μόνο με τετριμμένο τρόπο), θα λέγεται ανάγωγο στοιχείο.

Ορίζουμε τα πρώτα στοιχεία μίας ακέραιας περιοχής όπως στον προηγηθέντα δεύτερο ορισμό της σελίδας 1 του παρόντος, (όχι τον ορισμό του σχολικού βιβλίου Β΄ Λυκείου). Μπορούμε να δείξουμε ότι τα πρώτα στοιχεία μίας ακέραιας περιοχής έτσι όπως ορίστηκαν είναι ανάγωγα. Έστω p ένα πρώτο στοιχείο. Αν το $p = a\,b$ τότε, το $p|a\,b$ και από τον ορισμό του είτε $p|a$, είτε $p|b$. Έστω $p|a$. Τότε $a = p\,g$ και $p = a\,b = p\,g\,b$ ή $p\,(1 - g\,b) = 0$. Όμως $p \neq 0$ από τον ορισμό του. Δουλεύουμε σε ακέραια περιοχή που σημαίνει ότι κάθε γινόμενο ίσο με το 0 έχει έναν τουλάχιστον παράγοντα ίσο με μηδέν. Τελικά, $1 - g\,b = 0$ και $g\,b = 1$ που συνεπάγεται ότι το b είναι αντιστρέψιμο και η παραγοντοποίηση του p είναι τετριμμένη. Ομοίως δουλεύουμε αν $p|b$.

Να διευκρινίσουμε εδώ πως ο ορισμός των πρώτων τους θέλει μη μηδενικά, μη αντιστρέψιμα στοιχεία για τους πιο κάτω λόγους.

- Αν το $p = 0$ τότε, το $p|a\,b$ σημαίνει $a\,b = p\,g = 0\,g = 0$ και επειδή δουλεύουμε σε ακέραια περιοχή είτε $a = 0$, είτε $b = 0$ οπότε είναι σαν να λέμε $0|0$. Το 0 όντως διαιρεί τον εαυτό του αφού $0 = 0\,g$ για κάθε g όμως, η διαίρεση αυτή είναι «παθολογική», δεν έχει μοναδικό πηλίκο και το 0 διαιρεί μόνο το 0 κανένα άλλο μη μηδενικό στοιχείο.

- Αν το p είναι αντιστρέψιμο, το p διαιρεί κάθε στοιχείο της ακέραιας περιοχής αφού $a = p\,(p^{-1}\,a) = p\,b$ και $a = p\,b$ με p αντιστρέψιμο σημαίνει τετριμμένη παραγοντοποίηση για το a.

Δείξαμε πιο πάνω ότι, **τα πρώτα στοιχεία μίας ακέραιας περιοχής έτσι όπως ορίστηκαν είναι ανάγωγα**. Τώρα θα δείξουμε πως υπάρχουν ακέραιες περιοχές που κάποια ανάγωγα στοιχεία τους δεν είναι πρώτα. Το παράδειγμά μας είναι η ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

Είναι άμεση εφαρμογή των ιδιοτήτων της πρόσθεσης, του πολλαπλασιασμού και των ριζών να επαληθεύσουμε ότι το $\mathbb{Z}[\sqrt{-5}]$ είναι μεταθετικός δακτύλιος με μονάδα. Για να δείξουμε ότι είναι ακέραια περιοχή χρήσιμο είναι το εργαλείο της νόρμας ενός στοιχείου του $\mathbb{Z}[\sqrt{-5}]$ που ορίζεται ως εξής, αν $x = a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ τότε $\bar{x} = a - b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ και νόρμα του x είναι ο μη αρνητικός ακέραιος αριθμός $N(x) = x\,\bar{x} = a^2 + 5\,b^2$. Η νόρμα έχει τις ιδιότητες,

1. $N(x) = 0$ αν και μόνο αν $x = 0$. Πράγματι, αν $N(x) = 0 \Rightarrow a^2+5\,b^2 = 0$ που συνεπάγεται $a = 0$ και $b = 0$. Αν $a \neq 0$ ή $b \neq 0$ συνεπάγεται $a^2 + 5\,b^2 > 0$. Αντιστρόφως, αν $x = 0$ τότε $a + b\sqrt{-5} = 0$ συνεπάγεται $a = b = 0$ και $N(x) = 0$.

2. $N(x\,y) = N(x)\,N(y)$. Πράγματι, $N(x\,y) = (x\,y)\,\overline{(x\,y)} = x\,\bar{x}\,y\,\bar{y} = N(x)\,N(y)$.

3. $N(1 + 0\sqrt{-5}) = N(1) = 1$. Προκύπτει από τον ορισμό της νόρμας.

Έστω $x\,y = 0$ για δύο στοιχεία του $\mathbb{Z}[\sqrt{-5}]$. Τότε από την πρώτη και δεύτερη ιδιότητα της νόρμας έπεται $0 = N(x\,y) = N(x)\,N(y)$. Επειδή $N(x)$, $N(y)$ είναι ακέραιοι, έπεται είτε $N(x) = 0$, είτε $N(y) = 0$ που από την πρώτη ιδιότητα της νόρμας έπεται είτε $x = 0$, είτε $y = 0$.

Δείξαμε ότι το $\mathbb{Z}[\sqrt{-5}]$ είναι ακέραιη περιοχή. Για την νόρμα επίσης ισχύει το,

4. $N(x) = 1$ αν και μόνο αν το x είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$. Πράγματι, αν $N(x) = 1$ τότε, $x\,\bar{x} = 1$, το x αντιστρέφεται. Αντιστρόφως, έστω x αντιστρέψιμο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$. Τότε υπάρχει $y \in \mathbb{Z}[\sqrt{-5}]$ ώστε $x\,y = 1$ και $N(x\,y) = N(1) = 1$ από την τρίτη ιδιότητα της νόρμας. Από την δεύτερη ιδιότητα της νόρμας παίρνουμε $N(x)\,N(y) = 1$ και επειδή οι $N(x)$, $N(y)$ είναι μη αρνητικοί ακέραιοι έπεται $N(x) = 1$.

Τώρα θα δείξουμε πως υπάρχει ανάγωγο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$ που δεν είναι πρώτο. Ένα τέτοιο στοιχείο είναι το $2+\sqrt{-5}$. Αν το $2+\sqrt{-5}$ είχε μη τετριμμένη παραγοντοποίηση $2+\sqrt{-5}=a\,b$ τότε, τα a, b δεν είναι αντιστρέψιμα και $9=N(2+\sqrt{-5})=N(a)\,N(b)$. Όμως από την ιδιότητα 4 της νόρμας $N(a)\neq 1$, $N(b)\neq 1$ γιατί τα a, b δεν είναι αντιστρέψιμα. Από τον ορισμό της νόρμας, (μη αρνητικός ακέραιος), και το γεγονός ότι $2+\sqrt{-5}\neq 0$ έπεται ότι, $N(a)>1$, $N(b)>1$.

Άρα, $N(a)=N(b)=3$. Αν $a=g+d\sqrt{-5}$ τότε, $N(a)=3$ συνεπάγεται $g^2+5\,d^2=3$. Όμως g, d είναι ακέραιοι. Αν $d=0$ τότε, $g^2=3$ άτοπο γιατί $\sqrt{3}$ είναι άρρητος. Αν $d\neq 0$ τότε, $d^2\geq 1$ και $g^2+5\,d^2\geq 5$ αντιβαίνοντας το $g^2+5\,d^2=3$. Τελικά, το $2+\sqrt{-5}$ δεν έχει παραγοντοποίηση στο $\mathbb{Z}[\sqrt{-5}]$, $2+\sqrt{-5}=a\,b$ με a, b μη αντιστρέψιμα. Δείξαμε ότι το $2+\sqrt{-5}$ είναι ανάγωγο.

Όμως $(2+\sqrt{-5})\,(2-\sqrt{-5})=9=3\cdot 3$ έπεται ότι $(2+\sqrt{-5})|3\cdot 3$. Το $2+\sqrt{-5}$ δεν είναι αντιστρέψιμο από την ιδιότητα 4 της νόρμας. Αν το $2+\sqrt{-5}$ ήταν πρώτο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$ σύμφωνα με τον ορισμό των πρώτων στοιχείων σε ακέραιες περιοχές θα έπρεπε $(2+\sqrt{-5})|3$. Ας υποθέσουμε ότι $(2+\sqrt{-5})|3$. Τότε, $3=(2+\sqrt{-5})\,(a+b\sqrt{-5})$ και $N(3)=N(2+\sqrt{-5})\,N(a+b\sqrt{-5})$ ή $9=9\,(a^2+5\,b^2)$ ή $1=a^2+5\,b^2$ με a, b ακέραιους. Αν $b=0$ τότε, $a=\pm 1$ και $3=(2+\sqrt{-5})\,(\pm 1)$ ή $\pm 3-2=\sqrt{-5}$ άτοπο γιατί $\sqrt{-5}$ δεν είναι ακέραιος. Αν $b\neq 0$ τότε, $a^2+5\,b^2\geq 5$ αντιβαίνοντας το $1=a^2+5\,b^2$. Άρα, ο $2+\sqrt{-5}$ δεν διαιρεί το 3 και δεν είναι πρώτος στο $\mathbb{Z}[\sqrt{-5}]$.

Στη συνείδηση των ασχολούμενων με τα Μαθηματικά της δευτεροβάθμιας εκπαίδευσης είναι καταγεγραμμένο ότι πρώτοι αριθμοί είναι αυτοί που δεν παραγοντοποιούνται, ή που έχουν τετριμμένη παραγοντοποίηση του τύπου ο εαυτός τους επί ένα αντιστρέψιμο στοιχείο. Στο $\mathbb{Z}$ τα αντιστρέψιμα στοιχεία είναι τα ± 1. Όμως δείξαμε πως σε ευρύτερα του $\mathbb{Z}$ σύνολα ότι δεν παραγοντοποιείται δεν σημαίνει πως έχει υποχρεωτικά την ιδιότητα του Θεωρήματος 8 της σελίδας 165 του σχολικού βιβλίου της Β΄ Λυκείου.

Γι΄ αυτό ο ορισμός των πρώτων αριθμών σε ευρύτερα σύνολα του $\mathbb{Z}$ είναι ο δεύτερος ορισμός που ανφέρουμε στην πρώτη σελίδα του παρόντος ακριβώς για να μην γίνεται η προαναφερθείσα σύγχυση μεταξύ μη παραγοντοποιησιμότητας και της ιδιότητας του Θεωρήματος 8 της σελίδας 165 του σχολικού βιβλίου της Β΄ Λυκείου που είναι χαρακτηριστική των πρώτων αριθμών. Τελικά,

Ότι είναι πρώτος αριθμός δεν παραγοντοποιείται αλλά ότι δεν παραγοντοποιείται δεν είναι υποχρεωτικά πρώτος αριθμός σε σύνολα ευρύτερα του $\mathbb{Z}$. Στο $\mathbb{Z}$ όμως οι πιο πάνω έννοιες ταυτίζονται λόγω μιας επιπλέον ιδιότητας που έχουν οι ακέραιοι καθώς και κάποια άλλα σύνολα αριθμών να είναι περιοχές κυρίων ιδεωδών.