Εισαγωγή στη Θεωρία δακτυλίων

Βαγγέλης Φελουζής

Περιεχόμενα

Κεφάλαιο 1

Η Γενική Θεωρία

1.1 Στοιχεία από τη Θεωρία των Αριθμών

Για να κατανοήσει κάποιος καλύτερα τη Θεωρία Δακτυλίων είναι χρήσιμο να γνωρίζει κάποια στοιχειώδη πράγματα από τη Θεωρία των Αριθμών. Η παράγραφος αυτή δεν έχει σα σκοπό μια πλήρη ανάπτυξη της θεωρίας αριθμών αλλά να υπενθυμίσει περιληπτικά πως θεμελιώνονται οι έννοιες του «φυσικού αριθμού» και του «ακέραιου» αριθμού. Το σύνολο των ακεραίων αριθμών αποτελεί ένα είδους «πρότυπου» δακτυλίου και πολλές έννοιες που θα διαπραγματευτούμε στις σημειώσεις αυτές αντιστοιχούν σε έννοιες που ορίζονται στους ακέραιους. Πολλές μέθοδοι της θεωρίας αριθμών γενικεύονται άμεσα ή έμμεσα και στη θεωρία των δακτυλίων. Κάποιες από αυτές περιγράφονται εδώ για να βοηθηθεί (ελπίζουμε) ο σχετικά άπειρος στη θεωρία αριθμών αναγνώστης.

Με $\mathbb{N} = \{0, 1, 2, \dots\}$ θα συμβολίζουμε το σύνολο των φυσικών αριθμών και με $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \dots\}$ το σύνολο των ακεραίων.

Το σύνολο των φυσικών αριθμών διέπεται από τις παρακάτω αρχές που ονομάζονται τα Αξιώματα του Peano:

Αξίωμα 1

Το σύνολο $\mathbb{N}$ περιέχει ένα συγκεκριμένο στοιχείο που ονομάζεται ***μηδέν*** *και συμβολίζεται με 0.*

Αξίωμα 2

Στο σύνολο $\mathbb{N}$ ορίζεται μία 1-1 συνάρτηση $f : \mathbb{N} \to \mathbb{N}$ που λέγεται η ***συνάρτηση του επομένου****. Αν $n \in \mathbb{N}$ ο $f(n)$ λέγεται ο* ***επόμενος*** *του n.*

Αξίωμα 3

$0 \notin f(\mathbb{N})$, *δηλαδή δεν υπάρχει $n \in \mathbb{N}$ με $f(n) = 0$.*

Ορισμός 1

$$\boxed{\begin{array}{l} 1 = f(0) \\ 2 = f(1) = f(f(0)) \\ 3 = f(2) \\ 4 = f(3) \\ \ldots\ldots\ n+1 = f(n) \end{array}}$$

Αξίωμα 4 *[Αρχή Επαγωγής]*
Αν A είναι ένα υποσύνολο του συνόλου $\mathbb{N}$ των φυσικών αριθμών που ικανοποιεί τα εξής:
1. $0 \in A$
2. *Για κάθε $n \in A$ ισχύει ότι $n+1 \in A$,*
τότε $A = \mathbb{N}$.

Οι δύο βασικές πράξεις σε αυτά τα σύνολα είναι η πρόσθεση $+$ και ο πολλαπλασιασμός $\cdot$ που ορίζονται ως εξής:

Ορισμός 2 (Ορισμός της πρόσθεσης)
1. $n + 0 = n$ *για κάθε* $n \in \mathbb{N}$
2. $n + f(m) = f(n+m)$, *για οποιαδήποτε* $m, n \in \mathbb{N}$.

Ορισμός 3 (Ορισμός του Πολλαπλασιασμού)
1. $n0 = 0$ *για κάθε* $n \in \mathbb{N}$
2. $nf(m) = nm + n$, *για οποιαδήποτε* $m, n \in \mathbb{N}$.

Το ότι τα προηγούμενα ορίζουν πράγματι δύο πράξεις στο $\mathbb{N}$ εξασφαλίζεται από την Αρχή της Επαγωγής. Με τη βοήθεια αυτής της αρχής μπορούμε να αποδείξουμε ότι οι πράξεις ικανοποιούν τις εξής ιδιότητες:
1. **Προσεταιριστικότητα:** Για οποιαδήποτε $a, b, c \in \mathbb{N}$, $a+(b+c) = (a+b)+c$, $a(bc) = (ab)c$.
2. **Αντιμεταθετικότητα:** Για οποιαδήποτε $a, b \in \mathbb{N}$, $a + b = b + a$, $ab = ba$.
3. **Ύπαρξη Ουδέτερου στοιχείου:** Για κάθε $a \in \mathbb{N}$, $a + 0 = a$, $a1 = a$, όπου $1 = f(0)$.
4. **Επιμεριστικότητα του Πολλαπλασιασμού ως προς την Πρόσθεση:** Για οποιαδήποτε $a, b, c \in \mathbb{N}$, $a(b + c) = ab + ac$.

Ορισμός 4
*Στο $\mathbb{N}$ ορίζεται μία σχέση διάταξης $\leq$ όπου θα γράφουμε $a \leq b$ αν και μόνο αν υπάρχει ένα n με $a+n = b$. Ο a λέγεται μικρότερος ή ίσος από τον b και αντίστοιχα ο b μεγαλύτερος ή ίσος από τον a. Ο n είναι μοναδικός και συμβολίζεται με $b - a$. Ένα στοιχείο a ενός συνόλου A θα λέγεται το **μικρότερό** του στοιχείο (ή το ελάχιστό του) αν ισχύει $a \leq x$ για οποιοδήποτε $x \in A$. Θα γράφουμε $m < n$ αν $m \leq n$ και $m \neq m$.*

Από τον ορισμό είναι εύκολο να δείξουμε ότι ισχύουν τα παρακάτω:

1. Για κάθε n, $n \leq n$
2. Αν $m \leq n$, $n \leq r$ τότε $m \leq r$
3. Αν $m \leq n$ και $n \leq m$ τότε $n = m$
4. Για οποιαδήποτε m, n είτε $m \leq n$ είτε $n \leq m$.
5. Για οποιαδήποτε m, n, r αν $m \leq n$ τότε $n+r \leq m+r$.
6. Για οποιαδήποτε m, n, $r \neq 0$ αν $m \leq n$ τότε $mr \leq nr$.

Από την Αρχή της Επαγωγής έχουμε το παρακάτω βασικό και χρήσιμο θεώρημα:

Θεώρημα 1 *[Αρχή της Καλής Διάταξης]*
(α) Κάθε μη κενό υποσύνολο των φυσικών αριθμών έχει μικρότερο στοιχείο.
(β) Δεν υπάρχει γνήσια φθίνουσα ακολουθία φυσικών αριθμών.
Τα (α), (β) είναι ισοδύναμες προτάσεις.

Απόδειξη: Έστω A να είναι υποσύνολο των φυσικών αριθμών που δεν έχει μικρότερο στοιχείο και ας θεωρήσουμε το συμπλήρωμά του, $A^c = \{x \in \mathbb{N} : x \notin A\}$. Παρατηρείστε ότι $0 \in A^c$ διαφορετικά το A θα είχε μικρότερο στοιχείο (το 0). Ας υποθέσουμε ότι όλοι οι αριθμοί που είναι μικρότεροι ή ίσοι από n ανήκουν στο A^c. Τότε θα πρέπει και ο $n+1$ να ανήκει σε αυτό γιατί διαφορετικά ο $n+1$ θα ήταν το μικρότερο στοιχείο του A. Από την αρχή της επαγωγής θα πρέπει $A^c = \mathbb{N}$ άρα το A θα είναι το κενό σύνολο.Το πρώτο μέρος του θεωρήματος αποδείχτηκε.

Η ισοδυναμία του (α) με το (β) προκύπτει εύκολα, με την παρατήρηση ότι τα στοιχεία μίας γνήσια φθίνουσας ακολουθίας φυσικών αποτελούν ένα σύνολο χωρίς μικρότερο στοιχείο και αντίστροφα αν δοθεί ένα μη κενό υποσύνολο των φυσικών αριθμών χωρίς μικρότερο στοιχείο μπορούμε να φτιάξουμε μια γνήσια φθίνουσα ακολουθία από στοιχεία του (πως;). □

Με χρήση της Αρχής της Καλής Διάταξης αποδεικνύουμε την παρακάτω βασική ιδιότητα του συνόλου των φυσικών αριθμών:

Θεώρημα 2 (Η Αρχιμήδεια Ιδιότητα)
(α) Αν $a \neq 0$ τότε $1 < a$.
(β) Αν a, b είναι δύο φυσικοί αριθμοί με $0 < a < b$ τότε υπάρχει ένας αριθμός k με $b < ka$.

Απόδειξη: (α) Θα στηριχτούμε στην παρακάτω ιδιότητα της διάταξης:

$$\text{Αν } 0 < a < b \text{ και } 0 < a' \leq b' \text{ τότε } aa' < bb'$$

Αν υπάρχει φυσικός a με $0 < a < 1$ τότε θα είχαμε διαδοχικά ότι $0 < a^2 < a$, $0 < a^3 < a^2 \ldots$ και με αυτό τον τρόπο θα παίρναμε μία γνήσια φθίνουσα ακολουθία

$a > a^2 > a^3 > \cdots > a^n > a^{n+1} > \ldots$ και θα είχαμε έρθει σε αντίφαση με την Αρχή της Καλής Διάταξης.
(β). Αν $0 < a < b$ από το (α) θα έχουμε ότι $1 < a$ και πολλαπλασιάζοντας με b έχουμε ότι $b < ab$ που σημαίνει ότι για $k = b$ ισχύει ο ισχυρισμός μας. □

Περνάμε τώρα στα βασικά Θεωρήματα που μας ενδιαφέρουν.

Θεώρημα 3 *[Ευκλείδης-Η ταυτότητα της διαίρεσης.]*
Αν a, b είναι δύο φυσικοί αριθμοί με $0 < a \leq b$ τότε υπάρχουν δύο μοναδικού αριθμοί k, υ με το $0 \leq \upsilon < a$ τέτοιοι ώστε:

$$b = ka + \upsilon$$

Απόδειξη: Ας θεωρήσουμε το σύνολο A όλων των φυσικών αριθμών n που έχουν την ιδιότητα $na > b$. Το σύνολο αυτό είναι μη κενό λόγω της Αρχιμήδειας ιδιότητας. Συνεπώς θα έχει ένα μικρότερο στοιχείο $n_0 > 1$. Αν πάρουμε $k = n_0 - 1$ τότε $ka \leq b$ και υπάρχει υ με $b = ka + \upsilon$. Το υ είναι μικρότερο από a γιατί διαφορετικά θα υπήρχε φυσικός αριθμός c με $\upsilon = a + c$ και θα είχαμε ότι $b = ka + a + c = (k+1)a + c = n_0 a + c$. Αλλά $n_0 a > b$ και οδηγηθήκαμε σε άτοπο.

Η μοναδικότητα των k, υ προκύπτει ως εξής:

Ας υποθέσουμε ότι για κάποια k', υ' με $0 \leq \upsilon < a$ έχουμε ότι $b = k'a + \upsilon'$. Είτε $k \leq k'$ είτε $k' \leq k$ δηλαδή θα υπάρχει κάποιο d με $k' = k + d$ ή $k = k' + d$. Ας υποθέσουμε ότι $k' = k + d$ τότε $ka + ad + \upsilon' = ka + \upsilon = b$ και συνεπώς $\upsilon = ad + \upsilon'$. Επειδή $\upsilon < a$ θα έχουμε ότι $d = 0$ και συνεπώς $k = k', \upsilon = \upsilon'$.

Αν πάλι $k' = k + d$ με παρόμοιο συλλογισμό καταλήγουμε στο ίδιο συμπέρασμα.
□

> Ο μοναδικός αριθμός υ που ορίζεται στο προηγούμενο θεώρημα (για δοσμένους $0 < a \leq b$) λέγεται το **υπόλοιπο της διαίρεσης** του b με τον a και συμβολίζεται με $\Upsilon(b, a)$.

Μέχρι τώρα ασχολήθηκαμε αποκλειστικά με το σύνολο των φυσικών αριθμών. Περνάμε τώρα στο σύνολο $\mathbb{Z}$ των ακεραίων. Δίνουμε έναν πολύ σύντομο ορισμό του $\mathbb{Z}$. Για να δώσουμε την ιδέα που μας οδηγεί στον παρακάτω ορισμό - που από πρώτη άποψη φαίνεται περίεργος - σκεφτόμαστε για ποιό λογο να τους ορίσουμε. Από αλγεβρική άποψη ένα μειονέκτημα είναι οι φυσικοί αριθμοί ότι δεν αποτελούν ομάδα ως προς την πράξη της πρόσθεση [1], δεν λύνονται έτσι εξισώσεις της μορφής $x + a = b$. Αυτό μπορεί να διορθωθεί με την εισαγωγή των αρνητικών αριθμών, δηλαδή για κάθε μη μηδενικό $n \in \mathbb{N}$ να εισάγουμε ένα καινούργιο στοιχείο $\overline{n}$, ώστε $n + \overline{n} = 0$, τον **αντίθετο** του n.

[1] και ως προς τον πολλαπλασιασμό βέβαια, αλλά αυτό είναι ένα ζήτημα που θα ασχοληθούμε αφού λύσουμε τα προβλήματα της πρόσθεσης

Ας υποθέσουμε ότι τα έχουμε καταφέρει και έχουμε επεκτείνει το $\mathbb{N}$ σε ένα μεγαλύτερο σύνολο, όπου η εξίσωση $x + a = b$ λύνεται και η λύση της παριστάνεται με $a - b$. Ας φανταστούμε τον $a - b$ σαν ένα ζευγάρι (a, b). Έτσι το 2 αντιπροσωπεύεται από τα $(2, 0), (3, 1), (1000, 998) \ldots$ [2] και ο -2 από τα $(0, 2), (1, 3)$.

Ορισμός 5

Στο σύνολο $\mathbb{N} \times \mathbb{N}$ ορίζουμε μια σχέση ισοδυναμίας:

$$(m, n) \sim (m', n') \quad \Leftrightarrow m + n' = m' + n$$

και ορίζουμε σαν ***σύνολο των ακεραίων*** *το σύνολο πηλίκο*

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$$

Στο $\mathbb{Z}$ ορίζουμε δύο πράξεις $+, \cdot$ ως εξής:
Αν $[(m, n)]$ συμβολίζει την κλάση ισοδυναμίας που ορίζει το $(m, n) \in \mathbb{N} \times \mathbb{N}$ τότε

$$[(m, n)] + [(m', n')] = [(m + m', n + n')] \tag{1}$$

$$[(m, n)] \cdot [(m', n')] = [(mm' + nn', mn' + m'n)] \tag{2}$$

Εμείς παρακάτω για να επανέλθουμε στους συμβολισμούς που γνωρίζουμε από παλιά:
Με 0 θα συμβολίζουμε την κλάση του (0,0)
Με 1 θα συμβολίζουμε την κλάση του (1,0)
Αν n φυσικός με n θα συμβολίζουμε την κλάση του $(n, 0)$ και με $-n$ την κλάση του $(0, n)$.
Άλλες κλάσεις δεν υπάρχουν. Με αυτό τον τρόπο μπορούμε να φανταζόμαστε πάλι το σύνολο των ακεραίων σαν $\{\cdots - 5, -4, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Θα χρειαστούμε και μία γενίκευση της ταυτότητας της διαίρεσης για ακεραίους όταν ο διαιρέτης είναι θετικός και ο διαιρετέος οποιοσδήποτε ακέραιος. Η απόδειξη είναι ανάλογη με αυτή του Θεωρήματος 3. Παρ' όλα αυτά θα κάνουμε μία σκιαγράφηση της απόδειξης λόγω της ιδιαίτερης σημασίας που έχει το θεώρημα αυτό στην ανάπτυξη της Θεωρίας των Δακτυλίων.

Ορισμός 6

(a) Για κάθε ακέραιο αριθμό a ορίζουμε την ***απόλυτη τιμή*** *του $|a|$ να είναι ο παρακάτω φυσικός αριθμός:*

$$|a| = \begin{cases} a & \text{αν } a \geq 0 \\ -a & \text{αν } a < 0 \end{cases}$$

(a) Το ***πρόσημο*** $\operatorname{sign}(a)$ *ενός ακέραιου αριθμού $a \neq 0$ ορίζεται να είναι ο αριθμός $\frac{a}{|a|}$ ή ισοδύναμα:*

$$\operatorname{sign}(a) = \begin{cases} 1 & \text{αν } a > 0 \\ -1 & \text{αν } a < 0 \end{cases}$$

[2] Γιατί ταυτίζεται ο (2,0) με τον (1000,998); Γιατί 2+998=0+1000.

Θεώρημα 4 *[Ευκλείδης-Η ταυτότητα της διαίρεσης.]*
Αν a, b είναι δύο ακέραιοι αριθμοί με $a \neq 0$ τότε υπάρχουν δύο μοναδικού αριθμοί k, υ με το $0 \leq \upsilon < |a|$ ώστε

$$b = ka + \upsilon$$

Απόδειξη: Ας θεωρήσουμε το σύνολο

$$A = \{x \in \mathbb{Z} : b - xa \geq 0\}$$

Το σύνολο αυτό είναι μη κενό γιατί $x = -|b|\text{sign}(a) \in A$. Πράγματι, γιαυτό το x θα έχουμε ότι

$$\begin{aligned} b - xa &= b - (-|b|\text{sign}(a))a = \\ &= b + |b|\text{sign}(a))a = \\ &= b + |b||a| \geq \\ &\geq b + |b| \geq 0 \end{aligned}$$

Συνεπώς θα έχει ένα μικρότερο στοιχείο $\upsilon = b - ka$. Επαληθεύουμε ότι $0 \leq \upsilon < |a|$. Τη μοναδικότητα των υ, κ την αφήνουμε σαν άσκηση. □

Ορισμός 7
*Έστω a, b ακέραιοι αριθμοί με $a \neq 0$. Θα λέμε ότι ο a **διαιρεί** τον b αν υπάρχει ένας ακέραιος αριθμός d (απαραίτητα διαφορετικός από 0) με $b = ad$. Σε αυτή την περίπτωση θα γράφουμε $a|b$.*

Η σχέση $|$ που μπορούμε να τη δούμε σαν μια διμελή σχέση στο $\mathbb{Z} \setminus \{0\}$ είναι σχεδόν [3] μια σχέση διάταξης στο $\mathbb{Z} \setminus \{0\}$ συγκεκριμένα ικανοποιεί τα εξής:

$$\begin{aligned} &\text{Για κάθε } \ a \in \mathbb{Z} \setminus \{0\}, a|a \\ &\text{Αν } \ a|b \ \text{ και } \ b|a \ \text{ τότε } \ |a| = |b| \\ &\text{Αν } \ a|b \ \text{ και } \ b|c \ \text{ τότε } \ a|c \\ &\text{Αν } \ a|b \ \text{ και } \ b|c \ \text{ τότε } \ a|b + c \end{aligned}$$

Ορισμός 8
Έστω $a_1, a_2, \ldots a_k$ ακέραιοι αριθμοί που είναι όλοι διαφορετικοί από το 0.
*1. Ένας αριθμός $d > 0$ θα λέγεται **Μέγιστος Κοινός Διαιρέτης** των $a_1, \ldots, a_n$ και θα συμβολίζεται με $ΜΚΔ(a_1, \ldots a_n)$,ή απλούστερα $(a_1, \ldots, a_n)$, αν $d|a_1, \ldots, d|a_n$ και για οποιοδήποτε άλλο θετικό ακέραιο d' που έχει την ιδιότητα $d'|a_1, \ldots, d'|a_n$ ισχύει ότι $d'|d$.*

[3] Για να ήταν μία σχέση διάταξης θα έπρεπε να ικανοποιεί και την αντισυμμετρικότητα ($a|b$ και $b|a \Rightarrow a = b$). Αντί αυτού ικανοποιεί την ασθενέστερη ιδιότητα ($a|b$ και $b|a \Rightarrow |a| = |b|$). Για την ακρίβεια είναι σχέση διάταξης αν περιοριστεί στο σύνολο των αυστηρά θετικών ακέραιων.

2. Ένας αριθμός $m > 0$ θα λέγεται ***Ελάχιστο Κοινό Πολλαπλάσιο*** *των $a_1, \ldots, a_n$ και θα συμβολίζεται με ΕΚΠ$(a_1, \ldots a_n)$, αν $a_1|m, \ldots, a_n|m$ και για οποιοδήποτε άλλο θετικό ακέραιο m' που έχει την ιδιότητα $a_1|m', \ldots, a_n|m'$ ισχύει ότι $m|m'$.*

Είναι φανερό πως αν ο ΜΚΔ (και όμοια το ΕΚΠ) κάποιων αριθμών υπάρχει τότε είναι μοναδικό[4]. Θα περιοριστούμε στη μελέτη του Μέγιστου Κοινού Διαιρέτη, που μας ενδιαφέρει και πιο πολύ. Πριν αποδείξουμε πως υπάρχει δίνουμε μερικές ιδιότητες του:

Πρόταση 1
Έστω $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, τότε:
1. $(a_1, \ldots, a_n) = (|a_1|, \ldots, |a_n|)$.
2. $(a_1, a_2 \ldots, a_n) = (a_1, MK\Delta(a_2 \ldots, a_n))$.

Το πρώτο μέρος της πρότασης μας λέει ότι για να βρούμε το ΜΚΔ κάποιων αριθμών αρκεί να βρούμε τον ΜΚΔ των απόλυτων τιμών τους. Συνεπώς αν αποδείξουμε την ύπαρξη ΜΚΔ για οποιοδήποτε πλήθος μη μηδενικών θετικών ακεραίων το έχουμε δείξει και για οποιοδήποτε πλήθος ακέραιων. Το δεύτερο μας λέει ότι αν ξέρουμε ότι υπάρχει ο ΜΚΔ οποιωνδήποτε n αριθμών θα υπάρχει και για $n+1$ αριθμούς κοκ.

Συνδυάζοντας τα αυτά μαζί καταλήγουμε ότι αρκεί να δείξουμε ότι δύο οποιοιδήποτε θετικοί ακέραιοι έχουν μέγιστο κοινό διαιρέτη και να βρούμε και ένα τρόπο να τον υπολογίζουμε. Θα τα κάνουμε και τα δύο μαζί δίνοντας έναν περίφημο αλγόριθμο, που λέγεται Αλγόριθμος του Ευκλείδη και που περιγράφτηκε πρώτα (μαζί με άλλα σημαντικά Θεωρήματα της Θεωρίας Αριθμών) από τον Ευκλείδη στα «Στοιχεία» του.

Για να διευκολυνθούμε στους συλλογισμούς μας εισάγουμε την παρακάτω ορολογία:

Ορισμός 9
Έστω $a_1, \ldots, a_n$ ακέραιοι αριθμοί. Θα λέμε ότι ο c είναι ***ακέραιος συνδυασμός*** *των $a_1, \ldots, a_n$ αν υπάρχουν ακέραιοι αριθμοί $x_1, \ldots, x_n$ με $c = a_1x_1 + \cdots + a_nx_n$.*

Παρατηρείστε ότι:

Αν ένας ακέραιος d διαιρεί τους ακέραιους $a_1, \ldots, a_n$ τότε διαιρεί και οποιοδήποτε ακέραιο συνδυασμό τους.

Η έννοια αυτή έχει και ένα είδος μεταβατικότητας:

[4] Αν πχ υπήρχαν δύο Μέγιστοι Κοινοί διαιρέτες για κάποιους δοσμένους αριθμούς, ο ένας θα διαιρούσε τον άλλο και συνεπώς θα ήταν ίσοι μεταξύ τους.

Αν ο c είναι ακέραιος συνδυασμός των $a_1, \ldots, a_n$ και ο κάθε ένας από τούς a_i είναι ακέραιος συνδυασμός των $a'_1, \ldots, a'_n$ τότε και ο c θα είναι ακέραιος συνδυασμός των $a'_1, \ldots, a'_n$.

Ας ξεκινήσουμε τώρα με δύο αριθμούς a, b όπου $0 < a \leq b$ και ας ορίσουμε αναδρομικά μία ακολουθία $(x_n)_{n=1}^{\infty}$, από φυσικούς, ως εξής: [5], :

$$x_1 = b$$
$$x_2 = a$$
$$x_{n+2} = \begin{cases} \Upsilon(x_n, x_{n+1}) & \text{αν } x_{n+1} > 0 \\ 0 & \text{αν } x_{n+1} = 0 \end{cases}$$

Παρατηρείστε ότι αν $x_n > 0$ τότε $x_{n+1} < x_n$ και ότι αν $x_n = 0$ τότε -από τον ορισμό- $x_m = 0$ για κάθε $m > n$. Από την αρχή της καλής διάταξης (Θεώρημα 1, (β)) θα έχουμε ότι υπάρχει ένας αριθμός $n \geq 3$ με $x_n = 0$ και έστω n_0 ο μικρότερος τέτοιος αριθμός. Θέτουμε $d = x_{n_0-1}$.

Έχουμε δηλαδή την παρακάτω εικόνα:

$$b = ak_3 + x_3$$
$$a = x_3k_4 + x_4$$
$$x_3 = x_4k_5 + x_5$$
$$\ldots\ldots$$
$$x_{n_0-3} = x_{n_0-2}k_{n_0-1} + x_{n_0-1} = x_{n_0-2}k_{n_0-1} + d$$
$$x_{n_0-2} = x_{n_0-1}k_{n_0} = x_{n_0-1}d$$

Εξ ορισμού για κάθε $2 \leq n \leq n_0$ θα έχουμε ότι υπάρχει k_n ώστε

$$x_n = -k_nx_{n-1} + x_{n-2}$$

δηλαδή ο x_n είναι γραμμικός συνδυασμός των δύο προηγούμενών του x_{n-1}, x_{n-2}.

Παρατηρείστε τώρα ότι:

Αν ένας αριθμός y διαιρεί δύο διαδοχικά μη μηδενικά στοιχεία στοιχεία x_{n-1}, x_n της ακολουθίας (οπότε $n < n_0$) τότε αναγκαστικά θα διαιρεί και οποιοδήποτε στοιχείο x_m της ακολουθίας με $m < n$.

Επειδή $x_{n_0} = 0$, ο $d = x_{n_0-1} | x_{n_0-2}$ και φανερά διαιρεί τον εαυτό του. Από την προηγούμενη παρατήρηση θα διαιρεί κάθε προηγούμενό του άρα και τους $x_2 = a, x_1 = d$.

[5] Όπως έχουμε ήδη αναφέρει, ο $\Upsilon(b, a)$ συμβολίζει το υπόλοιπο της διαίρεσης του b με τον a.

Με άλλα λόγια ο

$$\text{Ο } d \text{ είναι κοινός διαιρέτης των } a, b. \qquad (*)$$

Ακολουθώντας την αντίστροφη πορεία, παρατηρείστε ότι:

Κάθε στοιχείο x_n της ακολουθίας σαν άκέραιος συνδυασμός των δύο προηγούμενών του θα γράφεται σαν ακέραιος συνδυασμός και των x_1, x_2 δηλαδή των a, b.

Με άλλα λόγια, θα υπάρχουν ακέραιοι x, y με

$$d = xa + yb \qquad (**)$$

Από το (**) θα έχουμε ότι οποιοσδήποτε κοινός διαιρέτης των a, b είναι διαιρέτης του d και δείχτηκε ότι ο d είναι ο μέγιστος κοινός διαιρέτης των a, b. Δείξαμε συνεπώς το:

Θεώρημα 5
Για οποιουσδήποτε μη μηδενικούς ακέραιους a, b υπάρχει ο μέγιστος κοινός διαιρέτης τους d. Επιπλέον ο d είναι ακέραιος συνδυασμός των a, b, δηλαδή υπάρχουν ακέραιοι x, y τέτοιοι ώστε

$$d = ax + by$$

Με επαγωγή μπορούμε να γενικεύσουμε ως εξής:

Θεώρημα 6
Για οποιουσδήποτε μη μηδενικούς ακέραιους $a_1, \ldots, a_n$ υπάρχει ο μέγιστος κοινός διαιρέτης τους d. Επιπλόν ο d είναι ακέραιος συνδυασμός τους, δηλαδή υπάρχουν ακέραιοι $x_1, \ldots, x_n$ τέτοιοι ώστε

$$d = a_1x_1 + \cdots + x_na_n$$

Ορισμός 10
Δύο ή περισσότεροι μη μηδενικοί ακέραιοι θα λέγονται ***πρώτοι μεταξύ τους*** *αν ο μέγιστος κοινός διαιρέτης τους είναι το 1.*

Η επόμενη έννοια είναι βασική.

Ορισμός 11
Ένας ακέραιος $n \neq 0$ θα λέγεται ***σύνθετος*** *αριθμός αν μπορεί να γραφτεί σαν $n = n_1n_2$ με $1 < n_1, n_2 < n$, με άλλα λόγια αν μπορεί να διαιρεθεί με κάποιον ακέραιο διαφορετικό από το 1 ή τον εαυτό του.*
Ένας θετικός ακέραιος $n \geq 2$ θα λέγεται ***πρώτος*** *αν δεν είναι σύνθετος.*

Παρατηρείστε ότι στον ορισμό του πρώτου αριθμού απαιτούμε να είναι μεγαλύτερος ή ίσος του 2 και ότι οι αριθμοί 0, 1 δεν κατατάσσονται ούτε στους πρώτους ούτε στους σύνθετους αριθμούς.

Θεώρημα 7 (Θεμελιώδες Θεώρημα της Αριθμητικής)

Αν $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι και p πρώτος αριθμός που διαιρεί το γινόμενό τους ab τότε θα διαιρεί έναν από αυτούς. Συμβολικά,
αν p πρώτος, $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ και $p|a_1 \ldots a_n$ τότε $p|a_1$ είτε...$p|a_n$.

Απόδειξη: Αρκεί να δείξουμε το Θεώρημα για $n = 2$ και μετά να εφαρμόσουμε επαγωγή. Ας υποθέσουμε λοιπόν ότι οι a, b είναι ακέραιοι μεγαλύτεροι ή ίσοι του 2 και ότι ο $p|ab$.

Έστω d να είναι ο μέγιστος κοινός διαιρέτης των a, p. Τότε $d = 1$ ή $d = p$, επειδή ο p είναι πρώτος και δεν έχει άλλους διαιρέτες. Αν $d = p$ καταλήγουμε στο ότι ο p διαιρεί τον a. Αν $d = 1$ θα υπάρχουν δύο ακέραιοι x, y με $1 = ax + py$ άρα $b = abx + pay$ και αφού ο p διαιρεί τον ab έχουμε άμεσα ότι διαιρεί τον b. Σε κάθε περίπτωση $p|a$ ή $p|b$. □

Από αυτό θα έχουμε το

Θεώρημα 8

Κάθε θετικός ακέραιος $a > 1$ θα γράφεται σαν ένα γινόμενο πρώτων αριθμών:

$$a = p_1 \ldots p_n \qquad (*)$$

*Επιπλέον η αναπαράσταση (*) θα είναι **μοναδική** με την εξής έννοια: Αν $a = q_1 \ldots q_m$, με $q_1 \ldots q_m$ πρώτους αριθμούς, τότε $m = n$ και μπορούμε να αλλάξουμε τη σειρά των $q_1, \ldots q_n$ σε $q'_1, \ldots q'_n$ ώστε να έχουμε $p_1 = q'_1, \ldots p_n = q'_n$* [6].

Απόδειξη: Το γεγονός ότι κάθε θετικός ακέραιος $a > 1$ γράφεται σαν γινόμενο πρώτων αποδεικνύεται εύκολα με επαγωγή. Για το 2 ισχύει αφού ο ίδιος είναι πρώτος. Ας υποθέσουμε ότι γνωρίζουμε ότι οι $2, \ldots, n$ αναλύονται σε γινόμενο πρώτων και ας εγετάσουμε τι συμβαίνει για τον $n + 1$. Είτε αυτός είναι πρώτος και έχουμε τελειώσει είτε δεν είναι και συνεπώς θα γράφεται σαν ένα γινόμενο $n + 1 = n_1 n_2$ με $2 \leq n_1, n_2 < n$. Ο καθένας από αυτούς τους αριθμούς θα είναι γινόμενο πρώτων (από την επαγωγική μας υπόθεση, $n_1 = p_1 \ldots p_k, n_2 = q_1 \ldots q_m$) άρα και ο $n + 1 = p_1 \ldots, p_k q_1 \ldots q_m$ θα είναι επίσης.

Για το μονοσήμαντο της αναπαράστασης παρατηρούμε το εξής. Ας υποθέσουμε ότι ο $n = p_1 \ldots p_n = q_1 \ldots q_m$ είχε δύο αναπαραστάσεις σε γινόμενο πρώτων τους οποίους έχουμε γράψει με αύξοντα τρόπο δηλαδή $p_1 \leq p_2 \ldots$, $q_1 \leq q_2 \ldots$ και επίσης ότι $n \leq m$. Ισχυριζόμαστε ότι $m = n$ και $p_i = q_i$ για κάθε $i = 1, \ldots n$. Πράγματι, αν αυτό που ισχυριζόμαστε δεν ίσχυε δύο περιπτώσεις θα μπορούσαν

[6] Με τον όρο «μπορούμε να αλλάξουμε τη σειρά» εννοούμε ότι μπορούμε να βρούμε μία μετάθεση (δηλαδή, μια 1-1 και επί απεικόνιση) $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ με $p_1 = q_{\pi(1)}, \ldots, q_n = q_{\pi(n)}$. Ένας άλλος ισοδύναμος τρόπος να μιλήσουμε για μοναδικότητα είναι να θεωρούμε ότι στην ανάλυση ενός αριθμού $a = q_1 \ldots p_m$ οι πρώτοι εμφανίζονται με αύξουσα σειρά, δηλαδή $p_1 \leq p_2 \leq \ldots$ και αυτό είναι που θα χρησιμοποιήσουμε στην απόδειξη. Η διατύπωση αυτή όμως δεν μπορεί να μεταφερθεί σε γενικούς δακτύλιους όπου δεν έχουμε κάποια σχέση ολικής διάταξης μεταξύ των στοιχείων τους.

να συμβαίνουν:
Είτε $p_i = q_i$ για κάθε $i = 1, \ldots, n$ και $n < m$, αλλά τότε θα καταλήγαμε ότι $1 = q_{n+1} \ldots q_m$ που είναι φανερά άτοπο.
Είτε θα υπάρχει κάποιο $1 \leq k \leq n$ με $p_k \neq q_k$. Τότε θα είχαμε $p_k \ldots p_n = q_k \ldots q_m$. Αν $p_k < q_k$ τότε το $p_k < q_i$ για όλα τα $i = k, k+1, \ldots, m$. Αλλά το $p_k | q_k \ldots q_m$ και συνεπώς θα υπάρχει κάποιο $i = k, k+1, \ldots, m$ με $p_k | q_i$. Επειδή όμως ο q_i είναι πρώτος θα είχαμε ότι $p_k = q_i$, άτοπο. Αν πάλι $q_k < p_k$ τότε $q_k < p_i$ για κάθε $i = k, \ldots, n$ αλλά $q_k | p_k \ldots p_n$ και πάλι θα έπρεπε να διαιρεί κάποιον από τους p_i με τον οποίο και θα ταυτιζόταν.

Καταλήξαμε πάλι σε άτοπο και το Θεώρημα αποδείχτηκε. □

Από το προηγούμενο θεώρημα θα έχουμε άμεσα το εξής:

Πρόταση και Ορισμός 1

(α) Κάθε θετικός ακέραιος $n \geq 2$ γράφεται κατά μοναδικό τρόπο στη μορφή:

$$n = p_1^{u_1} \ldots p_k^{u_k}$$

όπου οι $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί με $p_1 < \cdots < p_k$ και οι $u_1, \ldots, u_k$ ακέραιοι μεγαλύτεροι ή ίσοι του 1. Η παράσταση αυτή λέγεται η ***ανάλυση του n σε γινόμενο πρώτων.***
(β) Κάθε ακέραιος $n \neq 0, 1$ γράφεται κατά μοναδικό τρόπο στην μορφή:

$$n = \mathrm{sing}(a) p_1^{u_1} \ldots p_k^{u_k}$$

όπου οι $p_1, \ldots, p_k$ είναι πρώτοι αριθμοί με $p_1 < \cdots < p_k$, οι $u_1, \ldots, u_k$ ακέραιοι μεγαλύτεροι ή ίσοι του 1΄.

Θα τελειώσουμε αυτή την εισαγωγική παράγραφο ορίζοντας για κάθε αριθμό n μία πολύ χρήσιμη για τα παρακάτω σχέση ισοδυναμίας στο σύνολο $\mathbb{Z}$ των ακεραίων. Για να είναι ξεκάθαρο ως προς ποιο αριθμό n θεωρούμε τη σχέση ισοδυναμίας χρησιμοποιούμε τον κάπως ασυνήθιστο συμβολισμό $\cdots \equiv \ldots \pmod n$ για τη σχέση αυτή.

Ορισμός 12

Έστω n θετικός ακέραιος μεγαλύτερος ή ίσος του 2. Αν $a, b \in \mathbb{Z}$ θα γράφουμε ότι

$$a \equiv b \pmod n$$

αν και μόνο αν ο n διαιρεί τον $a - b$.

Η σχέση αυτή είναι μία σχέση ισοδυναμίας στους ακέραιους. Αυτήν και άλλες στοιχειώδεις ιδιότητες της σχέσης αυτής συνοψίζουμε στην επόμενη πρόταση:

Πρόταση 2

Έστω n θετικός ακέραιος μεγαλύτερος ή ίσος του 2 και $a, b, c, a', b', c' \in \mathbb{Z}$. Τότε:

1. $a \equiv a \pmod{n}$.
2. Αν $a \equiv b \pmod{n}$ *τότε* $b \equiv a \pmod{n}$.
3. Αν $a \equiv b \pmod{n}$ *και* $b \equiv c \pmod{n}$ *τότε* $a \equiv c \pmod{n}$.
4. Αν $a \equiv a' \pmod{n}$ *και* $b \equiv b' \pmod{n}$ *τότε* $a + b \equiv a' + b' \pmod{n}$
5. Αν $a \equiv a' \pmod{n}$ *και* $b \equiv b' \pmod{n}$ *τότε* $ab \equiv a'b' \pmod{n}$
6. Για κάθε $a \in \mathbb{Z}$ *υπάρχει μοναδικός* $j \in \{0, 1, \ldots, n-1\}$ *με* $j \equiv a \pmod{n}$.

Απόδειξη: Ας δείξουμε το (5). Αν Αν $a \equiv a' \pmod{n}$ και $b \equiv b' \pmod{n}$ τότε για κάποια $k, l \in \mathbb{Z}$ θα έχουμε ότι $a = kn + a'$,$b = ln + b'$, άρα $ab = (kln + kb' + la')n + a'b'$, δηλαδή $ab \equiv a'b' \pmod{n}$. Το (6) είναι άμεση συνέπεια της ταυτότητας της διαίρεσης (Θεώρημα 4).
Η απόδειξη των υπολοίπων αφήνεται στον αναγνώστη. □

1.1.1 Ασκήσεις

Ασκηση 1 *Αποδείξτε ότι* $2 \cdot 2 = 2 + 2 = 4$

Ασκηση 2 *Δείξτε ότι για οποιουσδήποτε φυσικούς αριθμούς a, b, c ισχύει:*
(1) $a + (b + c) = (a + b) + c$
(2) $a + b = b + a$
(3) $a(bc) = (ab)c$
(4) $ab = ba$

Ασκηση 3 *Δείξτε ότι για οποιουσδήποτε ακέραιους αριθμούς a, b, c ισχύει:*
(1) $a + (b + c) = (a + b) + c$
(2) $a + b = b + a$
(3) $a(bc) = (ab)c$
(4) $ab = ba$

Ασκηση 4 *Να αποδείξετε την μοναδικότητα των k, υ στο Θεώρημα 44*

Ασκηση 5 *Να βρείτε το μεγιστο κοινό διαιρέτη (a, b) των a, b και να τον εκφράσετε στη μορφή $xa + yb$ αν*
(1) $a = 198, b = 21$
(2) $a = -198, b = 21$
(3) $a = 17891, b = 23440$
(4) $a = -72, b = 26$

Ασκηση 6 *Να βρείτε το ανάπτυγμα σε γινόμενο πρώτων των αριθμών* $21, 270, 5040, 3467$.

Ασκηση 7 *Να δείξετε ότι ένας φυσικός αριθμός n είναι πρώτος αν και μόνο αν δεν διαιρείται από κανέναν πρώτο $p \leq \sqrt{n}$.*

Ασκηση 8 *Να δείξετε ότι αν m, n είναι μη μηδενικοί ακέραιοι τότε $(m, n) = (|m|, |n|)$.*

Ασκηση 9 *Να δείξετε ότι αν $(m, n) = 1$ και $k \in \mathbb{Z}\backslash\{0\}$ τότε $(km, kn) = |k|(m, n)$.*

Ασκηση 10 *Έστω n θετικός ακέραιος. Δείξτε ότι αν ένας πρώτος p διαιρεί τον $n! + 1$ τότε $p > n$.*

Ασκηση 11 *Να δείξετε ότι υπάρχουν άπειροι πρώτοι αριθμοί. Ένας τρόπος είναι να χρησιμοποιήσετε την προηγούμενη άσκηση κατάλληλα για να δείξετε ότι για κάθε n υπάρχει πρώτος $p > n$.*

Ασκηση 12 *Να δείξετε ότι αν p είναι πρώτος τότε είτε $p \equiv 3 \pmod 4$ είτε $p \equiv 1 \pmod 4$.*

Ασκηση 13 *Να δείξετε ότι υπάρχουν άπειροι πρώτοι της μορφής $4n + 3$.*

Ασκηση 14 *Να δείξετε ότι αν p είναι πρώτος τότε είτε $p \equiv 1 \pmod 6$ είτε $p \equiv 5 \pmod 6$.*

Ασκηση 15 *Να δείξετε ότι υπάρχουν άπειροι πρώτοι της μορφής $6n + 5$.*

Ασκηση 16 *Να δείξετε ότι αν n είναι θετικός ακέραιος μεγαλύτερος από 1 και $n|(n-1)! + 1$ τότε ο n είναι πρώτος αριθμός.*

Ασκηση 17 *Να δείξετε ότι αν $m|ab$ και $(m, a) = 1$ τότε $m|b$.*

Ασκηση 18 *Να δείξετε ότι αν $(m, n) = 1$ τότε*

$$(mn, a) = 1 \text{ αν και μόνο αν } (m, a) = 1 \text{ και } (n, a) = 1.$$

Ασκηση 19 *Να δείξετε ότι το ελάχιστο κοινό πολλαπλάσιο δύο θετικών ακεραίων m, n είναι ίσο με $\dfrac{mn}{(m, n)}$.*

1.2 Διμελείς Πράξεις. Παραδείγματα Αλγεβρικών Δομών.

Μια **διμελής πράξη** ή απλά μια **πράξη** σε ένα σύνολο X είναι μία συνάρτηση $f : X \times X \to X$, με άλλα λόγια ένας κανόνας f μέσω του οποίου σε οποιοδήποτε ζευγάρι (x, y) από στοιχεία του συνόλου X αντιστοιχούμε ένα τρίτο που το συμβολίζουμε με $f(x, y)$. Συνήθως η συνάρτηση f συμβολίζεται με σύμβολα όπως $+, \cdot, *$ και γράφουμε $x + y$ αντί $+(x, y)$.

Μια **αλγεβρική δομή** αποτελείται από ένα σύνολο X και κάποιες πράξεις που έχουν οριστεί σε αυτό. Ένας από τους σκοπούς της άλγεβρας είναι να κατατάξει και να μελετήσει τις αλγεβρικές δομές ανάλογα με γενικές ιδιότητες που μπορεί να έχουν οι πράξεις. Σαν παράδειγμα αναφέρουμε την πρόσθεση ακέραιων αριθμών, την πρόσθεση διανυσμάτων την πρόσθεση συναρτήσεων. Αν και είναι εντελώς διαφορετικές πράξεις σε διαφορετικά σύνολα μοιράζονται κάποιες κοινές ιδιότητες όπως η προσεταιριστικότητα , η ύπαρξη ουδέτερου στοιχείου κλπ...Είναι συνεπώς χρήσιμο να γνωρίζουμε τι συμπεράσματα μπορεί να προκύψουν με μόνη πληροφορία ιδιότητες της πράξης και ας μη γνωρίζουμε την ίδια την πράξη ώστε να μη χρειάζεται να αποδεικνύουμε σε κάθε ξεχωριστή αλγεβρική δομή τα ίδια πράγματα. Θα ξεκινήσουμε τη κατάταξη των αλγεβρικών δομών από τις πιο απλές (και πιο γενικές) προς τις πιο σύνθετες με κύρια αναφορά στην έννοια του δακτυλίου που θα ορίσουμε λίγο παρακάτω.

Ορισμός 13

Ημιομάδα *είναι ένα σύνολο X στο οποίο έχει οριστεί μία διμελής προσεταιριστική πράξη $*$, με άλλα λόγια έχει οριστεί μία συνάρτηση $* : X \times X \to X$ ώστε για οποιαδήποτε $x, y, z \in X$ ισχύει:*

(1) $$x * (y * z) = (x * y) * z.$$

Αν συμβαίνει να υπάρχει κάποιο στοιχείο e με την ιδιότητα $x * e = e * x = x$, για οποιοδήποτε $x \in X$, το e λέγεται ***ουδέτερο στοιχείο*** *για την ημιομάδα.*

Επίσης, αν συμβαίνει για κάποια $x, y \in X$, $x * y = y * x$ θα λέμε ότι τα δύο αυτά στοιχεία x, y ***αντιμετατίθενται****.*

Τέλος αν οποιαδήποτε δύο στοιχεία της ημιομάδας αντιμετατίθενται θα λέμε ότι η ημιομάδα είναι ***αντιμεταθετική***[7]*.*

Ένα παράδειγμα αντιμεταθετικής ημιομάδας με ουδέτερο στοιχείο είναι το σύνολο των φυσικών αριθμών με την πράξη της πρόσθεσης.
Ένα άλλο παράδειγμα ημιομάδας (μη αντιμεταθετικής) είναι το σύνολο X^X όλων των συναρτήσεων $f : X \to X$ από ένα σύνολο X στον εαυτό του με την πράξη της σύνθεσης συναρτήσεων.

Ορισμός 14

[7] Χρησιμοποιείται και ο όρος **αβελιανή**

Ομάδα *είναι ένα σύνολο X στο οποίο έχει οριστεί μία διμελής πράξη $*$ που έχει τις παρακάτω ιδιότητες:*

$$\text{Για οποιαδήποτε } x,y,z \in X, x*(y*z) = (x*y)*z \quad (1)$$
$$\text{Υπάρχει } e \in X \text{ ώστε για κάθε } x \in X, \text{ ισχύει } x*e = e*x = x \quad (2)$$
$$\text{Για κάθε } x \in X \text{ υπάρχει (μοναδικό) } y \in X, \text{ ώστε } x*y = y*x = e \quad (3)$$

Το στοιχείο e στην παραπάνω εξίσωση (2) είναι μοναδικό και λέγεται ***ουδέτερο*** *στοιχείο της πράξης.*
Επίσης το στοιχείο y στην παραπάνω εξίσωση (3) είναι μοναδικό για δοσμένο x, λέγεται δε ***αντίστροφο στοιχείο του*** *x.*

Παραδείγματα ομάδων είναι τα σύνολα $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ των ακεραίων, ρητών, πραγματικών αριθμών αντίστοιχα με την πράξη της πρόσθεσης. Ένα άλλο παράδειγμα ομάδας (μη αντιμεταθετικής) είναι το σύνολο X^X όλων των συναρτήσεων $f : X \to X$ από ένα σύνολο X στον εαυτό του που είναι 1-1 και επί, με την πράξη της σύνθεσης συναρτήσεων. Εδώ το ουδέτερο στοιχείο είναι η ταυτοτική απεικόνιση και το αντίστροφο στοιχείο μίας συνάρτησης $f : X \to X$ είναι η αντίστροφη συνάρτηση $f^{-1} : X \to X$.

Αν $*$ είναι μια πράξη ορισμένη σε ένα σύνολο X, ένα υποσύνολο A του X λέγεται **κλειστό** ώς προς την πράξη αυτή αν για οποιαδήποτε $a, b \in A$ συμβαίνει $a * b \in A$. Σε αυτή την περίπτωση μπορούμε να ορίσουμε μία πράξη $*$ στο A που είναι ο περιορισμός της αρχικής πράξης στο A. Αν το ζευγάρι $(X, *)$ έχει δομή ημιομάδας (αντίστοιχα, ομάδας) τότε ένα μη-κενό υποσύνολο A του X θα λέγεται **υπο-ημιομάδα** (αντίστοιχα **υπο-ομάδα**) αν είναι κλειστό ως προς την πράξη και το $(A, *)$ έχει δομή ημιομάδας (αντίστοιχα, ομάδας).

Παρατηρούμε ότι για να είναι ένα μη-κενό υποσύνολο A μιας ημιοομάδας υποημιομάδα πρέπει και αρκεί να είναι κλειστό ως προς την πράξη. Αυτό δεν είναι αρκετό όμως στην περίπτωση των ομάδων. Θυμίζουμε ότι σε αυτή την περίπτωση ένα μη-κενό υποσύνολο A μιας ομάδας είναι υποομάδα αν και μόνο αν για κάθε $a, b \in A$ τα $a + b, -a, -b \in A$. Ανάλογες έννοιες υπο-δομών (υπο-δακτύλιοι, υπο-σώματα κλπ) θα οριστούν παρακάτω.

1.3 Η έννοια του δακτυλίου. Ορισμός, μερικές βασικές ιδιότητες και παραδείγματα. Η έννοια του υπο-δακτύλιου.

Η επόμενη δομή που θα ορίσουμε έχει δύο πράξεις και είναι αυτή που θα αποτελέσει το κύριο αντικείμενο της μελέτης μας.

Ορισμός 15

Δακτύλιος[8] *είναι ένα σύνολο* R *στο οποίο έχουν οριστεί δύο διμελείς πράξεις* $+, \cdot$ *που έχει τις παρακάτω ιδιότητες:*

$$\begin{aligned}
&\text{Το } (R,+) \text{ είναι αντιμεταθετική ομάδα με ουδέτερο στοιχείο το } 0 && (1)\\
&\text{Το } (R,\cdot) \text{ είναι ημιομάδα} && (2)\\
&\text{Η πράξη } \cdot \text{ είναι επιμεριστική ως προς την } + \text{ δηλαδή}\\
&\text{για οποιαδήποτε } x,y,z \in R \text{ ισχύει}\\
&x\cdot(y+z) = (x\cdot y)+(x\cdot z) && (3)\\
&(x+y)\cdot z = (x\cdot y)+(x\cdot z) && (4)
\end{aligned}$$

Ορισμός 16
Θα ονομάζουμε ένα δακτύλιο $(R,+,\cdot)$*:*
(α) ***Μη-τετριμμένο****, αν έχει τουλάχιστον δύο στοιχεία.*

(β) ***Αντιμεταθετικό****, αν δύο οποιαδήποτε στοιχεία του* a, b *αντιμετατίθενται ως προς την* $\cdot$*, δηλαδή* $ab = ba$*.*

(γ) ***Δακτύλιο με μονάδα****, αν η ημιομάδα* $(R,\cdot)$ *έχει ουδέτερο στοιχείο, δηλαδή υπάρχει ένα* $1_R \in R$ *με την ιδιότητα για οποιοδήποτε* $a \in R$ *να συμβαίνει* $1_R a = a1_R = a$*.*

(δ) Αν $(R,+,\cdot)$ *είναι δακτύλιος με μονάδα* 1_R*, θα ονομάζουμε ένα στοιχείο του* a ***αντιστρέψιμο*** *αν υπάρχει κάποιο* $b \in R$ *με* $ab = ba = 1$*.*

Οι πράξεις $+, \cdot$ που ορίζουμε σε ένα δακτύλιο συμβολίζουν αφηρημένες πράξεις και όχι τις συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού. Ωστόσο θα ονομάζουμε συχνά την «$+$» πρόσθεση και την «$\cdot$» πολλαπλασιασμό.
Το ουδέτερο στοιχείο της $(R,+)$ συμβολίζεται με 0 και το αντίστροφο ενός στοιχείου x ως προς την πράξη $+$ με $-x$. Επίσης θα γράφουμε $x-y$ αντί του $x+(-y)$.
Ένας πολύ χρήσιμος συμβολισμός είναι ο παρακάτω :

Ορισμός 17 *Αν* A, B *είναι δύο οποιαδήποτε μη κενά υποσύνολα ενός δακτυλίου* R *θα συμβολίζουμε*

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

$$A\cdot B = \{a\cdot b : a \in A \text{ και } b \in B\}$$

$$A-B = \{a-b : a \in A \text{ και } b \in B\}$$

[8] Αγγλικά Ring

Ο παραπάνω ορισμός εισάγει δύο πράξεις στο σύνολο 2^R όλων των υποσυνόλων ενός δακτυλίου R. Πρέπει να παρατηρήσουμε ότι το 2^R δεν είναι δακτύλιος με αυτές τις πράξεις, αφού για παράδειγμα το $(2^R, +)$ απέχει πολύ από το να είναι ομάδα. Παρατηρείστε ωστόσο ότι θα έχουμε πάντοτε $A + B = B + A$ γιατί η πράξη $+$ είναι αντιμεταθετική σε κάθε δακτύλιο, όχι όμως απαραίτητα $A \cdot B = B \cdot A$, εκτός και αν ο δακτύλιος είναι αντιμεταθετικός.

Παράδειγμα 1 *Αν με* $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ *συμβολίσουμε τα σύνολα των ακεραίων, ρητών, πραγματικών, μιγαδικών αριθμών, αντίστοιχα, με τις συνηθισμένες πράξεις, αυτά αποτελούν παραδείγματα δακτυλίων. Ειδικά αυτά είναι και παραδείγματα αντιμεταθετικών δακτυλίων με μονάδα.*

Παράδειγμα 2 *Έστω X ένα οποιοδήποτε μη κενό σύνολο και R το σύνολο όλων των υποσυνόλων του. Στο R ορίζουμε δύο πράξεις:*

$$A + B = (A \cup B) \setminus (A \cap B)$$
$$A \cdot B = A \cap B$$

Τότε το $(R, +, \cdot)$ είναι δακτύλιος[9].

Παράδειγμα 3 *Έστω k ένας θετικός ακέραιος ≥ 2. Στο σύνολο $\mathbb{Z}$ όλων των ακεραίων ορίζουμε μία σχέση ισοδυναμίας*[10] *ως εξής:*

$$a \equiv b \pmod{k} \text{ αν και μόνο αν ο } k \text{ διαιρεί τον } a - b \tag{1.1}$$

Θέτουμε

$$\mathbb{Z}_k = \{0, 1, \ldots, k-1\} \tag{1.2}$$

Δεν είναι δύσκολο να δείξουμε ότι η παραπάνω διμελής σχέση είναι πράξη ισοδυναμίας και ότι για κάθε ακέραιο $a \in \mathbb{Z}$ υπάρχει ένας μοναδικός $j(a) \in \mathbb{Z}_k$ ώστε να συμβαίνει $a \equiv j(a) \pmod{k}$. Συγκεκριμένα ο $j(a)$ είναι το υπόλοιπο της διαίρεσης του a με k.

Στο σύνολο $\mathbb{Z}_k$ ορίζουμε δύο πράξεις $+, \cdot$ όπου

Αν $a, b \in \mathbb{Z}_k$ τότε
$a + b = j(a + b)$
$a \cdot b = j(ab)$

Οι πράξεις στο δεύτερο μέλος των παραπάνω εξισώσεων εννοείται ότι είναι οι συνήθεις πράξεις στο $\mathbb{Z}$. Για εξάσκηση γράφουμε τον πίνακα των πράξεων στο $\mathbb{Z}_6$ και αφήνουμε μερικά κενά να τα συμπληρώσει ο αναγνώστης.

[9] Το $A + B$ συμβολίζεται συνήθως με $A \triangle B$ και ονομάζεται **συμμετρική διαφορά** των δύο συνόλων A, B

[10] Μελετείστε την παράγραφο 1 και ειδικότερα την Πρόταση 2.

$a+\beta$	0	1	2	3	4	5
0	0	1	2	3		
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4						3
5				2		4

$a\cdot\beta$	0	1	2	3	4	5
0	0	0	0		0	
1	0	1	2	3	4	
2	0	2	4	0		4
3	0	3	0	3	0	3
4	0			0	4	2
5	0	5	4		2	

Παράδειγμα 4 *Έστω $(R,+,\cdot)$ ένας δακτύλιος, X ένα οποιοδήποτε μη κενό σύνολο και R^X το σύνολο όλων των απεικονίσεων από το X στο R. Για οποιαδήποτε $f,g\in R^X$ ορίζουμε δύο στοιχεία (συναρτήσεις) $f+g, f\cdot g\in R^X$ με*

$$\begin{aligned} f+g(x) &= f(x)+g(x)\\ f\cdot g(x) &= f(x)\cdot g(x)\end{aligned}$$

Το $(R^X,+,\cdot)$ είναι δακτύλιος.

Παράδειγμα 5 *Έστω $(R,+,\cdot)$ ένας δακτύλιος, n ένας θετικός ακέραιος και έστω $I_n=\{1,\dots,n\}$. Με $M_n(R)$ θα συμβολίζουμε το σύνολο όλων των απεικονίσεων $f: I_n\times I_n\to R$. Τα στοιχεία του $M_n(R)$ θα τα ονομάζουμε $n\times n-$* ***πίνακες με στοιχεία από το δακτύλιο*** *R.*

Συνήθως γράφουμε a_{ij} αντί του $f(i,j)$ και αντί της συνάρτησης f γράφουμε (a_{ij}) ή και όλο τον πίνακα των στοιχείων. Έτσι για παράδειγμα ο πίνακας

$$\begin{bmatrix} 0 & 1 & 3 & 0\\ 1 & 1 & 5 & 2\\ 2 & 1 & 1 & 1\\ 3 & 2 & 3 & 4\end{bmatrix}$$

παριστάνει το παρακάτω στοιχείο f του $M_4(\mathbb{Z}_5)$: $f(1,1)=a_{11}=0, f(1,2)=1, f(1,3)=3, f(1,4)=0, f(2,1)=1,\dots$.

Για να κάνουμε το συνολο $M_n(R)$ δακτύλιο ορίζουμε τις παρακάτω πράξεις:

$$(f+g)(i,j)=f(i,j)+g(i,j) \tag{1.3}$$

$$(f\cdot g)(i,j)=\sum_{k=1}^{n} f(i,k)g(k,j) \tag{1.4}$$

Το ουδέτερο στοιχείο για την πρόσθεση είναι η συνάρτηση που είναι ίση με 0 για κάθε $(i,j)\in I_n\times I_n$ ή με άλλα λόγια ο πίνακας που όλα τα στοιχεία του είναι ίσα με 0. Σημειώνουμε ότι ο $M_n(R)$ δεν είναι απαραίτητα αντιμεταθετικός δακτύλιος ακόμα και αν ο R είναι. Αν ο R έχει μονάδα τότε και ο $M_n(R)$ θα έχει. Είναι ο πίνακας I, *με*

$$\mathrm{I}(i,j)=\begin{cases}1 & \text{αν } i=j\\ 0 & \text{αν } i\neq j\end{cases}$$

Γενικά ο $M_n(R)$ δεν είναι αντιμεταθετικός δακτύλιος ακόμα και αν ο R είναι. Ένα τέτοιο παράδειγμα είναι οι 2×2 πίνακες στο $\mathbb{R}$.

Θα χρησιμοποιούμε συχνά και τον παρακάτω συμβολισμό. Αν $a_1, \ldots, a_n \in R$ θέτουμε

$$\sum_{i=0}^{n} a_i = a_1 + \cdots + a_n, \ \prod_{i=0}^{n} a_i = a_1 \cdot \cdots \cdot a_n$$

Σημειώστε ότι λόγω της προσεταιριστικότητας των πράξεων $+$ δεν απαιτείται η χρήση παρενθέσεων στο δεύτερο μέλος των παραπάνω σχέσεων.

Ορισμός 18 *Αν $n \in \mathbb{Z}$ και $a \in R$ θέτουμε*

$$na = \begin{cases} a + \cdots + a \ (n - \varphi o \rho \acute{\varepsilon} \varsigma) & \alpha \nu \ n > 0 \\ 0 & \alpha \nu \ n = 0 \\ (-a) + \cdots + (-a) \ (n - \varphi o \rho \acute{\varepsilon} \varsigma) & \alpha \nu \ n < 0 \end{cases}$$

Αν $n > 0$ τότε ορίζουμε

$$a^n = a \cdot a \cdot a \cdot \cdots a, \quad n - \varphi o \rho \acute{\varepsilon} \varsigma$$

Οι βασικές ιδιότητες των δακτυλίων συνοψίζονται στην παρακάτω πρόταση:

Πρόταση 3 *Έστω R ένας δακτύλιος n, m φυσικοί αριθμοί και a, b, c στοιχεία του R. Τότε:*

(1) $0a = a0 = 0$.

(2) $a(-b) = (-a)b = -(ab)$.

(3) $(-a)(-b) = ab$.

(4) $(\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} b_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$

(5) $n(ab) = (na)b = a(nb)$.

(6) $(a+b)^2 = a^2 + ab + ba + b^2$.

(7) $(n+m)a = na + ma$

(8) $a^{n+m} = a^n \cdot a^m$.

(9) Αν ο δακτύλιος έχει μονάδα και παραπάνω από ένα στοιχεία τότε θα έχουμε ότι $1 \neq 0$.

(10) Αν ο R είναι δακτύλιος με μονάδα και το a είναι αντιστρέψιμο τότε υπάρχει μοναδικό b με $ab = ba = 1$. Το b θα ονομάζεται ***αντίστροφο στοιχείο*** *του a και θα συμβολίζεται συχνά με a^{-1}.*

Απόδειξη:
1. $a0 = a(0+0) = a0 + a0$ συνεπώς $a0 = a0 + a0$ και επειδή το $(R, +)$ είναι ομάδα θα έχουμε $a0 = 0$. Όμοια, $0a = 0$.

2. Από το (1) $a0 = a(b + (-b)) = ab + a(-b) = 0$, συνεπώς $a(-b) = -(ab)$. Παρόμοια δείχνουμε ότι $(-a)b = -(ab)$.

3. $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

4. Θεωρούμε ένα m σταθερό και εφαρμόζουμε επαγωγή στο n. Για $n = 1$ η σχέση (4) είναι η

$$(a_1 + \cdots + a_m)b_m = a_1b_1 + \cdots + a_mb_1$$

και ισχύει λόγω της επιμεριστικής ιδιότητας του πολλαπλασιασμού ως προς την πρόσθεση.

Ας υποθέσουμε τώρα ότι γνωρίζουμε την ισχύ της σχέσης για δοσμένα m, n, δηλαδή για οποιαδήποτε $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$ γνωρίζουμε ότι ισχύει

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_ib_j \qquad (*)$$

Τότε

$$\begin{aligned}
\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n+1} b_j\right) &= \\
&= \left(\sum_{i=1}^{m} a_i\right)\left(\left(\sum_{j=1}^{n} b_j\right) + b_{n+1}\right) = \\
(\text{επιμεριστικότητα}) &= \left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) + \left(\sum_{i=1}^{m} a_i\right) b_{n+1} = \\
(\text{από επαγωγική υπόθεση } (*)\ ) &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_ib_j + \sum_{i=1}^{m} a_ib_{n+1} = \\
&= \sum_{i=1}^{m}\sum_{j=1}^{n+1} a_ib_j
\end{aligned}$$

5. Από (4), $ab + \cdots + ab = (a + \cdots + a)b$.
6. Από (4). Όμοια και τα (7), (8).
9. Αν $a \neq 0$ τότε $1a = a$ άρα $1 \neq 0$.
10. Ας υποθέσουμε ότι για το a υπάρχει ένα στοιχείο b με $ab = ba = 1_R$. Τότε αν για κάποια x, y συμβαίνει $ax = ay$ θα έχουμε ότι $bax = bay$ άρα και $x = y$. Αυτό δείχνει και τη μοναδικότητα του αντιστρόφου, αφού αν υπήρχε κάποιο b' με

$ab' = 1_R$, τότε $ab = ab'$ και από την προηγούμενη παρατήρηση θα είχαμε πως $b = b'$. □

Θα μπορούσε κάποιος να αναρωτηθεί αν η έννοια του δακτυλίου μπορεί να γενικευτεί αφαιρώντας την απαίτηση ο δακτύλιος να είναι αβελιανή ομάδα ως προς την πρόσθεση αλλά απλά μια ομάδα. Ωστόσο, αν ο δακτύλιος έχει μονάδα, η ίδια η επιμεριστικότητα των πράξεων απαιτεί την αντιμεταθετικότητα της πρόσθεσης. Πράγματι,ας υποθέσουμε ότι ισχύουν όλα τα αξιώματα του δακτυλίου εκτός από το «$a + b = b + a$» και ας πάρουμε δύο οποιαδήποτε στοιχεία a, b ενός δακτυλίου με μονάδα. Τότε

$$(a + b)(1 + 1) = (a + b)1 + (a + b)1 = a + b + a + b$$

αλλά και

$$(a + b)(1 + 1) = a(1 + 1) + b(1 + 1) = a + a + b + b$$

και εξισώνοντας θα έχουμε ότι

$$a + b = b + a$$

Αντίστοιχη έννοια με αυτή της υπο-ομάδας είναι αυτή του υπο-δακτυλίου.

Ορισμός 19 *Ένα μη κενό υποσύνολο A ενός δακτυλίου θα λέγεται* **υποδακτύλιος** *του R αν είναι δακτύλιος με τον περιορισμό των πράξεων σε αυτό.*

Σχεδόν άμεσο από τον ορισμό είναι το εξής:

Πρόταση 4 *Ένα μη κενό υποσύνολο A ενός δακτυλίου είναι υποδακτύλιος του R αν και μόνο αν ισχύουν τα εξής:*
1. Το A είναι κλειστό ως προς τις διαφορές δηλαδή αν $a, b \in A$ τότε $a - b = a + (-b) \in A$.
2. Το A είναι κλειστό ως προς τα γινόμενα, δηλαδή αν $a, b \in A$ τότε $ab \in A$.

Απόδειξη: Ας υποθέσουμε ότι ισχύουν τα (1), (2). Τότε θεωρώ $a \in A$ (αφού έχω υποθέσει ότι το A είναι μη κενό σύνολο). Λόγω του (1), $0 = a - a \in A$.
Επίσης αν $a \in A$ τότε αφού $0 \in A$, $0 - a = -a \in A$.
Τέλος αν $a, b \in A$ τότε $-b \in A$ και συνεπώς $a + b = a - (-b) \in A$ και $ab \in A$.
Άρα το $(A, +, \cdot)$ είναι δακτύλιος.

Αντίστροφα, αν υποθέσουμε ότι το $(A, +, \cdot)$ είναι δακτύλιος τότε το $(A, +)$ θα είναι ομάδα. Αν e είναι το ουδέτερο στοιχείο της ομάδας αυτής θα έχουμε $e+e = e$ και συνεπώς $e = 0$. Αυτό όμως σημαίνει ότι το $-a$ θα είναι το αντίστροφο στοιχείο του a στην $(A, +)$ και συνεπώς $-a \in A$. Επειδή από την υπόθεσή μας το $(A, +, \cdot)$ είναι δακτύλιος θα έχουμε ότι το A είναι κλειστό ως προς τις πράξεις και συνεπώς αν $a, b \in R$ θα έχουμε $ab \in R$, $a + (-b) \in R$ και δείξαμε ότι ικανοποιούνται οι (1), (2). □

Ας υποθέσουμε ότι $\mathcal{A}$ είναι ένα σύνολο από υποσύνολα ενός συνόλου R. Η **τομή** $\bigcap \mathcal{A}$ όλων των στοιχείων του $\mathcal{A}$ ορίζεται σαν το σύνολο όλων των στοιχείων του R που ανήκουν σε κάθε στοιχείο του $\mathcal{A}$,

$$x \in \bigcap \mathcal{A} \;\Leftrightarrow\; \forall A \in \mathcal{A}, x \in A$$

και συμβολίζεται με $\bigcap \mathcal{A}$.
Παρατηρείστε ότι αν το $\mathcal{A}$ περιέχει πεπερασμένο πλήθος στοιχείων πχ $\mathcal{A} = \{A_1, \ldots, A_n\}$ τότε το $\bigcap \mathcal{A} = A_1 \cap \cdots \cap A_n$. Ο συμβολισμός αυτός εισάγεται για να ορίσουμε την τομή «οποιουδήποτε πλήθους συνόλων». Γράφουμε επίσης και $\bigcap\{A : A \in \mathcal{A}\}$ αντί $\bigcap \mathcal{A}$.

Ένας ισοδύναμος τρόπος να βλέπουμε μια συλλογή από υποσύνολα ενός συνόλου R είναι σαν μια *οικογένεια* $(A_i)_{i\in I}$ από υποσύνολα του R δηλαδή σαν μία συνάρτηση που σε κάθε στοιχείο ενός δοσμένου συνόλου I αντιστοιχεί ένα σύνολο A_i.
Με αυτό τον συμβολισμό η τομή των στοιχείων της οικογένειας είναι το σύνολο:

$$\bigcap_{i\in I} A_i = \{x : \text{για κάθε } i,\ x \in A_i\}$$

Ειδικά αν το σύνολο δεικτών I είναι το σύνολο των φυσικών η οικογένεια συμβολίζεται και με $(A_i)_{i=1}^{\infty}$ και η τομή της με $\bigcap_{i=1}^{\infty} A_i$.

Πρόταση 5 *1. Η τομή ενός οποιουδήποτε μη κενού συνόλου υποδακτυλίων ενός δακτυλίου είναι υποδακτύλιος.*
2. Για κάθε υποσύνολο A ενός δακτυλίου R υπάρχει ένας ελάχιστος υποδακτύλιος $\langle A\rangle$ του R που περιέχει το A. Δηλαδή ο $\langle A\rangle$ είναι υποδακτύλιος του R, $A \subseteq \langle A\rangle$ και αν R' είναι ένας οποιοσδήποτε υποδακτύλιος του R με $A \subseteq R'$ θα έχουμε ότι $\langle A\rangle \subseteq R'$.

Απόδειξη: Ας υποθέσουμε ότι $\mathcal{A}$ είναι ένα σύνολο υποδακτυλίων. Το $\bigcap \mathcal{A}$ είναι μη κενό αφού περιέχει το 0. Αν $a, b \in \bigcap \mathcal{A}$ τότε $a, b \in S$ για κάθε $S \in \mathcal{A}$ και αφού κάθε στοιχείο S της $\mathcal{A}$ είναι υποδακτύλιος θα έχουμε ότι για κάθε $S \in \mathcal{A}$ $a - b, ab \in S$ άρα $a - b, ab \in \bigcap \mathcal{A}$ και το $\bigcap \mathcal{A}$ θα είναι υποδακτύλιος λόγω της Πρότασης 4.
2. Ας υποθέσουμε ότι $\mathcal{A}$ είναι το σύνολο όλων των υποδακτύλιων του R που περιέχουν το A. Το $\mathcal{A}$ είναι μη κενό αφού $R \in \mathcal{A}$. Αρκεί να πάρουμε $\langle A\rangle = \bigcap \mathcal{A}$ και να εφαρμόσουμε το πρώτο μέρος της Πρότασης. □

Σαν ένα παράδειγμα υποδακτυλίου του $\mathbb{Z}$ αναφέρουμε όλα τα υποσύνολά του της μορφής $k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$, για ένα k δοσμένο[11].

[11]Μερικοί συγγραφείς, όπως οι S. Mac Lane και G. Birkhoff στο πολύ γνωστό σύγγραμά τους «Algebra», στον ορισμό του δακτυλίου απαιτούν να έχει μονάδα. Αντίστοιχα στον ορισμό του υπο-δακτυλίου απαιτούν επιπλέον να περιέχει την μονάδα του δακτυλίου. Είναι φανερό πως με αυτόν τον ορισμό το $\mathbb{Z}$ δεν έχει κανένα γνήσιο μη τετριμμένο υπο-δακτύλιο.

Παράδειγμα 6 *Ας θεωρήσουμε έναν οποιοδήποτε δακτύλιο R και ένα στοιχείο του a. Από την Πρόταση 5 θα υπάρχει ένας ελάχιστος υποδακτύλιος του R που θα περιέχει το a, που τον συμβολίζουμε με $\langle a\rangle$. Ο δακτύλιος αυτός θα περιέχει αναγκαστικά τα $a, -a, 0$ αλλά και όλα τα αθροίσματά τους και γινόμενα τους. Έτσι είναι εύκολο να δούμε ότι θα περιέχει κάθε στοιχείο της μορφής:*

$$n_1 a^{k_1} + \ldots n_m a^{k_m}$$

όπου $m \in \mathbb{N}\setminus\{0\}$, $n_1, ..., n_m \in \mathbb{Z}$, $k_1, ..., k_m \in \mathbb{N}\setminus\{0\}$.

Άρα

$$\begin{aligned} A = & \\ &= \left\{n_1 a^{k_1} + \ldots n_m a^{k_m} : m \in \mathbb{N}\setminus\{0\}, n_1, ..., n_m \in \mathbb{Z}, k_1, ..., k_m \in \mathbb{N}\setminus\{0\}\right\} \subseteq \\ &\subseteq \langle a\rangle \end{aligned}$$

Όμως το άθροισμα, η διαφορά και το γινόμενο στοιχείων του A είναι στοιχείο του A[12]*, δηλαδή το A είναι υποδακτύλιος και αφού $a \in A$ θα πρέπει $\langle a\rangle \subseteq A$ και καταλήγουμε ότι:*

$$\langle a\rangle = A$$

Κλείνουμε την παράγραφο με έναν ορισμό:

Ορισμός 20 ***Κέντρο*** *ενός δακτυλίου R ονομάζουμε το σύνολο $C(R)$ όλων των στοιχείων του που αντιμετατίθενται με όλα τα υπόλοιπα. Δηλαδή*

$$C(R) = \{a \in R : \text{Για κάθε } x \in R, ax = xa\}$$

1.4 Ομομορφισμοί - Μονομορφισμοί - Ισομορφισμοί

Η γενική έννοια ενός **μορφισμού** (ή **ομομορφισμού**) μεταξύ δύο αλγεβρικών δομών X, Y του ιδίου τύπου (ημιομάδες, ομάδες, δακτύλιοι, ακέραιες περιοχές, σώματα κλπ) δίνεται σα μια συνάρτηση $f : X \to Y$ η οποία διατηρεί τις αντίστοιχες πράξεις. Εξειδικεύοντας στην περίπτωση των δακτυλίων έχουμε:

Ορισμός 21

(α) *Έστω R, R' δακτύλιοι και $f : R \to R'$. Θα ονομάζουμε την απεικόνιση f* ***ομομορφισμό δακτυλίων*** *ή απλά* ***ομομορφισμό*** *αν ικανοποιεί τις παρακάτω δύο ιδιότητες:*

(1) *Για οποιαδήποτε $a, b \in R$, $f(a+b) = f(a) + f(b)$.*

[12] Μια πολύ καλή άσκηση είναι να αποδείξετε με κάθε λεπτομέρεια τον παραπάνω ισχυρισμό

(**2**) *Για οποιαδήποτε* $a, b \in R$, $f(a \cdot b) = f(a) \cdot f(b)$.
Η ***εἰκόνα*** *του ομομορφισμού* f *είναι το σύνολο:*

$$\mathrm{Im} f = f(R) = \{f(x) : x \in R\} = \{y \in R' : \exists x \in R \text{ με } y = f(x)\}$$

Ο ***πυρήνας*** *του ομομορφισμού* f *είναι το σύνολο:*

$$\mathrm{Ker}\ f = \{x \in R : f(x) = 0\}$$

(β) *Αν ένας ομομορφισμός δακτυλίων είναι 1-1 συνάρτηση θα τον λέμε* ***μονομορφισμό δακτυλίων****.*

(γ) *Αν ένας ομομορφισμός* $f : R \to R'$ *δακτυλίων είναι συνάρτηση επί του* R' *θα τον λέμε* ***επι-μορφισμό δακτυλίων****.*

(δ) *Τέλος, αν ένας ομομορφισμός δακτυλίων είναι 1-1 και επί συνάρτηση θα τον λέμε* ***ισομορφισμό δακτυλίων****. Αν για δύο δακτυλίους* R, S *τυχαίνει να υπάρχει ισομορφισμός από τον* R *στον* S *οι δακτύλιοι θα λέγονται* ***ισόμορφοι*** *και θα γράφουμε* $R \cong S$.

Η επόμενη πρόταση είναι μία απλή και καλή **άσκηση** στις έννοιες που μόλις ορίσαμε:

Πρόταση 6
Έστω R, S *δακτύλιοι και* $f : R \to S$ *ένας ομομορφισμός. Τότε:*
(α) Η εικόνα $f(R)$ *του* f *είναι υποδακτύλιος του* S *και ο πυρήνας* $\mathrm{Ker} f$ *του* f *είναι υποδακτύλιος του* R.
(β) Η f *είναι μονομορφισμός αν και μόνο αν ο πυρήνας της είναι ίσος με* $\{0\}$.
(γ) Αν ο f *είναι μονομορφισμός τότε ο* R *είναι ισόμορφος με τον υποδακτύλιο* $f(R)$ *του* S.

Η σχέση $R \cong S$ έχει όλες τις ιδιότητες μίας σχέσης ισοδυναμίας[13] Πράγματι, αν πάρουμε τρεις οποιουσδήποτε δακτύλιους R, S, T τότε θα έχουμε ότι:

1. $R \cong R$
2. Αν $R \cong S$ τότε $S \cong R$.
3. Αν $R \cong S$ και $S \cong T$ τότε $R \cong T$.

Για να δούμε ότι ισχύει το (1) αρκεί να παρατηρήσουμε ότι η ταυτοτική απεικόνιση από ένα δακτύλιο στον εαυτό του είναι ισομορφισμός. Για το (2) αρκεί το γεγονός ότι η αντίστροφη απεικόνιση ισομορφισμού από τον R στον S είναι ισομορφισμός από τον S στον R. Τέλος το (3) προκύπτει από το γεγονός ότι η σύνθεση ισομορφισμών είναι ισομορφισμός.

[13] Δεν μπορούμε τυπικά να πούμε ότι η $\cong$ είναι μια σχέση ισοδυναμίας γιατί δεν μπορούμε να να καθορίσουμε το σύνολο στο οποίο ορίζεται. Θα μπορούσαμε να πούμε ότι ορίζεται στο «σύνολο όλων των δακτυλίων» αλλά αυτό δεν είναι επιτρεπτό στην συνολοθεωρία, όπως αυτή αναπτύσσεται στο αξιωματικό σύστημα των Zermelo-Fraenkel που είναι και το πιο διαδεδομένο. Για το λόγο αυτό συνήθως λέμε ότι η $\cong$ είναι σχέση ισοδυναμίας στην «κλάση» όλων των δακτυλίων.

Δύο ισόμορφους δακτύλιους ακόμα και αν είναι διαφορετικοί σαν σύνολα θα θεωρούμε ότι ταυτίζονται μεταξύ τους από αλγεβρική άποψη. Πράγματι, οποιαδήποτε αλγεβρική ιδιότητα έχει ένας δακτύλιος (πεπερασμένος, αντιμεταθετικός, έχει μονάδα, είναι ακέραια περιοχή, είναι σώμα κλπ) την ίδια θα έχει και οποιοσδήποτε άλλος δακτύλιος ισόμορφος με αυτόν. Με αυτή τη λογική θα λέμε ότι:

Ορισμός 22

Ένας δακτύλιος R **περιέχεται ισομορφικά** *σε ένα δακτύλιο S αν είναι ισομορφικός με ένα υποδακτύλιο του S - ή ισοδύναμα - αν υπάρχει ένας μονομορφισμός $f : R \to S$.*

Πρόταση 7

Κάθε δακτύλιος περιέχεται ισομορφικά σε ένα δακτύλιο με μονάδα.

Απόδειξη: Έστω R ένας δακτύλιος και έστω $S = R \times \mathbb{Z}$. Στο S ορίζουμε δύο πράξεις

$$(a, m) + (b, n) = (a + b, n + m)$$
$$(a, m) \cdot (b, n) = (ab + ma + nb, nm)$$

Ο S γίνεται με αυτές τις πράξεις δακτύλιος με μονάδα $1_S = (0, 1)$ και μηδέν το $0_S = (0, 0)$ όπως εύκολα μπορούμε να επαληθεύσουμε. Θεωρούμε την απεικόνιση $f : R \to S$ με $f(r) = (r, 0)$, που εύκολα δείχνουμε ότι είναι ομομορφισμός. Άρκεί να δείξουμε ότι είναι 1-1 και γι αυτό το σκοπό εξετάζουμε τον πυρήνα της: Αν $f(r) = (0, 0)$ τότε προφανώς $r = 0$ και συνεπώς $\mathrm{Ker} f = \{0\}$, δηλαδή η f είναι 1-1. □

Παράδειγμα 7 *Έστω R ένας οποιοσδήποτε δακτύλιος με μονάδα 1_R. Η απεικόνιση $f : \mathbb{Z} \to R$, που ορίζεται από τη σχέση $f(n) = n1_R$, είναι ομομορφισμός.*

1.4.1 Ασκήσεις

Ασκηση 20 *Δείξτε ότι ο δακτύλιος των ακεραίων δεν έχει γνήσιο υποδακτύλιο με μονάδα. Επίσης να δείξετε ότι αν S είναι ένας υποδακτύλιος του $\mathbb{Z}$ τότε θα υπάρχει ένα $a \in \mathbb{Z}$ με $S = (a) = \{xa : x \in \mathbb{Z}$.*

Ασκηση 21 *Να δείξετε ότι αν ένας γνήσιος υποδακτύλιος S του $\mathbb{Q}$ έχει μονάδα τότε αυτή είναι η μονάδα του $\mathbb{Q}$ και ότι ο S θα περιέχει τον $\mathbb{Z}$.*

Ασκηση 22 *Να βρείτε ένα γνήσιο υποδακτύλιο με μονάδα του δακτυλίου των ρητών αριθμών διαφορετικό από το δακτύλιο των ακεραίων.*

Ασκηση 23 *Να βρείτε τους υποδακτύλιους του $\mathbb{Z}$ που παράγονται από τα παρακάτω υποσύνολά του: $A = \{3\}, B = \{9\}, C = \{3, 9\}, D = \{4, 6\}, E = \{4, 11\}$.*

Ασκηση 24 *Έστω R, S δύο δακτύλιοι και στο $R \times S$ ορίζουμε $(r,s)+(r',s') = (r+r', s+s'), (r,s)(r',s') = (rr', ss')$. Επαληθεύσετε ότι το σύνολο $R \times S$ είναι δακτύλιος. Ο δακτύλιος αυτός συμβολίζεται με $R \oplus S$ και λέγεται το* **ευθύ άθροισμα** *των δύο δακτυλίων R, S.*

Ασκηση 25 *Αν R είναι ένας δακτύλιος τότε και $n \in \mathbb{N}$, μεγαλύτερο από 1, στο σύνολο $R^n = R \times \cdots \times R$ ορίζουμε δύο πράξεις:*
$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = ((x_1 + y_1), \ldots, (x_n + y_n))$
$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = ((x_1 y_1), \ldots, (x_n y_n))$.
Να εξετάσετε αν ο R^n με αυτές τις πράξεις είναι δακτύλιος.

Ασκηση 26 *(α) Έστω R ένας δακτύλιος, $a \in R$ και*

$$C(a) = \{x \in R : ax = xa\}$$

να δείξετε ότι ο $C(a)$ είναι υποδακτύλιος του R.
(β) Αν $A \subseteq X$ και ορίσουμε

$$C(A) = \{x : \text{ για κάθε } a \in A, ax = xa\}$$

να δείξετε ότι ο $C(A)$ είναι υποδακτύλιος του R καθώς και ότι $C(A) = \bigcap_{a \in A} C(a)$. Δείξτε ακόμα πως αν ο R είναι δακτύλιος με μονάδα τότε ο $C(R)$ είναι αντιμεταθετικός δακτύλιος με μονάδα.

Ασκηση 27 *Έστω $(G, +)$ μία αβελιανή ομάδα και $\mathrm{End}(G)$ το σύνολο όλων των ενδομορφισμών της ομάδας δηλαδή το σύνολο όλων των απεικονίσεων $f : X \to X$ με $f(x+y) = f(x) + f(y)$ για οποιαδήποτε $x, y \in G$. Το $\mathrm{End}(G)$ το εφοδιάζουμε με δύο πράξεις $f+g$, $f \cdot g$ όπου $(f+g)(x) = f(x) + g(x)$, $f \cdot g(x) = f(g(x))$. Να δείξετε ότι το $\mathrm{End}(G)$ με αυτές τις πράξεις είναι δακτύλιος.*

Ασκηση 28 *Έστω $\mathbb{C}$ ο δακτύλιος των μιγαδικών αριθμών. να εξέτασετε ποια από τα παρακάτω υποσύνολά του είναι υποδακτύλιοι.*
$A = \{m + n\sqrt{3}, m, n \in \mathbb{Z}\}$
$B = \{m + n\sqrt{3}, m, n \in \mathbb{Q}\}$
$C = \{m + n\sqrt[3]{3}, m, n \in \mathbb{Z}\}$
$D = \{m + n\sqrt{-1}, m, n \in \mathbb{Z}\}$.

Ασκηση 29 *Αν ο R είναι μεταθετικός δακτύλιος και $a \in R$ να δείξετε ότι το σύνολο $A = \{x \in R : ax = 0\}$ είναι υποδακτύλιος του R.*

Ασκηση 30 *Έστω $M_2(R)$ ο δακτύλιος όλων των 2×2 πινάκων πάνω σε ένα δακτύλιο R. Για ένα στοιχείο $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R)$ ορίζουμε $\det(x) = ad - bc$. Να δείξετε ότι $\det(xy) = \det(x)\det(y)$*

Ασκηση 31 *Έστω $M_2(\mathbb{Z}_p)$ ο δακτύλιος όλων των 2×2 πινάκων πάνω στο $\mathbb{Z}_p$, όπου ο p είναι πρώτος. Να δείξετε ότι ένα στοιχείο του $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ είναι αντιστρέψιμο αν και μόνο αν η «ορίζουσά» του $\det(A) = ad - bc$ είναι διαφορετική από 0.*

Ασκηση 32 *Αν ο R είναι μεταθετικός δακτύλιος και $a \in R$ να δείξετε ότι το σύνολο $A = \{x \in R : ax = 0\}$ είναι υποδακτύλιος του R.*

Ασκηση 33 *Ένα στοιχείο a ενός δακτυλίου θα λέγεται ένας **διαιρέτης του μηδενός** αν $a \neq 0$ και υπάρχει κάποιο $b \in R$ με $b \neq 0$ και $ab = 0$ ή $ba = 0$. Η ύπαρξη διαιρετών του μηδενός σε ένα δακτύλιο σημαίνει ότι **δεν** ισχύει ο ακόλουθος νόμος «$ab = 0 \Rightarrow a = 0$ ή $b = 0$».*
Να βρείτε τους διαιρέτες του μηδενός στους παρακάτω δακτυλίους: $\mathbb{Z}_6, \mathbb{Z}_7, \mathbb{Z}_8$.

Ασκηση 34 *Αν a, b είναι δύο στοιχεία ενός δακτυλίου που αντιμετατίθενται να δείξετε ότι:*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + b^n$$

όπου

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, k < n$$

Ορισμός 23 *Ένα στοιχείο a ενός δακτυλίου $(R, +, \cdot)$ θα λέγεται*
*(α) **ταυτοδύναμο** αν $a^2 = a$ (β) **μηδενοδύναμο** αν για κάποιο ακέραιο $n > 0$, $a^n = 0$*

Ασκηση 35 *(α) Δείξτε ότι ένα μη μηδενικό ταυτοδύναμο στοιχείο ενός δακτυλίου δεν είναι μηδενοδύναμο.*
(β) Δείξτε ότι κάθε μη μηδενικό μηδενοδύναμο στοιχείο είναι διαιρέτης του μηδενός.
(γ) Να βρείτε τα ταυτοδύναμα και μηδενοδύναμα στοιχεία στο $\mathbb{Z}_8$.
(δ) Να δείξετε ότι το μόνο μηδενοδύναμο στοιχείο μίας ακέραιας περιοχής είναι το 0 και το μόνο μη μηδενικό ταυτοδύναμο η μονάδα.

Ασκηση 36 *Στο σύνολο των ακεραίων $\mathbb{Z} \times \mathbb{Z}$ ορίζουμε δύο πράξεις με*
$(m.n) + (m', n') = (m + m', n + n')$
$(m.n) \cdot (m', n') = (mm', nn')$
Να δείξετε ότι το $\mathbb{Z} \times \mathbb{Z}$ με αυτές τις πράξεις είναι δακτύλιος με μονάδα και ότι το $\mathbb{Z} \times \{0\}$ είναι υποδακτύλιος του με μονάδα επίσης που όμως είναι διαφορετική από αυτήν του $\mathbb{Z} \times \mathbb{Z}$.

Ασκηση 37 *Ο ορισμός του υποδακτυλίου δεν απαιτεί να έχει μονάδα αν ο δακτύλιος έχει. Μπορεί να προκύψουν διάφορες περιπτώσεις όπως:*
(α) Ο δακτύλιος να μην έχει μονάδα αλλά υποδακτύλιος να έχει.
(β) Ο υποδακτύλιος να έχει μονάδα διαφορετική από αυτή του δακτυλίου.
Να δείξετε ότι αν συμβαίνει μία από τις παραπάνω περιπτώσεις τότε η μονάδα του υποδακτυλίου είναι διαιρέτης του 0. Προσπαθείστε να δώσετε παραδείγματα που δείχνουν ότι οι προηγούμενες καταστάσεις μπορεί να προκύψουν (δείτε και την προηγούμενη άσκηση)..

Ασκηση 38 *Αν R είναι ένας δακτύλιος με μονάδα 1 και το a είναι ένα μηδενοδύναμο στοιχείο του τότε το $1+a$ είναι αντιστρέψιμο. (Υπόδειξη: Αν $a^n = 0$ θεωρείστε το $1 - a + a^2 - \ldots (-1)^{n-1}a^{n-1}$).*

Ασκηση 39 *Να δείξετε ότι το κέντρο ενός δακτυλίου είναι υποδακτύλιος του.*

Ασκηση 40 *Ένα στοιχείο a μίας ημιομάδας $(H, *)$ θα λέγεται* ***ταυτοδύναμο*** *αν $a * a = a$. Το ουδέτερο στοιχείο μίας ημιομάδας, αν υπάρχει, είναι ταυτοδύναμο. Ας υποθέσουμε τώρα ότι το H είναι πεπεραμένο σύνολο. Να δείξετε ότι υπάρχει μια τουλάχιστον ελάχιστη υπο-ημιομάδα της H δηλαδή ένα μη κενό υποσύνολο A του H κλειστό ως προς την πράξη $*$ και τέτοιο ώστε κανένα γνήσιο υποσύνολο του δεν είναι κλειστό ως προς την πράξη. Στη συνέχεια να δείξετε ότι το A θα είναι αναγκαστικά μονοσύνολο και να συμπεράνετε ότι κάθε πεπερασμένη ημιομάδα πρέπει να έχει ταυτοδύναμο στοιχείο.*

Ασκηση 41 *Ένας δακτύλιος R λέγεται* ***δακτύλιος του Boole*** *αν έχει μονάδα και κάθε στοιχείο του είναι ταυτοδύναμο ως προς τον πολλαπλασιασμό. Να δείξετε ότι ένας τέτοιος δακτύλιος είναι αναγκαστικά αντιμεταθετικός.*

1.5 Η έννοια της χαρακτηριστικής ενός δακτυλίου

Συνεχίζουμε με μια ακόμη χρήσιμη έννοια που είναι η έννοια της χαρακτηριστικής ενός δακτυλίου.

Ορισμός 24
Έστω R δακτύλιος. Αν υπάρχει ένας αυστηρά θετικός ακέραιος n με την ιδιότητα $na = 0$ για όλα τα $a \in R$ τότε ο μικρότερος φυσικός $n \in \mathbb{N} \setminus \{0\}$ με την ιδιότητα για οποιοδήποτε $a \in R$ να ισχύει $na = 0$ λέγεται η ***χαρακτηριστική του δακτυλίου*** *και συμβολίζεται με $\chi(R)$.*

Αν δεν υπάρχει ένας τέτοιος φυσικός n θα λέμε ότι ο δακτύλιος έχει χαρακτηριστική 0 και θα συμβολίζουμε $\chi(R) = 0$.

Σημείωση 1 *Οι δακτύλιοι $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ έχουν όλοι χαρακτηριστική ίση με 0*[14]*. Ένας πεπερασμένος δακτύλιος δεν μπορεί να έχει χαρακτηριστική ίση με 0. Ένας δακτύλιος θα έχει χαρακτηριστική ίση με 1 αν και μόνο αν είναι τετριμένος.*

[14] Μερικοί συγγραφείς θέτουν χαρακτηριστική ίση με ∞ αντί 0

Είναι εύκολο να δούμε ότι ισχύει η παρακάτω πρόταση:

Πρόταση 8
Έστω R ένας μη τετριμένος δακτύλιος με μονάδα με χαρακτηριστική διαφορετική από 0. Τότε η χαρακτηριστική του είναι ο μικρότερος φυσικός αριθμός n με την ιδιότητα $n1_R = 0$.

Απόδειξη: Ας υποθέσουμε ότι k είναι ο μικρότερος φυσικός αριθμός n με την ιδιότητα $n1_R = 0$. Παρατηρούμε ότι για κάθε $a \in R$, n θα έχουμε ότι $na = (n1_R)a$, συνεπώς $ka = 0$ και συνεπώς $\chi(R) \leq k$. Αλλά $l = \chi(R) < k$ δεν μπορεί να συμβαίνει γιατί τότε $l1 = 0$ και η πρόταση αποδείχτηκε. □

1.5.1 Ασκήσεις

Ασκηση 42 *Δείξτε ότι ένας δακτύλιος με μονάδα έχει χαρακτηριστική ίση με 0 αν και μόνο αν περιέχει ισομορφικά το δακτύλιο των ακεραίων.*

Ασκηση 43 *Να υπολογίσετε την χαρακτηριστική των παρακάτω δακτυλίων: (α) $\mathbb{Z}_{22}$, (β)$\mathbb{Z}_{17}$, (γ) $\mathbb{C}$.*

1.6 Δακτύλιοι Διαίρεσης - Ακέραιες Περιοχές - Σώματα

Σε αυτή την παράγραφο θα κάνουμε μία πρώτη ταξινόμιση κατηγοριών δακτυλίων $(R, +, \cdot)$ κυρίως σε σχέση με τις ιδιότητες της πολλαπλασιαστικής ημιομάδας $(R, \cdot)$.

Ας θεωρήσουμε ένα μη τετριμμένο δακτύλιο $(R, +, \cdot)$ με μονάδα και την ημιομάδα $(R, \cdot)$. Μέχρι τώρα δεν έχουμε συζητήσει τίποτα σχετικά με αυτή την ημι-ομάδα. Αυτό που βλέπουμε αμέσως είναι ότι δεν μπορεί ποτέ να είναι ομάδα αφού το 0 δεν μπορεί να έχει αντίστροφο.

Ορισμός 25
*Ένα στοιχείο a ενός δακτυλίου R με μονάδα 1_R θα λέγεται **αντιστρέψιμο** αν υπάρχει ένα στοιχείο $b \in R$ με $ab = ba = 1$. Το στοιχείο αυτό -αν υπάρχει - είναι μοναδικό και συμβολίζεται με a^{-1}. Το σύνολο όλων των αντιστρέψιμων στοιχείων του R θα συμβολίζεται με R^*.*

Για παράδειγμα στο $\mathbb{Z}$ το μόνο αντιστρέψιμο στοιχείο είναι το 1.

Παράδειγμα 8 *Έστω X ένα μη κενό σύνολο και $\mathbb{R}^X$ ο δακτύλιος όλων των συναρτήσεων $f : X \to \mathbb{R}$ με τις συνηθισμένες πράξεις του αθροίσματος και γινομένου συναρτήσεων. Το 0 του δακτυλίου είναι η ταυτοτικά 0 συνάρτηση και η μονάδα του είναι η συνάρτηση που παίρνει παντού την τιμή 1. Με αυτές τις πράξεις μία $f \in \mathbb{R}^X$ είναι αντιστρέψιμη αν και μόνο αν για κάθε $x \in X$ $f(x) \neq 0$.*

Ορισμός 26
Ένας δακτύλιος με μονάδα στον οποίο κάθε μη μηδενικό στοιχείο αντιστρέφεται ως προς τον πολλαπλασιασμό θα λέγεται ***δακτύλιος διαίρεσης****. Αν επιπλέον ο δακτύλιος διαίρεσης είναι αντιμεταθετικός θα τον ονομάζουμε ένα* ***σώμα****.*

Ορισμός 27
Ένα υποσύνολο ενός δακτύλιου διαίρεσης D που είναι δακτύλιος διαίρεσης με τον περιορισμό των πράξεων σε αυτό λέγεται ***υπο-δακτύλιος διαίρεσης*** *του D. Ένα υποσύνολο ενός σώματος F που είναι σώμα με τον περιορισμό των πράξεων σε αυτό λέγεται* ***υπο-σώμα*** *του F.*

Τα βασικά παραδείγματα σωμάτων είναι οι ρητοί, οι πραγματικοί, οι μιγαδικοί αριθμοί. Υπάρχουν πολλά άλλα παραδείγματα σωμάτων που θα συναντήσουμε παρακάτω. Σημειώνουμε εδώ ότι οι ρητοί αριθμοί κατασκευάζονται από τους ακέραιους με μια τυπική διαδικασία που θα περιγράψουμε σε επόμενη παράγραφο.

Στους κλασικούς δακτυλίους αριθμών γνωρίζουμε ότι αν το γινόμενο δύο αριθμών είναι μηδέν τότε ένας από τους δύο θα είναι. Αυτή η ιδιότητα είναι πολύ χρήσιμη και την χρησιμοποιούμε πχ για να λύνουμε εξισώσεις. Αυτό όμως δεν συμβαίνει γενικά σε δακτύλιους. Έτσι, δεν είναι δύσκολο να βρούμε δύο μη μηδενικούς τετραγωνικούς πίνακες που το γινόμενό τους να είναι ο μηδενικός πίνακας ή δύο μη μηδενικές πραγματικές συναρτήσεις που το γινόμενό τους να είναι η μηδενική συνάρτηση κοκ...Για να εξετάσουμε τέτοιου είδους περιπτώσεις εισάγουμε τον παρακάτω ορισμό:

Ορισμός 28 *Έστω R δακτύλιος και $a, b \in R$ με $a, b \neq 0$. Αν συμβαίνει $ab = 0$ τα a, b θα ονομάζονται* ***διαιρέτες του μηδενός****. Συγκεκριμμένα το a θα λέγεται* ***αριστερός διαιρέτης του μηδενός*** *και το b* ***δεξιός διαιρέτης του μηδενός****.*

Παράδειγμα 9 *Ένα χαρακτηριστό παράδειγμα δακτυλίου (που μάλιστα είναι αντιμεταθετικός με μονάδα) που έχει διαιρέτες του μηδενός είναι ο $\mathbb{Z}_6$ αφού $2 \cdot 3 = 0$. Είναι φανερό ότι κάθε δακτύλιος της μορφής $\mathbb{Z}_k$ με τον k να μην είναι πρώτος αριθμός θα έχει διαιρέτες του μηδενός. Πράγματι, αν ο k δεν είναι πρώτος τότε γράφεται σαν $k = k_1 k_2$, με $1 < k_1, k_2 < k$. Οι $k_1, k_2 \in \mathbb{Z}_k$ και $k_1 k_2 = 0$. Αντίστροφα, αν ο k είναι πρώτος δεν μπορεί να έχει διαιρέτες του μηδενός. Πράγματι αν αυτό συνέβαινε θα υπήρχαν δύο $0 < i, j < k$ τέτοιοι ώστε $ij = 0$ στο $\mathbb{Z}_k$ δηλαδή ο k θα διαιρούσε Συνεπώς ο k θα διαιρούσε τον i είτε τον j. Αυτό όμως είναι άτοπο αφού οι αριθμοί i, j είναι θετικοί ακέραιοι αυστηρά μικρότεροι από τον k.*

Οι αντιμεταθετικοί δακτύλιοι με μονάδα χωρίς διαιρέτες του μηδενός αποτελούν μία σημαντική κατηγορία δακτυλίων και θα τους δώσουμε ένα ξεχωριστό όνομα.

Ορισμός 29

Ένας αντιμεταθετικός δακτύλιος με μονάδα χωρίς διαιρέτες του μηδενός θα ονομάζεται μία ***ακέραια περιοχή****.*

Πρόταση 9

Σε μία ακέραια περιοχή ισύει ο νόμος της διαγραφής για τα μη μηδενικά στοιχεία ως προς τον πολλαπλασιασμό. Με άλλα λόγια, αν R είναι μία ακέραια περιοχή και a στοιχείο της διαφορετικό από 0 και $b, c \in R$ τότε θα έχουμε $ab = ac$ αν και μόνο αν $b = c$.

Απόδειξη: Η σχέση $ab = ac$ είναι ισοδύναμη με τη $a(b - c) = 0$ και συνεπώς (αφού δεν έχουμε διαιρέτες του 0) θα ισχύει αν και μόνο αν $a \neq 0$ είτε $b - c = 0$. Η πρώτη περίπτωση αποκλείεται από υπόθεση άρα θα ισχύει η δεύτερη, δηλαδή $b = c$. □

Πρόταση 10

Η χαρακτηριστική μίας ακέραιας περιοχής R είναι είτε 0 είτε πρώτος αριθμός.

Απόδειξη: Ας υποθέσουμε ότι η χαρακτηριστική της ακέραιας περιοχής A της οποίας τη μονάδα συμβολίζουμε μα 1_A είναι ίση με $n > 0$. Η χαρακτηριστική μίας ακέραιας περιοχής δεν μπορεί να είναι ίση με 1 γιατί οι ακέραιες περιοχές δεν είναι τετριμμένοι δακτύλιοι συνεπώς θα είναι κάποιος αριθμός n μεγαλύτερος ή ίσος του 2. Ας υποθέσουμε λοιπόν ότι το n δεν είναι πρώτος οπότε θα συμβαίνει $n = n_1 n_2$ με $1 < n_1, n_2 < n$. Αλλά τότε θα είχαμε ότι $n1_A = n_1 1_A \cdot n_2 1_A$ συνεπώς θα συνέβαινε $n_1 1_A = 0$ ή $n_2 1_A = 0$ και από την προηγούμενη Πρόταση 8 θα είχαμε ότι η χαρακτηριστική θα ήταν n_1 ή n_2, άτοπο. □

Ένα άμεσο πόρισμα της πρότασης αυτής είναι η

Πρόταση 11

Κάθε πεπερασμένη ακέραια περιοχή έχει χαρακτηριστική ίση με πρώτο αριθμό.

Υπάρχουν δακτύλιοι διαίρεσης που δεν είναι σώματα. Ένα σημαντικό παράδειγμα μη αντιμεταθετικού δακτύλιου διαίρεσης είναι οι «τετράδες του Hamilton» που θα δούμε αμέσως παρακάτω.

Παράδειγμα 10 ***Οι τετράδες (ή τετράνια) του Hamilton****.*

Ας ξεκινήσουμε υπενθυμίζοντας τον ορισμό των μιγαδικών αριθμών. Το σύνολο $\mathbb{C}$ μιγαδικών αριθμών ταυτίζεται με το σύνολο $\mathbb{R}\times\mathbb{R}$ όλων των ζευγαριών πραγματικών αριθμών στο οποίο έχουμε ορίσει δύο πράξεις:

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

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

Συνήθως το ζευγάρι (a_1, b_1) *το γράφουμε σαν* $a_1\mathbf{1}+a_2\mathbf{i}$ *όπου* $\mathbf{1} = (0, 1)$ *και* $\mathbf{i} = (1, 0)$ *και ο πολλαπλασιασμός καθορίζεται μονοσήμαντα από τους κανόνες:*

$$\boxed{\begin{array}{l}\mathbf{1}\cdot\mathbf{1} = \mathbf{1}\\ \mathbf{1}\cdot\mathbf{i} = \mathbf{i}\cdot\mathbf{1} = \mathbf{i}\\ \mathbf{i}\cdot\mathbf{i} = -\mathbf{1}\end{array}}$$

Με αυτές τις πράξεις οι δυάδες πραγματικών αριθμών γίνονται ένα σώμα, που είναι το γνωστό μας σώμα των μιγαδικών αριθμών.

Ο William Rowan Hamilton ανακάλυψε ένα τρόπο να ορίσει δύο πράξεις μεταξύ των τετράδων πραγματικών αριθμών ώστε να μετατρέψει το $\mathbb{R}^4$ *σε δακτύλιο διαίρεσης*[15]*. Η ιδέα είναι να θεωρήσουμε μία τετράδα* (a_1, a_2, a_3, a_4) *στη μορφή* $a_1\mathbf{1} + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$*, να προσθέτουμε κατά τον συνήθη τρόπο*

$$\boxed{\begin{array}{l}(a_1\mathbf{1} + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}) + (b_1\mathbf{1} + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}) =\\ = (a_1 + b_1)\mathbf{1} + (a_2 + b_2)\mathbf{i} + (a_3 + b_3)\mathbf{j} + (a_4 + b_4)\mathbf{k}\end{array}}$$

Ο πολλαπλασιασμός (που είναι το περίπλοκο σημείο της υπόθεσης) καθορίζεται από τους εξής κανόνες:

$$\boxed{\begin{array}{l}\mathbf{1} \text{ } \textit{είναι η μονάδα}\\ \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}\\ \mathbf{ij} = \mathbf{k}\\ \mathbf{jk} = \mathbf{i}\\ \mathbf{ki} = \mathbf{j}\\ \mathbf{ji} = -\mathbf{k}\\ \mathbf{kj} = -\mathbf{i}\\ \mathbf{ik} = -\mathbf{j}\end{array}}$$

Με αυτούς τους κανόνες και με λίγο κόπο μπορούμε να δούμε ότι ο πολλαπλασιασμός ορίζεται ως εξής (στο εξής θα παραλείπουμε το σύμβολο $\mathbf{1}$*, όπως και στους μιγαδικούς, για λόγους απλότητας):*

$$\boxed{\begin{array}{l}(a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}) + (b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}) =\\ = c_1 + c_2\mathbf{i} + c_3\mathbf{j} + c_4\mathbf{k}\end{array}}$$

[15] Η ιδέα να θεωρεί τους μιγαδικούς αριθμούς σαν ζευγάρια πραγματικών αριθμών οφείλεται στον Hamilton που την ανακάλυψε γύρω στο 1830. Ο ίδιος αναφέρει ότι την εξήγησε στους μικρούς γιούς του οι οποίοι κάθε πρωί τον ρωτούσαν «Αφού μπαμπά μπορείς και πολλαπλάσιάζεις ζευγάρια αριθμών μπορείς να πολλαπλασιάσεις και τριάδες;» και αυτός τους απαντούσε πάντα το ίδιο «Όχι. Μόνο να τους προσθέσω και να τους αφαιρέσω μπορώ». Η ιδέα του ορισμού πολλαπλασιασμού στον $\mathbb{R}^3$ είχε γίνει σχεδόν έμμονη ιδέα στον Hamilton ο οποίος κατάλαβε σε ένα περίπατό του το 1843 ότι αυτό δεν θα μπορούσε να γίνει στο $\mathbb{R}^3$ αλλά στο $\mathbb{R}^4$ και ενθουσιασμένος χάραξε τις εξισώσεις $i^2 = j^2 = k^2 = ijk = -1$ σε μία γέφυρα του Δουβλίνου, όπου μπορεί να τις βρει κανείς μέχρι σήμερα. Αργότερα ο John Graves, ένας φίλος και πρώην συμφοιτητής του Hamilton ανακάλυψε ένα τρόπο να πολλαπλασιάζει οκτάδες, τα καλούμενα **οκτόνια**. Ο πολλαπλασιασμός τους όμως δεν είναι ούτε προσεταιριστικός! Σημειώνουμε ότι οι τετράδες και τα οκτόνια αποτελούν και σήμερα αντικείμενο έρευνας.

όπου

$$\boxed{\begin{array}{l} c_1 = a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 \\ c_2 = a_1b_2 + a_2b_1 + a_3b_4 + a_4b_3 \\ c_3 = a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2 \\ c_4 = a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1 \end{array}}$$

Ας συμβολίσουμε με $\mathbb{H}$ το σύνολο όλων των τετράδων εφοδιασμένο με τις παραπάνω πράξεις. Το να δείξουμε ότι το $\mathbb{H}$ είναι δακτύλιος (μη αντιμεταθετικός) δεν παρουσιάζει ιδιαίτερες δυσκολίες, Η μόνη δυσκολία είναι να δείξουμε ότι κάθε μη μηδενικό του στοιχείο έχει αντίστροφο ως προς τον πολλαπλασιασμό. Θα κάνουμε κάτι ανάλογο με τους μιγαδικούς. Αν $z = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ ορίζουμε τη συζυγή τετράδα του z να είναι ο αριθμός

$$\overline{z} = a_1 - a_2\mathbf{i} - a_3\mathbf{j} - a_4\mathbf{k}$$

Επίσης ορίζουμε το μέτρο z να είναι ο πραγματικός αριθμός

$$|z| = \sqrt{a_1^2 + a_2^2 + a_2^2 + a_4^2}$$

και με κάποιους υπολογισμούς μπορούμε να αποδείξουμε τους κανόνες (για οποιαδήποτε $x, y \in \mathbb{H}$):

$$\boxed{\begin{array}{l} \overline{\overline{x}} = x \\ \overline{(x+y)} = \overline{x} + \overline{y} \\ \overline{xy} = \overline{yx} \\ x\overline{x} = \sqrt{|x|} \end{array}}$$

Η τελευταία εξίσωση δείχνει ότι κάθε $x \in \mathbb{H}$ που δεν είναι ίσο με μηδέν αντιστέφεται και έχει αντίστροφο το $\dfrac{\overline{x}}{|x|}$.

1.6.1 Ασκήσεις

Ασκηση 44 *Δείξτε ότι κάθε υποδακτύλιος με μονάδα του σώματος των ρητών πρέπει να περιέχει τον δακτύλιο των ακεραίων.*

Ασκηση 45 *Να βρείτε ένα γνήσιο υποδακτύλιο με μονάδα του σώματος των ρητών διαφορετικό από τους ακεραίους.*

Ασκηση 46 *Να δείξετε ότι κάθε υποσώμα των πραγματικών αριθμών θα περιέχει το σώμα των ρητών.*

Ασκηση 47 *Να δείξετε ότι αν p είναι πρώτος αριθμός το σύνολο*

$$\{a + b\sqrt{p} : a, b \in \mathbb{R}\}$$

είναι υποσώμα του $\mathbb{R}$.

Ασκηση 48 *Να δείξετε ότι η απεικόνιση $f; \mathbb{C} \to \mathbb{C}$ με $f(z) = \overline{z}$, όπου με $\overline{z}$ συμβολίζουμε τον συζυγή μιγαδικό του z, είναι αυτομορφισμός. Χρησιμοποιώντας το παραπάνω να αποδείξετε την ταυτότητα:*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

Ασκηση 49 *Να βρείτε το κέντρο του δακτύλιου διαίρεσης $\mathbb{H}$ των τετράδων του Hamilton*

Ασκηση 50 *Έστω $M_2(\mathbb{R})$ ο δακτύλιος όλων των 2×2 πινάκων πάνω στο $\mathbb{R}$. Να δείξετε ότι το υποσύνολό του:*

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

είναι σώμα.

Ασκηση 51 *Δείξτε ότι σε μία ακέραια περιοχή $(R, +, \cdot)$ ισχύει ο νόμος της διαγραφής στον πολλαπλασιασμό για μη μηδενικά στοιχεία, δηλαδή αν $a, b \neq 0$ και $ab = ac$ τότε $b = c$*

Ασκηση 52 *Αν $z = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k} \in \mathbb{H}$ ορίζουμε τη συζυγή τετράδα του z να είναι ο αριθμός*

$$\overline{z} = a_1 - a_2\mathbf{i} - a_3\mathbf{j} - a_4\mathbf{k}$$

Επίσης ορίζουμε το μέτρο μίας τετράδας z να είναι ο πραγματικός αριθμός

$$|z| = \sqrt{a_1^2 + a_2^2 + a_2^2 + a_4^2}$$

Αποδείξτε ότι για οποιαδήποτε $x, y \in \mathbb{H}$ ισχύει:

$$\begin{gathered} \overline{\overline{x}} = x \\ \overline{(x + y)} = \overline{x} + \overline{y} \\ \overline{xy} = \overline{yx} \\ x\overline{x} = \sqrt{|x|} \end{gathered}$$

Ασκηση 53 *Αποδείξτε την παρακάτω ταυτότητα του Lagrange:*

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

όπου

$$\begin{aligned} c_1 &= a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 \\ c_2 &= a_1b_2 + a_2b_1 + a_3b_4 + a_4b_3 \\ c_3 &= a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2 \\ c_4 &= a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1 \end{aligned}$$

1.7 Πεπερασμένοι Δακτύλιοι - Μελέτη του $\mathbb{Z}_n$ - Μερικές εφαρμογές στη Θεωρία των Αριθμών

Ας επιστρέψουμε στην περίπτωση των πεπερασμένων δακτυλίων. Το πρώτο που θα δείξουμε είναι η παρακάτω πρόταση:

Πρόταση 12
Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη: Αυτό που θέλουμε να δείξουμε είναι ότι αν ένας αντιμεταθετικός δακτύλιος με μονάδα R έχει πεπερασμένο πλήθος στοιχείων και δεν έχει διαιρέτες του μηδενός τότε κάθε μη μηδενικό στοιχείο του θα αντιστρέφεται.

Ας υποθέσουμε ότι έχουμε ένα τέτοιο δακτύλιο $R = \{a_0 = 0, a_1 = 1, \ldots, a_n\}$ με $n+1$ στοιχεία και έστω $a \neq 0$ ένα οποιοδήποτε στοιχείο του διαφορετικό από το 0. Για να δείξουμε ότι το a αντιστρέφεται πρέπει να δείξουμε οτι υπάρχει κάποιο $r \neq 0$ με $ar = 1$ δηλαδή ότι το 1 είναι στοιχείο του συνόλου

$$A = \{ar : r \in R \setminus \{0\}\}$$

Παρατηρούμε το εξής:
Αν r, r' είναι δύο μη μηδενικά στοιχεία διαφορετικά μεταξύ τους τότε $ar \neq ar'$ που σημαίνει ότι το A έχει ακριβώς τόσα στοιχεία όσα και το $R \setminus \{0\}$. Πράγματι, αν συνέβαινε $ar = ar'$ τότε $a(r - r') = 0$ και επειδή είμαστε σε ακέραια περιοχή πρέπει $a = 0$ ή $r - r' = 0$. Έχουμε υποθέσει ότι $a \neq 0$ και καταλήγουμε ότι θα πρέπει $r = r'$.
Επίσης το $0 \notin A$, για τον ίδιο λόγο όπως και πριν.
Συνεπώς θα έχουμε ότι $A = R \setminus \{0\}$ και άρα $1 \in A$. □

Από αυτό έχουμε σαν πόρισμα το παρακάτω:

Πρόταση 13
Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν το n είναι πρώτος αριθμός.

Απόδειξη: Αν ο $\mathbb{Z}_n$ είναι σώμα τότε δεν έχει διαιρέτες του μηδενός, άρα ο n θα είναι πρώτος (γιατί;).

Αντίστροφα, αν ο n είναι πρώτος δεν μπορεί στο $\mathbb{Z}_n$ να έχουμε διαιρέτες του μηδενός γιατί αν για κάποια $a, b \in \mathbb{Z}_n \setminus \{0\}$ ίσχυε $ab = 0$ τότε θα είχαμε $n|ab$ οπότε $n|a$ ή $n|b$, που είναι αδύνατο αφού $1 \leq a, b \leq n - 1$. Συνεπώς, από την προηγούμενη πρόταση το $\mathbb{Z}_n$ θα είναι σώμα. □

Επειδή υπάρχουν άπειροι πρώτοι υπάρχουν και άπειρα πεπερασμένα σώματα. Παρατηρείστε ότι δύο πεπερασμένα σώματα είναι ισομορφικά αν και μόνο αν έχουν το ίδιο πλήθος στοιχείων. Αργότερα θα εξετάσουμε το ζήτημα αν υπάρχουν άλλα πεπερασμένα σώματα εκτός από τα $\mathbb{Z}_p$ (και θα δείξουμε ότι υπάρχουν) και επίσης αν υπάρχουν πεπερασμένα σώματα μη αντιμεταθετικά. Η απάντηση σε αυτό το ερώτημα είναι αρνητική όπως δείχνει το παρακάτω σημαντικό θεώρημα.

Θεώρημα 9 (Wedderburn)
Κάθε πεπερασμένο σώμα είναι αντιμεταθετικό.

Η απόδειξη του θεωρήματος αυτού είναι σχετικά δύσκολη και θα γίνει αφού δώσουμε κάποιες ακόμη έννοιες της θεωρίας δακτυλίων.

Ας επιστρέψουμε στους πεπερασμένους δακτύλιους της μορφής $\mathbb{Z}_n$ και ας εξετάσουμε πότε ένα στοιχείο του είναι η αντιστρέψιμο ως προς τον πολλαπλασιασμό. Η επόμενη πρόταση δίνει μια πλήρη απάντηση σε αυτό το ερώτημα και προφανώς συνεπάγεται την Πρόταση 13.

Πρόταση 14
Ένα μη μηδενικό στοιχείο a του $\mathbb{Z}_n$ είναι αντιστρέψιμο αν και μόνο αν οι a, n είναι σχετικά πρώτοι αριθμοί, δηλαδή έχουν σαν μέγιστο κοινό διαιρέτη την μονάδα.

Απόδειξη: Ας υποθέσουμε ότι οι a, n είναι σχετικά πρώτοι και συνεπώς θα υπάρχουν δύο ακέραιοι x, y με $1 = ax + yn$, δηλαδή $1 \equiv ax \pmod{n}$. Αν θεωρήσουμε $x_1 \in \mathbb{Z}_n$ με $x_1 \equiv x \pmod{n}$,τότε βλέπουμε ότι $ax_1 \equiv 1 \pmod{n}$ που σημαίνει ότι ο a έχει αντίστροφο στο $\mathbb{Z}_n$ τον x_1.

Αντίστροφα, αν ο a αντιστρέφεται τότε για κάποιο $x \in \mathbb{Z}_n$ θα έχουμε ότι (στο $\mathbb{Z}_n$) $ax = 1$ ή ισοδύναμα $ax \equiv 1 \pmod{n}$ ή ισοδύναμα θα υπάρχει $y \in \mathbb{Z}$ με $ax + ny = 1$. Αλλά τότε οι a, n θα πρέπει να είναι πρώτοι μεταξύ τους αφού ο μεγιστος κοινός διαιρέτης θα διαιρούσε το 1 και συνεπώς θα συνέπιπτε με αυτό. □

Για κάθε φυσικό αριθμό ας ορίσουμε $\phi(n)$ να είναι το πλήθος των φυσικών που είναι μικρότεροι από n και πρώτοι ως προς n, δηλαδή το πλήθος των στοιχείων του συνόλου $\{m \in \mathbb{N} : 1 \leq m \leq n-1 \text{ και } (m, n) = 1\}$. Ορίζεται έτσι μία συνάρτηση[16] $\phi : \mathbb{N} \to \mathbb{N}$ η οποία λέγεται η συνάρτηση του Euler και παίζει σημαντικό ρόλο στη θεωρία των αριθμών. Μπορούμε να υπολογίσουμε την τιμή $\phi(n)$ αν γνωρίζουμε την ανάλυση του n σε γινόμενο πρώτων. Αυτό προκύπτει από την «πολλαπλασιαστική ιδιότητα» της συνάρτησης που σημαίνει ότι αν δύο φυσικοί m, n είναι πρώτοι μεταξύ τους τότε $\phi(mn) = \phi(m)\phi(n)$. Επειδή οι έννοιες αυτές παίζουν σημαντικό ρόλο δίνουμε έναν επίσημο ορισμό γι αυτές.

Ορισμός 30
*Μία **αριθμητική συνάρτηση** είναι μία συνάρτηση $f : \mathbb{N} \to \mathbb{C}$.*
*Μια αριθμητική συνάρτηση f θα λέγεται **πολλαπλασιαστική** αν για οποιαδήποτε $m, n \in \mathbb{N}$ **που είναι πρώτοι μεταξύ τους** ισχύει*

$$f(mn) = f(m)f(n)$$

[16] Η συνάρτηση έχει πεδίο ορισμού τους μη μηδενικούς φυσικούς αλλά μπορούμε συμβατικά να θέσουμε $\phi(0) = 0$.

Ορισμός 31

Αν n είναι ένας φυσικός αριθμός μεγαλύτερος ή ίσος του 1 τότε η ***συνάρτηση*** ϕ ***του Euler*** *ορίζεται να είναι:*

$$\phi(n) = |\{x : 1 \leq x \leq n-1, (x,n) = 1\}|$$

Πρόταση 15

(1) Η συνάρτηση $\phi(n)$ είναι πολλαπλασιαστική.

(2) Αν p είναι πρώτος και $u \in \mathbb{N}, u \geq 1$ τότε

$$\phi(p^u) = p^u - p^{u-1} = p^u \left(1 - \frac{1}{p}\right)$$

(3) Αν n είναι ένας φυσικός αριθμός του οποίου γνωρίζουμε την ανάλυσή του σε πρώτους $n = p_1^{u_1} \dots p_k^{u_k}$ τότε

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Απόδειξη: (1) Ας υποθέσουμε ότι οι m, n είναι θετικοί ακέραιοι με $(m,n) = 1$ και ας θεωρήσουμε το όλα τα στοιχεία του $\mathbb{Z}_{mn}$ της μορφής[17]

$$xm + yn, \quad x = 1, \dots, n-1, \quad y = 1, \dots, m-1$$

Οι αριθμοί αυτοί είναι όλοι διαφορετικά στοιχεία του $\mathbb{Z}_{mn}$ και έχουν προφανώς πλήθος mn. Πράγματι, $xm + yn = x'm + y'n$ με πράξεις μέσα στο $\mathbb{Z}_{mn}$ σημαίνει ότι $xm + yn \equiv x'm + y'n \pmod{mn}$ και θα έχουμε:

Αν	$xm + yn \equiv x'm + y'n \pmod{mn}$
τότε	$xm \equiv x'm \pmod{n}$
επειδή	$(m,n) = 1$
θα έχουμε	$x \equiv x' \pmod{n}$.
Με όμοιο τρόπο θα πάρουμε	
	$y \equiv y' \pmod{m}$

Συνεπώς οι αριθμοί αυτοί αναπαριστούν όλα τα στοιχεία του $\mathbb{Z}_{mn}$ και αρκεί να δούμε ποιοί από αυτούς είναι πρώτοι με τον mn.

Θα έχουμε:

[17] Οι πράξεις μέσα στο $\mathbb{Z}_{mn}$

$$(xm+yn, mn) = 1$$

Ισοδυναμεί με $(xm+yn, mn) = 1$ και $(xm+yn, mn) = 1$

επειδή $(m, n) = 1$

αυτό ισοδυναμεί με $(xm, n) = 1$ και $(yn, m) = 1$

που ισοδυναμεί με $(x, n) = 1$ και $(y, m) = 1$

Συνεπώς όλοι οι πρώτοι προς τον mn είναι οι $xm+yn$ με $(x, n) = 1$ και $(y, m) = 1$. Επειδή έχουμε $\phi(n)$ αριθμούς x πρώτους πρός n διαφορετικούς $\pmod n$ και $\phi(m)$ αριθμούς y πρώτους πρός m διαφορετικούς ανά δύο $\pmod n$ καταλήγουμε ότι θα έχουμε ακριβώς $\phi(n)\phi(m)$ αριθμούς στο $\mathbb{Z}_{mn} \setminus \{0\}$ πρώτους με τον mn.
(2) Αν p είναι πρώτος και $u \geq 1$ ακέραιος τότε οι μόνοι αριθμοί $< p^u$ που έχουν κοινό διαιρέτη με τον p^u είναι τα πολλαπλάσια του p, δηλαδή οι
$p, 2p, 3p, \ldots, (p^{u-1}-1)p$, συνεπώς

$$\phi(p^u) = (p^u - 1) - \left(p^{(u-1)} - 1\right) = p^u \left(1 - \frac{1}{p}\right)$$

(3) Αν $n = p_1^{u_1} \ldots p_k^{u_k}$ από (1) και (2) θα έχουμε

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{u_1}\right) \ldots \phi\left(p_k^{u_k}\right) = \\ &= p_1^{u_1} \ldots p_k^{u_k} \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right) = \\ &= n \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

□

Αν θεωρήσουμε όλα τα αντιστρέψιμα στοιχεία ενός δακτυλίου με μονάδα αυτά αποτελούν μία ομάδα ως προς τον πολλαπλασιασμό με ουδέτερο στοιχείο το 1. Αν συνεπώς θεωρήσουμε το σύνολο

$$\mathbb{H}_n = \{x \in \mathbb{Z}_n \setminus \{0\} : (x, n) = 1\}$$

τότε από την Πρόταση 14 αυτό είναι ακριβώς το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$ και συνεπώς είναι μια ομάδα ως προς τον πολλαπλασιαμό με ουδέτερο στοιχείο $e = 1$.

Γνωρίζουμε από την Θεωρία ομάδων ότι για κάθε πεπερασμένη ομάδα $(G, \cdot)$ και οποιοδήποτε $x \in G$ θα ισχύει $x^{|G|} = e$, όπου $|G|$ το πλήθος των στοιχείων της ομάδας (η τάξη της ομάδας). Επίσης εξ ορισμού $|\mathbb{H}_n| = \phi(n)$. Συνεπώς αν πάρουμε ένα οποιοδήποτε ακέραιο a πρώτο ως πρός n θα υπάρχει ένα μοναδικό $b \in \mathbb{H}_n$ με $a \equiv b \pmod n$ για το οποίο θα έχουμε ότι $b^{\phi(n)} = 1$ που σημαίνει ότι $n | b^{\phi(n)} - 1$. Αφού $n | a - b$ θα έχουμε ότι και $n | a^{\phi(n)} - 1$. Συνδυάζοντας τα όλα αυτά καταλήγουμε άμεσα στο παρακάτω:

Θεώρημα 10 (Euler)
Αν $n \geq 2, a$ μη μηδενικοί ακέραιοι πρώτοι μεταξύ τους τότε

$$n|a^{\phi(n)} - 1$$

Με άμεσο πόρισμα το :

Θεώρημα 11 (Fermat)
Αν a μη μηδενικός ακέραιος και p πρώτος που δεν διαιρεί τον a τότε

$$p|a^{p-1} - 1$$

Ασκηση 54
Δείξτε ότι ο 21 διαιρεί τον $(5 \cdot 17 \cdot 19)^{12k} - 1$ για οποιοδήποτε $k \geq 1$.

Ας πάρουμε ένα οποιοδήποτε πρώτο p. Από όσα έχουμε πεί εδώ το $\mathbb{H}_p = \{1, \ldots, p-1\}$ είναι ομάδα ως πρός τον πολλαπλασιασμό στο $\mathbb{Z}_p$. Θεωρείστε ένα $a \in \mathbb{H}_p$. Τότε με πράξεις στο $\mathbb{Z}_p$

$$\begin{aligned} a^2 = 1 \Leftrightarrow a^2 - 1 = 0 \Leftrightarrow \\ \Leftrightarrow (a-1)(a+1) = 0 \Leftrightarrow \\ \Leftrightarrow a = 1 \text{ ή } a = p-1 \end{aligned}$$

Συνεπώς κάθε στοιχείο του $\mathbb{Z}_p \setminus \{0\}$ διαφορετικό από 1 ή $p-1$ έχει αντίστροφο διαφορετικό από τον εαυτό του που σημαίνει ότι στο $\mathbb{Z}_p$ $2 \cdot 3 \cdot (p-1) = p-1 = -1$ δηλαδή $(p-1)! \equiv -1 \pmod{p}$ δηλαδή $p|(p-1)! + 1$.

Αντίστροφα, ας πάρουμε ένα οποιοδήποτε θετικό ακέραιο ≥ 2 που να έχει την ιδιότητα $n|(n-1)! + 1$ και ας θεωρήσουμε ένα οποιοδήποτε θετικό διαιρέτη του διαφορετικό από τον εαυτό του. Τότε αυτός διαιρεί τον $n|(n-1)! + 1$ και είναι κάποιος από τους $\{1, \ldots, n-1\}$. Αλλά ο κάθε αριθμός $x \neq 1$ που ανήκει στο σύνολο αυτό αφήνει υπόλοιπο διαίρεσης με τον $(n-1)! + 1$ την μονάδα δηλαδή δεν διαιρεί τον $(n-1)! + 1$. Άρα ο μόνος θετικός διαιρέτης του n εκτός από τον εαυτό του είναι το 1 ή με άλλα λόγια ο n είναι πρώτος αριθμός. Καταλήξαμε να αποδείξουμε έτσι το γνωστό:

Θεώρημα 12 (Wilson)
Ένας ακέραιος $n \geq 2$ είναι πρώτος αν και μόνο αν διαιρεί τον $(n-1)! + 1$.

1.8 Ιδεώδη - Δακτύλιοι Πηλίκα

Ας ξεκινήσουμε με ένα παράδειγμα, που το έχουμε ήδη συναντήσει στην προηγούμενη παράγραφο. Ας θεωρήσουμε το δακτύλιο $\mathbb{Z}$, ένα στοιχείο του k και τον υποδακτύλιο

$$A = k\mathbb{Z} = \{kn : n \in \mathbb{Z}\}$$

Στον $\mathbb{Z}$ ορίζουμε μία σχέση ισοδυναμίας

$$a \equiv b \pmod{k} \text{ αν και μόνο αν } a - b \in A\}$$

Ο χώρος πηλίκο που ορίζει αυτή η σχέση ισοδυναμίας γίνεται αντιμεταθετικός δακτύλιος με τις πράξεις της πρόσθεσης και γινομένου δύο κλάσεων ισοδυναμίας. Δεν είναι δύσκολο να διαπιστώσουμε ότι ο δακτύλιος που παίρνουμε με αυτή τη διαδικασία είναι ο $\mathbb{Z}_k$ που ορίσαμε σε προηγούμενη παράγραφο (για την ακρίβεια είναι ισόμορφος με αυτόν, αλλά έχουμε συμφωνήσει να μη διακρίνουμε μεταξύ τους δύο τυπικά διαφορετικούς αλλά ισόμορφους δακτυλίους).

Αν προσπαθήσουμε να επεκτείνουμε την κατασκευή αυτή σε οποιοδήποτε δακτύλιο R ως προς κάποιο υποδακτύλιό του A με ακριβώς τον ίδιο τρόπο θα συναντήσουμε δυσκολία. Για την ακρίβεια, ας ξεκινήσουμε με τον ίδιο τρόπο ορίζοντας τη σχέση $\sim$ με $x \sim y$ αν και μόνο αν $x - y \in A$. Εύκολα θα μπορέσουμε να δείξουμε ότι η σχέση αυτή είναι σχέση ισοδυναμίας. Το πρόβλημα θα προκύψει όταν προσπαθήσουμε να ορίσουμε τις πράξεις στο σύνολο πηλίκο αυτής της σχέσης. Στην περίπτωση του $\mathbb{Z}$ αυτό γινόταν γιατί ίσχυαν οι σχέσεις

$$[x] + [y] = [x + y] \tag{1}$$
$$[x][y] = [xy] \tag{2}$$

όπου $[x]$ είναι η κλάση ισοδυναμίας του στοιχείου x και $[x] + [y]$, $[x][y]$ συμβολίζει το συνηθισμένο άθροισμα και γινόμενο υποσυνόλων σε δακτύλιο.

Η σχέση (1) δεν είναι δύσκολο να επαληθευτεί. Ας προσπαθήσουμε να δείξουμε την σχέση (2): Ας πάρουμε πρώτα ένα $z \in [x][y]$. Επιθυμούμε να δείξουμε πως $z \in [xy]$. Το z γράφεται αν $z = (x + a)(y + b)$ όπου $a, b \in A$. Άρα $z = xy + (xb + ay + ab)$.Αν τα xb, ay, ab ανήκαν στο A τότε θα ανήκε και το άθροισμά τους $xb + ay + ab$ και θα είχαμε δείξει ότι $z \in [xy]$. Το $ab \in A$ αφού το A είναι υποδακτύλιος και τα a, b είναι στοιχεία του. Τα x, y όμως δεν είναι στοιχεία του A και συνεπώς δεν μπορούμε να ξέρουμε ότι τα $xb, ay \in A$. Στην προηγούμενη περίπτωση του $\mathbb{Z}$ τα είχαμε καταφέρει γιατί το A που είχαμε διαλέξει είχε την επιπλέον ιδιότητα:

Για οποιοδήποτε $x \in \mathbb{Z}$ και οποιοδήποτε $a \in A$ ισχύει $ax, xa \in A$.

Ακριβώς αυτή την ιδιότητα των υποσυνόλων $A = k\mathbb{Z}$ του $\mathbb{Z}$ που εκμεταλευτήκαμε για να ορίσουμε το χώρο πηλίκο $\mathbb{Z}_k$ θέλουμε να έχει ένας υποδακτύλιος στην γενική περίπτωση και έτσι ορίζουμε:

Ορισμός 32
Αμφίπλευρο Ιδεώδες *ή απλά* ***Ιδεώδες*** *ενός δακτυλίου R είναι ένα μη κενό υποσύνολο A του R τέτοιο ώστε:*
(a) Για οποιαδήποτε $a, b \in A$, $a - b \in A$

(β) Για οποιοδήποτε $r \in R$ και οποιοδήποτε $a \in A$, $ra \in A$ και $ar \in A$.
Αν αντί της συνθήκης (β) θεωρήσουμε την ασθενέστερη:
(β′) Για οποιοδήποτε $r \in R$ και οποιοδήποτε $a \in A$, $ar \in A$.
θα λέμε ότι το A είναι ένα ***δεξιό ιδεώδες****.*
Αν αντίστοιχα, αντί της συνθήκης (β) θεωρήσουμε την ασθενέστερη:
(β′) Για οποιοδήποτε $r \in R$ και οποιοδήποτε $a \in A$, $ra \in A$.
θα λέμε ότι το A είναι ένα ***αριστερό ιδεώδες****.*
Φανερά ένα υποσύνολο του R είναι ιδεώδες αν και μόνο αν είναι και αριστερό και δεξιό ιδεώδες.
Ο δακτύλιος R και το μονοσύνολο $\{0\}$ είναι ιδεώδη που λέγονται τα ***μη-γνήσια*** *ιδεώδη του δακτυλίου. Όλα τα υπόλοιπα ιδεώδη (αν υπάρχουν) λέγονται* ***γνήσια****.*

Μια απλή αναδιατύπωση των ορισμών είναι η παρακάτω:

Ένα μη κενό υποσύνολο A ενός δακτυλίου R είναι:
Υποδακτύλιος *αν και μόνο αν $A - A \subseteq A$ και $A \cdot A \subseteq A$*
Ιδεώδες *αν και μόνο αν $A - A \subseteq A$, $R \cdot A \subseteq A$ και $A \cdot R \subseteq A$.*

Παράδειγμα 11 *Τα υποσύνολα του $\mathbb{Z}$ της μορφής $k\mathbb{Z}$, είναι τα ιδεώδη του $\mathbb{Z}$, όπως έχουμε ήδη αναφέρει.*

Μια απλή παρατήρηση για τα ιδεώδη είναι η παρακάτω:

Πρόταση 16
Έστω R δακτύλιος με μονάδα και I ένα ιδεώδες του. Αν $1 \in I$ τότε $I = R$. Ειδικά κανένα στοιχείο ενός γνήσιου ιδεώδους δεν μπορεί να είναι αντιστρέψιμο.

Απόδειξη: Αν $1 \in I$ τότε για κάθε $r \in R$ θα είχαμε ότι $r = 1r \in I$ και συνεπώς $I = R$. Ας υποθέσουμε ότι το ιδεώδες I περιείχε κάποιο αντιστρέψιμο στοιχείο του δακτυλίου a και έστω a^{-1} το αντίστροφό του. Τότε το I θα περιείχε και το $aa^{-1} = 1$ άρα θα είχαμε ότι $I = R$. □

Η παρατήρηση αυτή μας δείχνει ότι τα σώματα $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, ...)$ δεν περιέχουν μη τετριμμένα ιδεώδη.

Παράδειγμα 12 *Ένα άλλο παράδειγμα δακτυλίου στον οποίο δεν μπορούμε να βρούμε μη τετριμμένα ιδεώδη είναι ο δακτύλιος $M_n\mathbb{R}$ των $n \times n$ πινάκων με πραγματικούς συντελεστές. Πράγματι, αν I είναι ένα μη τετριμμένο ιδεώδες του $M_n\mathbb{R}$ τότε θα περιέχει ένα μη μηδενικό πίνακα $A = (a_{ij})$. Θεωρούμε ένα μη μηδενικό στοιχείο a_{kl} του πίνακα A και έστω O_{ij} να είναι ο πίνακας που είναι παντού 0 εκτός από το στοιχείο στην ij θέση που είναι ίσο με 1. Ας συμβολίσουμε επίσης με $\mathbf{1}$ τον*

μοναδιαίο $n \times n$ πίνακα. Τότε θα έχουμε

$$O_{ij} = O_{ir}O_{rj} \tag{1}$$
$$O_{kl} = \left[O_{kk}(a_{kl}^{-1}\mathbf{1})\right] A \left[O_{ll}\right] \in I \tag{2}$$
από (1) και (2) θα έχουμε: $$O_{ij} = O_{ik}O_{kl}O_{lj} \in I \tag{3}$$
$$\text{Άρα,} \qquad \mathbf{1} = \sum_{i=1}^{n} O_{ii} \in I$$

Συνεπώς, $I = M_n(\mathbb{R})$.

Ας δούμε τώρα πως ορίζεται ο δακτύλιος-πηλίκο ως προς κάποιο ιδεώδες:

Πρόταση και Ορισμός 2
Έστω R δακτύλιος και A ένα ιδεώδες του. Η σχέση $\sim$ που ορίζεται στον R με $a \sim b$ αν και μόνο αν $a - b \in A$ είναι μία σχέση ισοδυναμίας στο R που έχει τις εξής ιδιότητες:

Αν $x \sim y, x' \sim y'$ τότε
$$x + x' \sim y + y' \tag{1}$$
$$xx' \sim yy' \tag{2}$$

Επιπλέον το σύνολο πηλίκο $R/\sim$ που συμβολίζεται και με R/A άποτελείται από όλα τα υποσύνολα του R της μορφής $[x] = x + A = \{x + a : a \in A\}$, $x \in R$ και είναι δακτύλιος ως πρός τις πράξεις

$$[x] + [y] = [x + y] \tag{3}$$
$$[x] \cdot [y] = [x \cdot y] \tag{4}$$

Ο δακτύλιος R/A θα λέγεται ο ***δακτύλιος πηλίκο*** *του R ως προς το ιδεώδες A.*

Απόδειξη: Αν $x \in R$ τότε $x - x = 0 \in A$ και συνεπώς $x \sim x$.
Αν $x \sim y$ τότε $x - y \in A$ και άρα $-(x - y) = y - x \in A$,δηλαδή $y \sim x$.
Αν $x \sim y$ και $y \sim z$ τότε $x - z = (x - y) - (y - z) \in A$ και συνεπώς $x \sim z$. Άρα η σχέση $\sim$ είναι σχέση ισοδυναμίας.

Ας υποθέσουμε ότι $x \sim y$ και $x' \sim y'$. Τότε $x - y \in A$ και $x' - y' \in x$. Συνεπώς $(x - y) + (x' - y') \in A$ αφού το A είναι ιδεώδες άρα $(x + x') - (y + y') \in A$, που σημαίνει ότι $x + x' \sim y + y'$.
Για να δείξουμε ότι $xx' \sim yy'$, θεωρούμε $a, a' \in A$ με $x = y + a, x' = y' + a'$ και θα έχουμε ότι $xx' = yy' + (ay' + aa' + a'y)$. Αλλά το $ay' + aa' + a'y \in A$ επειδή το A είναι ιδεώδες και συνεπώς $xx' \sim yy'$.

Η κλάση ισοδυναμίας ενός στοιχείου x είναι το σύνολο

$$[x] = \{r \in R : r - x \in A\} = x + A$$

Για να δείξουμε ότι η πράξεις στο σύνολο πηλίκο R/A που ορίσαμε από τις σχέσεις (3), (4) είναι πράγματι καλά ορισμένες που σημαίνει ότι πρέπει να δείξουμε πως αν $[x] = [x']$ και $[y] = [y']$ (ή ισοδύναμα ότι αν $x \sim x'$ και $y \sim y'$) τότε $[x + y] = [x' + y'], [x \cdot y] = [x' \cdot y']$. Αλλά αυτό ακριβώς μας εξασφαλίζουν οι σχέσεις (1), (2) που αποδείξαμε πιο πριν. Είναι εύκολο να δείξουμε ότι το R/A με τις πράξεις αυτές έχει όλες τις ιδιότητες του δακτυλίου, δηλαδή είναι ένας δακτύλιος που ονομάζεται ο δακτύλιος πηλίκο (ως προς το ιδεώδες A).

Ας δείξουμε για παράδειγμα την επιμεριστικότητα του πολλαπλασιαμού: Αν $[x], [y], [z] \in R/A$ τότε

$$\begin{aligned}[x]([y] + [z]) = \\ &= [x][y + z] = [x(y + z)] = \\ &= [xy + xz] = [xy] + [xz] = \\ &= [x][y] + [x][z]\end{aligned}$$

Τέλος σημειώνουμε πως αν ο R έχει μονάδα τότε και ο R/A θα έχει σαν μονάδα το $[1] = \{a + 1 : a \in A\}$. $\square$

Ας δούμε ένα τρόπο να «κατασκευάζουμε» ιδεώδη σε ένα οποιοδήποτε δακτύλιο. Έστω $A \subseteq R$ ένα οποιοδήποτε υποσύνολο ενός δακτυλίου R. Στην προηγούμενη παράγραφο είχαμε δείξει ότι υπάρχει ένας ελάχιστος υποδακτύλιος που περιέχει το A και αυτό προέκυψε από το γεγονός ότι η τομή ενός οποιουδήποτε συνόλου υποδακτυλίων είναι επίσης υποδακτύλιος. Το ίδιο συμβαίνει και στα ιδεώδη.

Πρόταση και Ορισμός 3
(α) Αν $(A_i)_{i \in I}$ είναι μία οικογένεια από ιδεώδη ενός δακτυλίου R, η τομή τους είναι ένα ιδεώδες.
(β) Αν A είναι ένα οποιοδήποτε μη κενό υποσύνολο ενός δακτυλίου R η τομή όλων των ιδεωδών που περιέχουν το A είναι το ελάχιστο ιδεώδες που περιέχει το A σαν υποσύνολό του και το οποίο θα συμβολίζουμε με (A) και θα ονομάζουμε το ***ιδεώδες που παράγεται από το σύνολο*** *A.*
Στην ειδική περίπτωση που το $A = \{a_1, \ldots, a_k\}$ είναι ένα πεπερασμένο σύνολο θα γράφουμε και $(a_1, \ldots, a_k)$ αντί του (A).

Απόδειξη: Έστω $A = \bigcap_{i \in I}$ η τομή της οικογένειας των ιδεωδών. Αν $a, b \in A$ τότε για οποιοδήποτε $i \in I$ θα συμβαίνει $a, b \in A_i$ και αφού το A_i είναι ιδεώδες θα έχουμε ότι $a - b \in A_i$. Αυτό όμως σημαίνει ότι $a - b \in A$.
Τέλος αν $a \in A$ και $r \in R$ θα έχουμε ότι για κάθε στοιχείο A_i της οικογένειας θα συμβαίνει $a \in A_i$, άρα και $ra, ar \in A_i$, άρα $ra, ar \in A$ και το πρώτο μέρος της πρότασης αποδείχτηκε. Το (β) είναι άμεση συνέπεια του (α). $\square$

Παράδειγμα 13 *Αν R είναι δακτύλιος τότε το ιδεώδες που παράγεται από ένα οποιοδήποτε στοιχείο του $a \in R$ αποτελείται από όλα τα στοιχεία της μορφής*

$$na + ra + as + \sum_{i=1} kr_i as_i$$

με το $n \in \mathbb{Z}$, $k \in \mathbb{N}$ και τα $r, s, r_1, \ldots, r_k, s_1, \ldots, s_k$ στοιχεία του δακτυλίου. Αυτό το επαληθεύει κανείς παρατηρώντας ότι η διαφορά δύο στοιχείων αυτής της μορφής είναι στοιχείο αυτής της μορφής, το ίδιο και το γινόμενο ενός τέτοιου στοιχείου με οποιοδήποτε στοιχείο του δακτυλίου. Στη ειδική περίπτωση που ο δακτύλιος έχει μονάδα τα πράγματα απλοποιούνται και έχουμε την αμέσως παρακάτω πρόταση.

Πρόταση 17 *Αν είναι ένας δακτύλιος με μονάδα και a ένα στοιχείο του τότε το ιδεώδες που παράγει το a είναι*

$$(a) = \left\{ \sum_{i=1}^{k} r_i a s_i : k \in \mathbb{N}, r_i, s_i \in R \right\}$$

Αν επιπλέον ο δακτύλιος είναι αντιμεταθετικός θα έχουμε

$$(a) = \{ra : r \in R\}$$

Απόδειξη: Ας συμβολίσουμε με A το σύνολο $\left\{ \sum_{i=1}^{k} r_i a s_i : k \in \mathbb{N}, r_i, s_i \in R \right\}$. Αν $x, y \in A$ τότε αυτά γράφονται σαν $x = \sum_{i=1}^{k} r_i a s_i, y = \sum_{i=1}^{k'} r'_i a s'_i$, οπότε θα έχουμε ότι $x - y = \sum_{i=1}^{k+k'} r''_i a s''_i$, όπου

$$r''_i = \begin{cases} r_i & \text{αν } 1 \leq i \leq k \\ (-r'_i) & \text{αν } k+1 \leq i \leq k+k' \end{cases}, s''_i = \begin{cases} s_i & \text{αν } 1 \leq i \leq k \\ s'_i & \text{αν } k+1 \leq i \leq k+k' \end{cases}$$

συνεπώς $x - y \in A$. Παρόμοια, αν $x \in A$ τότε για οποιοδήποτε $r \in R$ θα έχουμε ότι $rx, xr \in A$ (αυτό προκύπτει εύκολα λόγω της επιμεριστικής ιδιότητας) και συνεπώς το A είναι ιδεώδες. Επειδή $a = 1_R a 1_R$ και το $a \in A$. Συνεπώς το A είναι ιδεώδες που περιέχει το a και επειδή το (a) είναι το ελάχιστο ιδεώδες με αυτή την ιδιότητα καταλήγουμε ότι:

$$(a) \subseteq A$$

Αντίστροφα αν $x = r_1 a s_1 + \cdots + r_k a s_k$ είναι ένα οποιοδήποτε στοιχείο του A επειδή $a \in (a)$ και το (a) είναι ιδεώδες θα έχουμε ότι τα $r_1 a s_1, \ldots, r_k a s_k \in A$ και άρα $x = r_1 a s_1 + \cdots + r_k a s_k \in A$. Συνεπώς και $A \subseteq (a)$.

Αν ο δακτύλιος είναι αντιμεταθετικός τότε για το τυχόν στοιχείο του (a),

$$x = r_1 a s_1 + \cdots + r_k a s_k = \\ = r_1 s_1 a + \cdots + r_k s_k a$$

□

Παράδειγμα 14 *Ας θεωρήσουμε τον δακτύλιο R^X όλων των συναρτήσεων από ένα σύνολο X σε ένα δακτύλιο R και έστω $x \in R$. Το σύνολο*

$$I_x = \{f \in R^X : f(x) = 0\}$$

είναι ένα ιδεώδες του R^X. Αν θεωρήσουμε ένα μη κενό υποσύνολο Y του X και πάρουμε σαν

$$I_Y = \{f \in R^X : \text{ για κάθε } x \in Y,\ f(x) = 0\}$$

είναι ένα ιδεώδες επίσης που εκφράζεται και σαν μια τομή ιδεωδών:

$$I_Y = \bigcap_{y \in Y} I_y$$

Θυμίζουμε ότι ο πυρήνας ενός ομομορφισμού δακτυλίων $f : R \to R'$ είναι υποδακτύλιος του R. Η επόμενη πρόταση δείχνει ότι είναι κάτι παραπάνω. Είναι ιδεώδες. Την απόδειξή της την αφήνουμε σαν άσκηση.

Πρόταση 18 *Έστω R, R' δακτύλιοι και $f : R \to R'$ ένας ομομορφισμός. Ο πυρήνας* $\mathrm{Ker} f$ *του f είναι ιδεώδες του R.*

Πρόταση και Ορισμός 4
Αν R είναι ένας δακτύλιος και I ένα ιδεώδες του τότε η απεικόνιση $\phi : R \to R/I$ με

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

είναι ομομορφισμός δακτυλίων και $\mathrm{Ker}\phi = I$. *Η απεικόνιση αυτή ονομάζεται η* ***κανονική απεικόνιση*** *από το R στο R/I.*

Απόδειξη: Αρκεί να δείξουμε πώς αν $x, y \in R$ ισχύει $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ και $\phi(x-y) = \phi(x)-\phi(y)$. Αλλά από την Πρόταση 2 $\phi(x \cdot y) = xy+I = (x+I)(y+I) = \phi(x)\phi(y)$ και $\phi(x-y) = (x-y)+I = (x+I)+(-y+I) = \phi(x)+\phi(-y) = \phi(x)-\phi(y)$. Τέλος $\phi(x) = 0$ ισοδυναμεί με $x + I = I$ που ισοδυναμεί με $x \in I$ (Άσκηση). □

1.9 Τα Θεωρήματα Ομομορφισμού

Τα θεωρήματα ομομορφισμού σε δακτυλίους είναι εντελώς ανάλογα με τα αντίστοιχα θεωρήματα που ισχύουν σε ομάδες.

Θεώρημα 13 (Πρώτο Θεώρημα Ομομορφισμών)
Έστω R, R' δακτύλιοι και ένας επιμορφισμός δακτυλίων $f : R \to R'$. Τότε

$$R/\mathrm{Ker} f \cong R'$$

Απόδειξη: Είναι γνωστό πως αν $f : R \to R'$ είναι ένας ομορφισμός δακτυλίων τότε ο πυρήνας του $K = \mathrm{Ker}f$ είναι ένα ιδεώδες του R και συνεπώς ορίζεται ο δακτύλιος πηλίκο R/K. Θεωρούμε την απεικόνιση $g : R/K \to R'$ που ορίζεται από την σχέση

$$g(x + K) = f(x)$$

Θα δείξουμε πρώτα ότι είναι καλά ορισμένη και μετά ότι είναι ισομορφισμός. Για το πρώτο παρατηρείστε πως αν $x \sim x'$ τότε θα έχουμε ότι $x - x' \in K$ που σημαίνει ότι $f(x - x') = f(x) - f(x') = 0$ δηλαδή $f(x) = f(x')$, που είναι ακριβώς αυτό που πρέπει να δείξουμε.

Η g είναι ομομορφισμός δακτυλίων. Πράγματι, αν $x + K, x' + K \in R/K$ τότε

$$\begin{aligned} g\left((x + K) + (x' + K)\right) &= \\ &= g\left((x + x') + K)\right) = \\ &= f(x + x') = \\ &= f(x) + f(x') = \\ &= g(x + K) + g(x' + K) \\ g\left((x + K) \cdot (x' + K)\right) &= \\ &= g\left((x \cdot x') + K)\right) = \\ &= f(x \cdot x') = \\ &= f(x) \cdot f(x') = \\ &= g(x + K) \cdot g(x' + K) \end{aligned}$$

Απομένει να δείξουμε ότι η g είναι 1-1 και επί. Επειδή η $f : R \to R'$ είναι επί για κάθε $y \in R'$ υπάρχει $x \in R$ με $f(x) = y$ και προφανώς $g(x + K) = y$, δηλαδή η g είναι επί.

Επίσης αν $g(x+K) = g(x'+K)$ θα έχουμε ότι $f(x) = f(x')$ δηλαδή $f(x-x') = 0$ ή ισοδύναμα $x - x' \in \mathrm{Ker}f = K$, άρα $x + K = x' + K$ που σημαίνει ότι η g είναι 1-1. □

Ασκηση 55 *Σαν παράδειγμα εφαρμογής του παραπάνω θεωρήματος θεωρούμε $R = \mathbb{R}^{\mathbb{R}}$, το δακτύλιο όλων των συναρτήσεων από το $\mathbb{R}$ στο $\mathbb{R}$ και $R' = \mathbb{R}$, διαλέγουμε ένα οποιοδήποτε στοιχείο a του $\mathbb{R}$ και ορίζουμε $F : \mathbb{R}^{\mathbb{R}} \to \mathbb{R}$ με $F(f) = f(a)$. Δείξτε ότι η F είναι επιμορφισμός δακτυλίων και ότι ο δακτύλιος πηλίκο είναι ισομορφικός με το σύνολο όλων των πραγματικών αριθμών.*

Ας θεωρήσουμε τώρα δύο δακτύλιους R, R' ένα επιμορφισμό $f : R \to R'$ και τον πυρήνα K του f που είναι ένα ιδεώδες του R. Ας θεωρήσουμε ένα οποιοδήποτε ιδεώδες I' του R' και ας εξετάσουμε την αντίστροφη εικόνα του, που είναι ένα υποσύνολο του R:

$$f^{-1}(I') = \{x \in R : f(x) \in I'\} = f^{-1}(I') \tag{1.5}$$

Τότε το $f^{-1}(I')$ είναι ένα ιδεώδες του R το οποίο περιέχει σαν υποσύνολό του το K, το οποίο είναι και ιδεώδες του $f^{-1}(I')$. Η απεικόνιση f περιορισμένη στο $f^{-1}(I')$ είναι ένας επιμορφισμός από το $f^{-1}(I')$ επί του I' και έχει πυρήνα το K, οπότε από το Πρώτο Θεώρημα Ομομορφισμού θα έχουμε ότι

$$f^{-1}(I')/K \cong I'$$

Επιπλέον η απεικόνιση f^{-1} είναι 1-1 και επί του συνόλου όλων των ιδεωδών του R που περιέχουν το K.

Το ότι η f^{-1} είναι 1-1 προκύπτει γενικά από το γεγονός είναι αν έχουμε μία απεικόνιση μεταξύ δύο συνόλων $f : X \to Y$ που είναι επί του Y τότε η αντίστροφη συνολοσυνάρτηση $f^{-1} : 2^Y \to 2^Y$ είναι 1-1.[18]

Για να δείξουμε ότι είναι επί θεωρούμε ένα είναι ένα οποιοδήποτε ιδεώδες I του R με $K \subseteq R$ τότε το $f(I) = \{f(x) : x \in I\}$ είναι ένα ιδεώδες[19] του R'. Απομένει να δείξουμε ότι $f^{-1}(f(I)) = I$. Γενικά $f^{-1}(f(I)) \supset I$. Ας δείξουμε ότι και $f^{-1}(f(I)) \subseteq I$. Αν $x \in f^{-1}(f(I))$ τότε $f(x) \in f(I)$ δηλαδή $f(x) = f(a)$ για κάποιο $a \in I$ οπότε $f(x-a) = 0$ δηλαδή το $x - a \in K$. Αλλά $K \subseteq I$ και συνεπώς $x \in I$.

Καταλήξαμε έτσι να αποδείξουμε το ακόλουθο:

Θεώρημα 14 (Θεώρημα της Αντιστοιχίας)
Έστω R, R' δακτύλιοι και $f : R \to R'$ ένας επιμορφισμός. Τότε η αντίστροφη συνολοσυνάρτηση f^{-1} της f είναι μία 1-1 και επί απεικόνιση μεταξύ των ιδεωδών του R' και των ιδεωδών του R που περιέχουν τον πυρήνα K της f.

Πριν διατυπώσουμε το επόμενο θεώρημα παρατηρούμε ότι το άθροισμα ιδεωδών είναι ιδεώδες και το άθροισμα υποδακτυλίου με ιδεώδες είναι υποδακτύλιος (το οποίο δεν ισχύει αν προσθέσουμε δύο υποδακτύλιους)

Πρόταση 19
Αν A είναι υποδακτύλιος ενός δακτυλίου R και I ένα ιδεώδες του R τότε το σύνολο

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

είναι υποδακτύλιος του R. Αν επιπλέον το A είναι ιδεώδες τότε θα είναι επίσης και το $A + I$.

Απόδειξη: Θεωρείστε $x, y \in A + I$. Τότε μπορούμε να γράψουμε $x = a + b, y = a' + b'$ όπου $a, a' \in A$ και $b, b' \in I$. Τότε $x - y = (a - a') + (b - b') \in A + I$ και $xy = (aa') + (bb' + ab' + ba') \in A + I$. □

[18] θεωρούμε A, B οποιαδήποτε υποσύνολα του R' με $f^{-1}(A) = f^{-1}(B)$. Ας δείξουμε ότι $A \subseteq B$. Αν $a \in A$ επειδή η f είναι επί μπορούμε να γράψουμε $a = f(x)$ για κάποιο $x \in R$. Προφανώς $x \in f^{-1}(A) = f^{-1}(B)$ δηλαδή θα υπάρχει $b \in B$ με $a = f(x) = b$ και άρα $a \in B$. Όμοια δείχνουμε ότι και $B \subseteq A$.

[19] Πράγματι, αν $a, b \in f(I)$ τότε $a = f(x), b = f(y)$ για κάποια $x, y \in I$. Επειδή $x - y \in I$ θα έχουμε ότι $a - b = f(x) - f(y) = f(x - y) \in f(I)$. Επίσης αν $r' \in R'$ επειδή ο f είναι επιμορφισμός θα υπάρχει $r \in R$ με $f(r) = r'$. Αλλά $xr' \in I$ και συνεπώς $ar' = f(x)r' = f(xr') \in f(I)$.

Θεώρημα 15 (Δεύτερο Θεώρημα Ομομορφισμού)
Έστω A να είναι ένας υποδακτύλιος ενός δακτυλίου R και I ιδεώδες του R, τότε

$$A/(A \cap I) \cong (A + I)/I$$

Απόδειξη: Ένα τυπικό στοιχείο του $A/(A \cap I)$ είναι το $X = x + A \cap I$ με $x \in A$. Θεωρείστε την απεικόνιση $f : A/(A \cap I) \to (A + I)/I$ με

$$f(x + (A \cap I)) = x + I$$

Η απεικόνιση είναι καλά ορισμένη αφού αν $x \in A$ τότε και $x \in A + I$. Εύκολα δείχνουμε ότι είναι ομομορφισμός και αρκεί να δείξουμε ότι είναι 1-1 και επί.

Για να δείξουμε ότι είναι 1-1 αρκεί να δείξουμε ότι ο πυρήνας της είναι το $A \cap I$. Πράγματι το μηδέν στον $A + I/I$ είναι το I και αν $f(x + (A \cap I)) = I$ τότε $x + I = I$ και συνεπώς $x \in I$. Αφού $x \in A$ θα έχουμε ότι $x \in A \cap I$ και συνεπώς $x + A \cap I = A \cap I$.

Για να δείξουμε ότι είναι επί, θεωρούμε ένα $x \in A + I$. Τότε $x = a + b$ με $a \in A, b \in I$. Αλλά $f(a + A \cap I) = a + (A + I) = x - b + (A + I) = x + (A + I)$. □

Τέλος έχουμε το ακόλουθο:

Θεώρημα 16 (Τρίτο Θεώρημα Ομομορφισμού)
(α) Αν $f : R \to R'$ είναι ένας επιμορφισμός δακτυλίων με $\mathrm{Ker}f = K$ και I ένα ιδεώδες του R με $K \subseteq I$. Τότε το $f(I)$ είναι ιδεώδες του R' και

$$R/I \cong R'/f(I)$$

(β) Αν K είναι ένα ιδεώδες σε ένα δακτύλιο R και I ένα ιδεώδες του R με $K \subseteq I$ τότε:

$$R/I \cong (R/K)/(I/K)$$

Απόδειξη: (α) Επαληθεύουμε πρώτα ότι το $f(I)$ είναι ιδεώδες στο R' και ορίζουμε μία απεικόνιση $g : R \to R'/f(I)$ με

$$g(x) = f(x) + f(I)$$

Η απεικόνιση αυτή είναι επί[20]. Επίσης επειδή $\mathrm{Ker}f \subseteq I$ θα έχουμε[21] ότι $f^{-1}(f(I)) = I$ που οδηγεί στο ότι $\mathrm{Ker}g = I$ αφού

$$\begin{aligned} g(x) = 0_{R'/f(I)} \Leftrightarrow & \\ & f(x) \in f(I) \Leftrightarrow \\ & x \in f^{-1}(f(I)) = I \end{aligned}$$

[20] Είτε το δείχνουμε απευθείας είτε παρατηρούμε ότι είναι σύνθεση δύο επιμορφισμών $g = \phi \circ f$ όπου η $\phi : R \to R/f(I)$ η κανονική απεικόνιση.

[21] Δες το Θεώρημα Αντιστοιχίας

Εφαρμόζουμε το Πρώτο Θεώρημα Ομομορφισμού και έχουμε άμεσα ότι $R/I \cong R'/f(I)$.

(β) Ας θεωρήσουμε τον φυσικό ομομορφισμό $\phi_K : R \to R/K$ με $\phi_K(x) = x + K$. Τότε $\phi_K(I) = I/K$, $\mathrm{Ker}\phi_K = K \subseteq I$ και εφαρόζουμε το (α). □

1.9.1 Ασκήσεις

Ασκηση 56 *Θεωρούμε ένα οποιοδήποτε πρώτο p και το σύνολο R όλων των ρητών $\frac{a}{b}$, $a \in \mathbb{Z}, b \in \mathbb{N} \setminus \{0\}$, $(a,b) = 1$ και $p \not| b$, με άλλα λόγια όλους τους ρητούς που αν γραφούν στη μορφή ανάγωγου κλάσματος ο p δεν διαιρεί τον παρανομαστή. Έστω I το σύνολο όλων των $\frac{a}{b} \in R$ (σε μορφή ανάγωγου κλάσματος) με $p|a$. Να δείξετε ότι το R είναι υποδακτύλιος του δακτυλίου των ρητών, το I είναι ένα ιδεώδες του και R/I είναι ισόμορφο με το $\mathbb{Z}_p$.*

Ασκηση 57 *Αν $f : R \to R'$ είναι ένας επιμορφισμός δακτυλίων να δείξετε ότι για οποιοδήποτε ιδεώδες I' του R' θα ισχύει:*

$$R/f^{-1}(I') \cong R'/I'$$

Ασκηση 58 *Έστω $\equiv$ μια σχέση ισοδυναμίας σε ένα δακτύλιο R που έχει τις παρακάτω ιδιότητες:*
1. Αν $a \equiv b$ και $a' \equiv b'$ τότε $a + b \equiv a' + b'$
2. Αν $a \equiv b$ και $a' \equiv b'$ τότε $ab \equiv a'b'$
Δείξτε ότι υπάρχει ένα μοναδικό ιδεώδες I στο δακτύλιο που να ορίζει την σχέση αυτή δηλαδή $a \equiv b \Leftrightarrow a - b \in I$.

Ασκηση 59 *Έστω R ένας δακτύλιος και I ένα ιδεώδες του. Να δείξετε ότι: Ο R/I δεν έχει διαιρέτες του 0 αν και μόνο αν*

$$ab \in I \Rightarrow a \in I \ \text{ είτε } \ b \in I$$

Ασκηση 60 *Έστω R ένας δακτύλιος και I ένα ιδεώδες του. Να δείξετε ότι: Ο R/I ειναι αντιμεταθετικός αν και μόνο αν*

$$\text{Για κάθε } \ a, b \in R, ab - ba \in I$$

Ασκηση 61 *Έστω R ένας δακτύλιος και I ένα ιδεώδες του. Να δείξετε ότι: Ο R/I έχει μονάδα αν και μόνο αν*

$$\text{Υπάρχει } \ e \in R \text{τέτοιο ώστε για οποιοδήποτε } \ \ a \in R, ae - a, ea - a \in I$$

Ασκηση 62 *Έστω R ένας δακτύλιος και έστω N το σύνολο των μηδενοδύναμων στοιχείων του, δηλαδή*

$$N = \{x \in R : \text{Υπάρχει ακέραιος } \ n \geq 1 \text{ με } x^n = 0\}$$

Να δείξετε ότι το N είναι ιδεώδες του R και ότι ο δακτύλιος R/N δεν έχει μηδενοδύναμα στοιχεία.

1.10 Μεγιστικά Ιδεώδη-Πρώτα ιδεώδη

Ας ξεκινήσουμε με ένα απλό λήμμα:

Λήμμα 1
Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα. Τότε ένα στοιχείο του a είναι αντιστρέψιμο αν και μόνο αν το ιδεώδες (a) που παράγει το a είναι όλος ο δακτύλιος R.

Απόδειξη: Ας θυμηθούμε ότι

$$(a) = \{ar : r \in R\}$$

Αν το a αντιστρέφεται τότε θα υπάρχει ένα $x \in R$ με $ax = 1$. Αλλά τότε $ax = 1 \in (a)$ που συνεπάγεται ότι $(a) = R$.

Αντίστροφα, αν $(a) = R$ τότε $1 \in (a)$ οπότε θα υπάρχει $r \in R$ με $ar = 1$, δηλαδή το a αντιστρέφεται. □

Από αυτό θα έχουμε άμεσα ότι:

Πρόταση 20
Ένας αντιμεταθετικός δακτύλιος με μονάδα είναι σώμα αν και μόνο δεν έχει τετριμμένα ιδεώδη.

Ορισμός 33
Ένα γνήσιο ιδεώδες M ενός δακτυλίου R θα λέγεται ***μεγιστικό ιδεώδες*** *αν δεν υπάρχει γνήσιο ιδεώδες που να το περιέχει διαφορετικό από αυτό. Με άλλα λόγια το M είναι μεγιστικό αν $M \neq R$ και αν το I είναι ιδεώδες με $M \subseteq I$ τότε $I = M$ ή $I = R$.*

Αναφέρουμε το παρακάτω Θεώρημα χωρίς απόδειξη:

Θεώρημα 17 (Θεώρημα Krull-Zorn)
Κάθε γνήσιο ιδεώδες ενός δακτυλίου με μονάδα περιέχεται σε μεγιστικό ιδεώδες.

Τα μεγιστικά ιδεώδη του $\mathbb{Z}$ είναι ακριβώς αυτά που παράγονται από τους πρώτους αριθμούς, δηλαδή τα $(p) = \{kp : k \in \mathbb{Z}\}$. Από όλους τους δακτύλιους πηλίκο $\mathbb{Z}_n = \mathbb{Z}/(n)$ αυτοί που είναι σώματα είναι ακριβώς αυτοί που παράγονται από τα μεγιστικά ιδεώδη του $\mathbb{Z}$. Αυτό δεν είναι σύμπτωση.

Το επόμενο θεώρημα είναι ένα από τα πιο σημαντικά στη Θεωρία Δακτυλίων. Η σημασία του θα φανεί κυρίως στη Θεωρία Σωμάτων.

Θεώρημα 18
Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα και I ένα γνήσιο ιδεώδες του. Τότε ο δακτύλιος R/I είναι σώμα αν και μόνο αν το I είναι μεγιστικό ιδεώδες.

Απόδειξη: Ας υποθέσουμε ότι το I είναι μεγιστικό ιδεώδες του R. Το R/I είναι αντιμεταθετικός δακτύλιος με μονάδα αφού και το R είναι και η μονάδα του είναι το $1+I$.

Ας θεωρήσουμε την κανονικά απεικόνιση $\phi : R \to R/I$, που είναι επιμοφισμός και ας θυμηθούμε το Θεώρημα της Αντιστοιχίας. Η ϕ^{-1} είναι μια 1-1 και επί απεικόνιση από τα ιδεώδη του R/I στα ιδεώδη του R που περιέχουν το I. Αλλά τα τελευταία είναι μόνο τα I, R που σημαίνει ότι το R/I έχει ακριβώς δύο ιδεώδη που αναγκαστικά θα είναι τα τετριμμένα. Με άλλα λόγια το R/I δεν έχει μη τετριμμένα ιδεώδη και από την Πρόταση 33 θα είναι σώμα.

Ο ίδιος συλλογισμός μας δείχνει και το αντίστροφο (άσκηση) □

Μια άλλη σημαντική κατηγορία ιδεωδών εκτός από τα μεγιστικά ιδεώδη είναι αυτή των πρώτων ιδεωδών.

Ορισμός 34

Ένα ιδεώδες I ενός δακτυλίου R θα λέγεται ***πρώτο ιδεώδες*** *αν $ab \in I$ συνεπάγεται ότι $a \in I$ είτε $b \in I$.*

Η επόμενη πρόταση είναι άμεση συνέπεια του ορισμού.

Πρόταση 21

Ένας αντιμεταθετικός δακτύλιος με μονάδα είναι ακέραια περιοχή αν και μόνο αν το (0) είναι πρώτο ιδεώδες.

Ένας χαρακτηρισμός των πρώτων ιδεωδών ενός αντιμεταθετικού δακτύλιου με μονάδα ανάλογος με αυτόν που μας έδωσε το Θεώρημα 18 δίνεται από το ακόλουθο:

Θεώρημα 19

Έστω R αντιμεταθετικός δακτύλιος με μονάδα. Ένα ιδεώδες I του R είναι πρώτο αν και μόνο αν το R/I είναι ακέραια περιοχή.

Απόδειξη: Ας υποθέσουμε ότι το I είναι πρώτο ιδεώδες ενός αντιμεταθετικού δακτύλιου με μονάδα R. Για να δείξουμε ότι το R/I είναι ακέραια περιοχή πρέπει να δείξουμε ότι αν το γινόμενο δύο στοιχείων του ειναι μηδέν ένα από αυτά τουλάχιστον θα είναι μηδέν. Με άλλα λόγια αν $(a+I)(b+I) = I$ πρέπει $a+I = I$(ισοδύναμα $a \in I$)) είτε $b+I = I$(ισοδύναμα $b \in I$).Αλλά αν $(a+I)(b+I) = ab+I = I$ τότε $ab \in I$ και αφού το I είναι πρώτο ιδεώδες θα έχουμε ότι είτε $a \in I$ είτε $b \in I$. Για το αντίστροφο απλά αντιστρέφουμε τον προηγούμενο συλλογισμό. □

Θεώρημα 20

Κάθε μεγιστικό ιδεώδες ενός αντιμεταθετικού δακτύλιου με μονάδα είναι πρώτο ιδεώδες.

Απόδειξη: Άμεση συνέπεια των Θεωρημάτων 18 και 19 □

Παράδειγμα 15 *Αν θεωρήσουμε τον δακτύλιο $\mathbb{Z} \times \mathbb{Z}$ με $(m,n)+(m',n') = (m+m', n+n')$, $(m,n)(m',n') = (mm', nn')$ τότε το $\mathbb{Z} \times \{0\}$ είναι πρώτο αλλά όχι μεγιστικό ιδεώδες.*

Παράδειγμα 16 *Ονομάζουμε* ***δακτύλιο του Gauss*** *το δακτύλιο*

$$G = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$$

που είναι μεταθετικός δακτύλιος με μονάδα υποδακτύλιος του δακτυλίου των μιγαδικών αριθμών. Τα στοιχεία του λέγονται και ***ακέραιοι του Gauss****. Έστω n ένας θετικός ακέραιος αριθμός και ας ορίσουμε*

$$I_n = \{a + bi : n|a \text{ και } n|b\}$$

Τα I_n είναι ιδεώδη. Το I_3 είναι μεγιστικό ιδεώδες. Πράγματι, ας υποθέσουμε ότι το $I_3 \subseteq M$ με M ιδεώδες διαφορετικό από αυτό. Ας πάρουμε ένα $x + iy \in M \setminus I_3$. Τότε $3 \not| x$ είτε $3 \not| y$. Αλλά τότε $3 \not| x^2 + y^2$ (γιατί;). Ο αριθμός $t = x^2 + y^2 = (x + iy)(x - iy) \in M$ αφού $x + iy \in M$.

Αφού $(3, t) = 1$ θα υπάρχουν a, b με $3a + bt = 1$. Τώρα $3a \in M$ αφού $3 \in M$ και $bt \in M$ αφού $t \in M$. Άρα $1 \in M$ και συνεπώς $M = G$ που σημαίνει ότι το I_3 είναι μεγιστικό.

Παρατηρείστε τώρα ότι $5 = (2 + i)(2 - i)$ και $5 \in I_5, 2 + i \notin I_5, 2 - i \notin I_5$, δηλαδή το I_5 δεν είναι πρώτο ιδεώδες άρα ούτε και μεγιστικό.

1.10.1 Ασκήσεις

Ασκηση 63 *Αποδείξτε την αντίστροφη κατεύθυνση του Θεωρήματος 18.*

Ασκηση 64 *Να δείξετε ότι τα μόνα ιδεώδη του $\mathbb{Z}$ είναι αυτά της μορφής (n) με n φυσικός αριθμός και ότι ένα ιδεώδες του $\mathbb{Z}$ είναι μεγιστικό αν και μόνο αν παράγεται από πρώτο αριθμό.*

Ασκηση 65 *Ας θεωρήσουμε το δακτύλιο του Gauss, δηλαδή το δακτύλιο*

$$G = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$$

που είναι μεταθετικός δακτύλιος με μονάδα υποδακτύλιος του δακτυλίου των μιγαδικών αριθμών. Έστω

$$I_3 = \{a + bi : 3|a \text{ και } 3|b$$

Να αποδείξετε ότι ο δακτύλιος G/M_3 είναι ένα σώμα που έχει ακριβώς 9 στοιχεία.

Ασκηση 66 *Στο G να θεωρήσετε το $M = \{z(2 + i) : z \in G\}$. Να αποδείξετε ότι*

$$G/M \cong \mathbb{Z}_5$$

Ασκηση 67 *Έστω*

$$\mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

και

$$M = \{a + b\sqrt{2} \in \mathbb{Z}(\sqrt{2}) : 5|a, 5|b\}$$

Να αποδείξετε ότι το $\mathbb{Z}(\sqrt{2})/M$ είναι ένα σώμα με 25 στοιχεία.

1.11 Θεωρία Διαιρετότητας σε ακέραιες περιοχές

Στην παράγραφο αυτή θα επιχειρήσουμε να επεκτείνουμε την θεωρία διαιρετότητας που αναπτύξαμε στο $\mathbb{Z}$ σε μία αφηρημένη ακέραια περιοχή. Όλοι οι δακτύλιοι που θα θεωρούμε σε αυτή την παράγραφο θα είναι ακέραιες περιοχές. Στη «θεωρία διαιρετότητας» σημαντικό ρόλο παίζουν τα ιδεώδη της ακέραιας περιοχής και κυρίως τα ιδεώδη που παράγονται από ένα πεπερασμένο πλήθος στοιχείων $a_1, a_2, \dots a_n$ της ακέραιας περιοχής. Θυμίζουμε ότι τα **κύρια ιδεώδη** μίας ακέραιας περιοχής R είναι τα ιδεώδη που παράγονται από ένα στοιχείο, δηλαδή αυτά της μορφής

$$(a) = \{ar : r \in R\}$$

Επίσης θυμίζουμε ότι το ιδεώδες που παράγουν τα $a_1, a_2, \dots a_n$ είναι το σύνολο όλων των στοιχείων της μορφής $r_1a_1 + \cdots + r_na_n : r_1, \dots, r_n \in R$. Τα στοιχεία αυτά ονομάζονται και οι **συνδυασμοί** των $a_1, a_2, \dots a_n$.

$$(a_1, a_2, \dots a_n) = \{r_1a_1 + \cdots + r_na_n : r_1, \dots, r_n \in R\}$$

Παρατηρείστε επίσης ότι:

$$(a_1) \cap \cdots \cap (a_n) \subseteq (a_1, \dots, a_n)$$

Ξεκινάμε με ένα προφανή ορισμό:

Ορισμός 35
*Έστω a, b δύο μη μηδενικά στοιχεία μίας ακέραιας περιοχής R. Θα λέμε ότι a το **διαιρεί** το b αν υπάρχει $c \in R$ τέτοιο ώστε $b = ac$. Σε αυτή την περίπτωση θα γράφουμε $a|b$. Αν $a|b$ θα λέμε επίσης ότι το b **διαιρείται** από το a. Θα θεωρούμε ότι το $0|a$ για κάθε $a \in R$.*

Μία ισοδύναμη διατύπωση στην γλώσσα των ιδεωδών είναι η παρακάτω:

Πρόταση 22
Το στοιχείο a διαιρεί το b αν και μόνο αν $(a) \subseteq (b)$

$$a|b \Leftrightarrow (b) \subseteq (a) \tag{1.6}$$

Απόδειξη:

$$a|b \quad \Longleftrightarrow \exists r : b = ar \iff b \in (a) \iff \forall r \;\; br \in (a) \iff (b) \subseteq (a)$$

□

Ορισμός 36
*Δύο στοιχεία a, b μίας ακέραιας περιοχής R θα λέγονται **ομόλογα** (ως προς την διαιρετότητα) αν το ένα διαιρεί το άλλο ή ισοδύναμα αν τα ιδεώδη που παράγουν συμπίπτουν.*

Θα γράφουμε $a \sim b$ αν τα a, b είναι ομόλογα. Η σχέση αυτή είναι φανερά σχέση ισοδυναμίας σε μία ακέραια περιοχή [22]. Μερικές απλές παρατηρήσεις σχετικά με τις παραπάνω έννοιες τις συνοψίζουμε σε μία πρόταση:

Πρόταση 23
Έστω R μία ακέραια περιοχή.
1. Ένα στοιχείο της R είναι αντιστρέψιμο αν και μόνο αν είναι ομόλογο του 1.
2. Δύο στοιχεία a, b είναι ομόλογα αν και μόνο αν υπάρχει ένα αντιστρέψιμο στοιχείο ϵ με $a = \epsilon b$.

Αφού τα αντιστρέψιμα στοιχεία είναι ακριβώς αυτά που είναι ομόλογα με τη μονάδα θα τα λέμε και *μοναδιαία*.

Σαν παράδειγμα αναφέρουμε ότι στο δακτύλιο των ακεραίων του Gauss τα μοναδιαία στοιχεία είναι τα $1, -1, i, -i$ και μόνο αυτά.

Συνεχίζοντας την ανάπτυξη μίας «γενικής θεωρίας διαιρετότητας» εισάγουμε τις έννοιες του μέγιστου κοινού διαιρέτη και του ελάχιστου κοινού πολλαπλασίου[23].

Ορισμός 37 *Έστω $a_1, a_2, \ldots a_n$ μη μηδενικά στοιχεία μίας ακέραιας περιοχής R. Ένα στοιχείο $d \neq 0$ θα λέγεται κοινός διαιρέτης των $a_1, a_2, \ldots a_n$ αν διαιρεί το κάθε ένα από αυτά και* ***μέγιστος κοινός διαιρέτης*** *των $a_1, a_2, \ldots a_n$ αν*
(α) Το d είναι κοινός διαιρέτης των $a_1, a_2, \ldots a_n$.
(β) Κάθε άλλος κοινός διαιρέτης d' των $a_1, a_2, \ldots a_n$ διαιρεί τον d.

Ένα στοιχείο $m \neq 0$ θα λέγεται κοινό πολλαπλάσιο των $a_1, a_2, \ldots a_n$ αν διαιρείται από το κάθε ένα από αυτά και θα λέγεται ***ελάχιστο κοινό πολλαπλάσιο*** *των $a_1, a_2, \ldots a_n$ αν*
(α) Το d είναι κοινό πολλαπλάσιο των $a_1, a_2, \ldots a_n$.
(β) Κάθε άλλο κοινό πολλαπλάσιο m' των $a_1, a_2, \ldots a_n$ διαιρείται από τον m.

Παρατηρείστε ότι οι ορισμοί είναι σχεδόν ίδιοι με αυτούς που είχαμε στο δακτύλιο των ακεραίων με τη διαφορά ότι εκεί ο μέγιστος κοινός διαιρέτης θέλαμε να είναι θετικός αριθμός. Αυτή η επιπλέον συνθήκη και το γεγονός ότι στο $\mathbb{Z}$ τα μόνα αντιστρέψιμα στοιχεία είναι τα $1, -1$ μας εξασφάλιζε την μοναδικότητα του μέγιστου κοινού διαιρέτη (και αντίστοιχα του ελάχιστου κοινού πολλαπλάσιου). Σε μία ακέραια περιοχή δεν έχουμε βέβαια ούτε γραμμική διάταξη και πιθανότατα πολλά (ή ακόμα και άπειρα) αντιστρέψιμα στοιχεία οπότε δεν μπορούμε να έχουμε μοναδικότητα αυτών των εννοιών. Έχουμε όμως μοναδικότητα ως προς τη σχέση ισοδυναμίας $\sim$ που ορίσαμε λίγο πριν.

[22] και γενικά σε ένα δακτύλιο αφού οι ορισμοί αυτοί μπορούν να επεκταθούν σε οποιοδήποτε δακτύλιο

[23] Παρατηρείστε τον δυϊσμό των δύο αυτών εννοιών όπου η έννοια του ελάχιστου κοινού πολλαπλάσιου προκύπτει αν στον ορισμό του μέγιστου κοινού διαιρέτη αντικαταστήσουμε το «διαιρεί» με «διαιρείται»

Αν $a_1, a_2, \ldots a_n$ είναι μη μηδενικά στοιχεία τότε οι μέγιστοι κοινοί διαιρέτες τους (αν υπάρχουν) θα είναι όλοι ομόλογοι μεταξύ τους. Με άλλα λόγια:
Αν d είναι ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \ldots a_n$ τότε κάθε άλλος μέγιστος κοινός διαιρέτης d' θα γράφεται σαν $d' = ed$ με e μοναδιαίο στοιχείο, αλλά και κάθε στοιχείο της μορφής ed με e μοναδιαίο θα είναι μέγιστος κοινός διαιρέτης των $a_1, a_2, \ldots a_n$.
Ανάλογη παρατήρηση ισχύει και για το ελάχιστο κοινό πολλαπλάσιο.

Μέγιστοι κοινοί διαιρέτες δεν υπάρχουν απαραίτητα σε κάθε ακέραια περιοχή. Για να προχωρήσουμε περισσότερο πρέπει να περιοριστούμε σε περιοχές όπου μπορούμε να εξασφαλίσουμε την ύπαρξη μέγιστου κοινού διαιρέτη. Θα στραφούμε κυρίως στη μελέτη του μέγιστου κοινού διαιρέτη παρά σε αυτήν του ελάχιστου κοινού πολλαπλάσιου για δύο λόγους. Η έννοια του μέγιστου κοινού διαιρέτη είναι πολύ πιο σημαντική για να μελετάμε προβλήματα διαιρετότητας και επίσης αν γνωρίζουμε ότι υπάρχει ο μέγιστος κοινός διαιρέτης ξέρουμε ότι υπάρχει και ελάχιστο κοινό πολλαπλάσιο. Για να το δείξουμε αυτό θα δείξουμε πρώτα ένα λήμμα.

Λήμμα 2 *Έστω $a_1, \ldots, a_n, r$ μη μηδενικά στοιχεία μίας ακέραιας περιοχής. Τότε:*

(α) *Αν υπάρχει ένας μέγιστος κοινός διαιρέτης d των $ra_1, \ldots, ra_n$ τότε υπάρχει ένας μέγιστος κοινός διαιρέτης d' των $a_1, \ldots, a_n$ με $d = rd'$.*

(β) *Αν υπάρχει ένα ελάχιστο κοινό πολλαπλάσιο m των $a_1, \ldots, a_n$ τότε υπάρχει ένα ελάχιστο κοινό πολλαπλάσιο m' των $ra_1, \ldots, ra_n$ με $m' = rm$.*

Απόδειξη: (α) Ας υποθέσουμε ότι υπάρχει ένας μέγιστος κοινός διαιρέτης d των $ra_1, \ldots, ra_n$. Το r είναι ένας κοινός διαιρέτης των $ra_1, \ldots, ra_n$ άρα διαιρεί το d που σημαίνει ότι υπάρχει d' με $d = rd'$. Θα δείξουμε ότι ο d' είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$. Φανερά είναι κοινός διαιρέτης. Μένει να δείξουμε ότι κάθε άλλος κοινός διαιρέτης t των $a_1, \ldots, a_n$ θα τον διαιρεί. Ο rt είναι κοινός διαιρέτης των $ra_1, \ldots, ra_n$ και συνεπώς $rt|d$ δηλαδή $rt|rd'$. Αλλά τότε $t|d'$, και δείξαμε αυτό που θέλαμε.
Το (β) το αφήνουμε σαν άσκηση. □

Σημείωση 2 *Από το προηγούμενο Λήμμα αν υπάρχει μέγιστος κοινός διαιρέτης των $ra_1, \ldots, ra_n$ θα υπάρχει και μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$. Το αντίστροφο ΔΕΝ ισχύει πάντοτε. Επίσης αν γνωρίζουμε την ύπαρξη ελάχιστου κοινού πολλαπλάσιου για τους $a_1, \ldots, a_n$ ξέρουμε ότι υπάρχει και για τους $ra_1, \ldots, ra_n$. Κι εδώ ΔΕΝ ισχύει πάντοτε το αντίστροφο. Αυτό μας δείχνει το επόμενο παράδειγμα.*

Παράδειγμα 17 *Ας θεωρήσουμε το δακτύλιο*

$$R = \mathbb{Z}(\sqrt{-5}) = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

που είναι ακέραια περιοχή σαν υποδακτύλιος του σώματος των μιγαδικών[24]*. Είναι χρήσιμο να ορίσουμε και μία εκτίμηση $N(x)$ που σε κάθε στοιχείο x του R θα αντιστοιχεί ένα θετικό ακέραιο $N(x)$ και η οποία να σέβεται τον πολλαπλασιασμό:*

$$N(xy) = N(x)N(y) \tag{1.7}$$

Αυτή ορίζεται από τη σχέση

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 \tag{1.8}$$

Δεν είναι δύσκολο να δούμε ότι με αυτό τον ορισμό ικανοποιείται η σχέση 1.7 λόγω της γενικής ταυτότητας[25] *:*

$$(a^2 + mb^2)(c^2 + md^2) = (ac - mbd)^2 + m(ad + bc)^2 \tag{1.9}$$

Αν για κάποια στοιχεία x, y του R συνέβαινε $xy = 1$ λόγω της σχέσης 1.7 θα είχαμε ότι $N(x)N(y) = 1$ άρα θα έπρεπε $N(x) = N(y) = 1$. Αλλά η σχέση $a^2 + 5b^2 = 1$ στους ακέραιους σημαίνει ότι $a = \pm 1, b = 0$ και καταλήγουμε ότι τα μόνα μοναδιαία (=αντιστρέψιμα) στοιχεία του R είναι τα 1, -1. Γενικότερα θα έχουμε[26]*:*

$$a|b \Rightarrow N(a)|N(b)$$

Ας θεωρήσουμε τους αριθμούς

$$A = 3, \qquad B = 2 + \sqrt{-5}$$

Είναι εύκολο να δούμε ότι:

Υπάρχουν μέγιστοι κοινοί διαιρέτες των A, B στο $\mathbb{Z}(\sqrt{-5})$ και είναι οι ± 1.

Ας δούμε τώρα αν υπάρχουν μέγιστοι κοινοί διαιρέτες των αριθμών

$$3A = 9, \quad 3B = 6 + 3\sqrt{-5}$$

Θα έχουμε

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$
$$6 + 3\sqrt{-5} = 3 \cdot (2 + \sqrt{-5})$$

Δεν είναι δύσκολο να δούμε[27] *ότι οι μόνοι διαιρέτες του 9 είναι οι*
$\pm 1, \pm 3, \pm(2 + \sqrt{-5}), \pm(2 - \sqrt{-5}), \pm 9$

[24] δηλαδή οι πράξεις είναι οι συνήθεις πράξεις μιγαδικών αριθμών

[25] Για $m = 5$

[26] αν $a|b$ τότε για κάποιο c θα είχαμε ότι $b = ac$ και από την σχέση 1.7, $N(b) = N(a)N(c)$ άρα $N(a)|N(b)$

[27] Αν ο $a + b\sqrt{-5}$ διαιρεί τον 9 τότε θα πρέπει $a^2 + 5b^2|81$ δηλαδή θα πρέπει $a^2 + 5b^2 = 1$ ή $a^2 + 5b^2 = 3$ ή $a^2 + 5b^2 = 9$ ή $a^2 + 5b^2 = 27$ ή $a^2 + 5b^2 = 81$

και του $6+3\sqrt{-5}$ *οι*
$\pm 1, \pm 3, \pm(2+\sqrt{-5}), \pm(6+3\sqrt{-5})$
και συνεπώς ο ***κοινοί*** *διαιρέτες είναι οι*

$$\pm 1, \pm 3, \pm(2+\sqrt{-5})$$

Κανείς όμως από αυτούς δεν μπορεί να διαιρείται από ΟΛΟΥΣ τους υπόλοιπους κοινούς διαιρέτες και καταλήγουμε ότι

Δεν υπάρχει μέγιστος κοινός διαιρέτης των $3A=9,\ 3B=6+3\sqrt{-5}$ ***στο*** $\mathbb{Z}(\sqrt{-5})$**.**

Ας θυμηθούμε εδώ ότι αν υπάρχει κάποιος μέγιστος κοινός διαιρέτης d για κάποια στοιχεία $a_1, \ldots, a_n$ μιας ακέραιας περιοχής τότε αυτός δεν μεν είναι μοναδικός αλλά καθορίζει όλους τους υπόλοιπους που είναι ακριβώς όσοι είναι ομόλογοι με αυτόν, δηλαδή της μορφής ed με e ένα μοναδιαίο (=αντιστρέψιμο) στοιχείο[28].

Το προηγούμενο Λήμμα μας έλεγε ότι αν γνωρίζουμε την ύπαρξη ενός μέγιστου κοινού διαιρέτη d για τα $ra_1, ra_2, \ldots, ra_n$ την γνωρίζουμε και για τα $a_1, a_2, \ldots, a_n$ και μάλιστα ο d είναι της μορφής rd' με d' μέγιστος κοινός διαιρέτης των $a_1, a_2, \ldots, a_n$. Το αντίστροφο δεν ισχύει πάντοτε, όπως το προηγούμενο παράδειγμα μας έδειξε.

Το επόμενο Λήμμα μας λέει ότι **αν γνωρίζουμε** την ύπαρξη μέγιστου κοινού διαιρέτη για οποιαδήποτε (μη μηδενικά) στοιχεία μίας ακέραιας περιοχής τότε ο κάθε κοινός διαιρέτης d των $a_1, a_2, \ldots, a_n$ **καθορίζει πλήρως** τους μέγιστους κοινούς διαιρέτες των $ra_1, ra_2, \ldots, ra_n$ σαν όλους αυτούς που είναι ομόλογοι με τον rd. Αλλά και αντίστροφα αν ξέρουμε μέγιστο κοινό διαιρέτη για τους $ra_1, ra_2, \ldots, ra_n$ αυτός είναι πολλαπλάσιο του r και καθορίζει έτσι όλους τους μέγιστους κοινούς διαιρέτες των $a_1, ra_2, \ldots, a_n$ με τη σχέση[29]

$$MK\Delta(ra_1, \ldots, ra_n) = rMK\Delta(a_1, \ldots, a_n) \tag{1.10}$$

Λήμμα 3

Αν R είναι μία ακέραια περιοχή με την ιδιότητα για οποιαδήποτε δύο μη μηδενικά στοιχεία της να υπάρχει ένας μέγιστος κοινός διαιρέτης τους τότε για οποιαδήποτε μη μηδενικά στοιχεία $a, b, r \in R$ ισχύει το εξής:

Ο d είναι μέγιστος κοινός διαιρέτης των a, b αν και μόνο αν ο dr είναι μέγιστος κοινός διαιρέτης των ra, rb.

[28] Κάτω από αυτό το πρίσμα μπορούμε να μιλάμε για ένα μέγιστο κοινό διαιρέτη σα να είναι μοναδικός.

[29] ΠΡΟΣΟΧΗ όμως, η σχέση αυτή ισχύει σε ακέραιες περιοχές που γνωρίζουμε ότι όποια στοιχεία και να πάρουμε αυτά έχουν μέγιστο κοινό διαιρέτη.

Απόδειξη: Ας υποθέσουμε ότι d είναι μέγιστος κοινός διαιρέτης των a, b τότε ο rd είναι ένας κοινός διαιρέτης των ra, rb. Ας υποθέσουμε ότι ο d' είναι ένας μέγιστος κοινός διαιρέτης των ra, rb (που υπάρχει λόγω της υπόθεσης ότι δύο οποιαδήποτε μη μηδενικά στοιχεία έχουν μέγιστο κοινό διαιρέτη). Από το Λήμμα 2 θα υπάρχει μέγιστος κοινός διαιρέτης d_1 των a, b με $d_1 = rd'$. Δύο οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των a, b είναι ομόλογοι μεταξύ τους δηλαδή $d_1 = ed$ για κάποιο αντιστρέψιμο στοιχείο e. Αλλά τότε ο dr θα είναι ομόλογος με τον $d_1 r = d'$ και συνεπώς μέγιστος κοινός διαιρέτης.

Με τον ίδιο συλλογισμό αποδεικνύεται και το αντίστροφο. □

Τελειώνουμε αυτή την παράγραφο δείχνοντας ότι σε ακέραιες περιοχές που ξέρουμε ότι υπάρχει μέγιστος κοινός διαιρέτης για οποιαδήποτε δύο μη μηδενικά στοιχεία τους τότε υπάρχει μέγιστος κοινός διαιρέτης και ελάχιστο κοινό πολλαπλάσιο για οσοδήποτε πολλά μη μηδενικά στοιχεία.

Πρόταση 24
(α) *Αν σε μία ακέραια περιοχή υπάρχει μέγιστος κοινός διαιρέτης δύο οποιωνδήποτε μη μηδενικών στοιχείων της τότε θα υπάρχει μέγιστος κοινός διαιρέτης οποιουδήποτε(πεπερασμένου) πλήθους μη μηδενικών στοιχείων της.*
(β) *Αν σε μία ακέραια περιοχή υπάρχει ελάχιστο κοινό πολλαπλάσιο δύο οποιωνδήποτε μη μηδενικών στοιχείων της τότε θα υπάρχει το ελάχιστο κοινό πολλαπλάσιο οποιουδήποτε(πεπερασμένου) πλήθους μη μηδενικών στοιχείων της.*
(γ) *Αν σε μία ακέραια περιοχή υπάρχει μέγιστος κοινός διαιρέτης (αντίστοιχα, ελάχιστο κοινό πολλαπλάσιο) δύο οποιωνδήποτε μη μηδενικών στοιχείων της τότε θα υπάρχει ελάχιστο κοινό πολλαπλάσιο (αντίστοιχα, μέγιστος κοινός διαιρέτης) δύο (άρα από **(α)** και **(β)**, και οποιουδήποτε πλήθους) μη μηδενικών στοιχείων της.*

Απόδειξη: (α) Έστω R μία ακέραια περιοχή στην οποία υπάρχει μέγιστος κοινός διαιρέτης δύο οποιωνδήποτε μη μηδενικών στοιχείων της. Θα δείξουμε με επαγωγή στο $n \geq 2$ ότι αν έχουμε $a_1, \ldots, a_n$ μη μηδενικά στοιχεία της R θα υπάρχει ο μέγιστος κοινός διαιρέτης τους. Για $n = 2$ αυτό είναι η υπόθεσή μας. Ας υποθέσουμε ότι το γνωρίζουμε για κάποιο $n-1 \geq 2$ και ας θεωρήσουμε $a_1, \ldots, a_n$ μη μηδενικά στοιχεία της R.

Έστω d_0 να είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_{n-1}$, ο οποίος υπάρχει από την επαγωγική μας υπόθεση, και d να είναι μέγιστος κοινός διαιρέτης των d_0, a_n. Θα δείξουμε ότι ο d είναι μέγιστος κοινός των $a_1, \ldots, a_{n-1}, a_n$.

Φανερά ο d είναι κοινός διαιρέτης. Ας υποθέσουμε ότι d' είναι ένας κοινός διαιρέτης των $a_1, \ldots, a_{n-1}, a_n$ τότε θα είναι και κοινός διαιρέτης των $a_1, \ldots, a_{n-1}$ και αφού ο d_0 είναι ο μέγιστος κοινός διαιρέτης αυτών των αριθμών θα έχουμε ότι $d'|d_0$. Συνεπώς ο d' είναι ένας κοινός διαιρέτης των d_0, a_n και αφού ο d είναι ο μέγιστος κοινός διαιρέτης των d_0, a_n θα έχουμε ότι $d'|d$, που σημαίνει ότι ο d είναι μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_{n-1}, a_n$.

Όμοια δείχνουμε και το **(β)**.

Για το **(γ)**: Ας υποθέσουμε έχουμε μία ακέραια περιοχή R όπου υπάρχει ο μέγιστος κοινός διαιρέτης δύο οποιωνδήποτε μη μηδενικών στοιχείων της. Ας θεωρήσουμε a, b μη μηδενικά στοιχεία της R και έστω d να είναι ένας μέγιστος κοινός διαιρέτης τους, οπότε για κάποια $a_1, b_1 \in R$ θα έχουμε ότι

$$a = da_1, b = db_1 \tag{1.11}$$

για κάποια $a_1, b_1 \in R$. Τότε αφού το $d \cdot 1$ είναι μέγιστος κοινός διαιρέτης των da_1, da_2 το Λήμμα 3 μας εξασφαλίζει ότι

(*) *Το 1 είναι μέγιστος κοινός διαιρέτης των* a_1, b_1.

Ισχυρίζομαι ότι:

(**) *Ο* $m = da_1a_2$ *είναι ελάχιστο κοινό πολλαπλάσιο των* a, b.

Αφού $m = ab_1 = a_1b$ προφανώς είναι κοινό πολλαπλάσιο. Αρκεί να δείξω ότι θα διαιρεί οποιοδήποτε άλλο κοινό πολλαπλάσιο m' των a, b. Θεωρούμε λοιπόν ένα τέτοιο m'. Τότε θα υπάρχουν x, y με $m' = xa = yb$ και από την 1.11

$$m' = xa = yb \Rightarrow xda_1 = ydb_1 \Rightarrow xa_1 = yb_1 \tag{1.12}$$

Λόγω της (*) το 1 είναι μέγιστος κοινός διαιρέτης των a_1, b_1 και συνεπώς από το Λήμμα 3 το y θα είναι μέγιστος κοινός διαιρέτης των ya_1, yb_1. Αλλά από την 1.12 έχουμε ότι ο a_1 είναι κοινός διαιρέτης των ya_1, yb_1 και συνεπώς θα διαιρεί τον y. Αλλά τότε ο m θα διαιρεί τον a'. □

Ορισμός 38
Θα ονομάζουμε μία ακέραια περιοχή R, μια ***ΜΚΔ-περιοχή*** *αν οποιαδήποτε δύο μη μηδενικά στοιχεία της R έχουν μέγιστο κοινό διαιρέτη.*

1.12 Ανάγωγα στοιχεία -Πρώτα στοιχεία- Ορισμός της Περιοχής μονοσήμαντης ανάλυσης

Κάθε στοιχείο a μιας ακέραιας περιοχής μπορεί να διασπαστεί σε γινόμενο με ένα τετριμένο τρόπο: $a = 1 \cdot a$, ή ακόμα $a = (-1) \cdot (-a)$ και γενικά

$$a = e \cdot (e^{-1}a), \quad e \text{ αντιστρέψιμο στοιχείο της } R \tag{1.13}$$

Εμείς ενδιαφερόμαστε για στοιχεία μίας ακέραιας περιοχής για τα οποία ο μόνος τρόπος να διασπαστούν σε γινόμενο είναι ο προηγούμενος. Τα στοιχεία αυτά τα λέμε ανάγωγα. Στο $\mathbb{Z}$ τα ανάγωγα στοιχεία είναι αυτά της μορφής $\pm p$ όπου p είναι πρώτος αριθμός.

Ορισμός 39 *Ένα μη μηδενικό στοιχείο p μίας ακέραιας περιοχής θα το ονομάζουμε:*
1. ***Ανάγωγο*** *αν δεν είναι μηδέν ή αντιστρέψιμο 1 και αν οποτεδήποτε ισχύει $p = ab$ τότε είτε το a είτε το b είναι αντιστρέψιμο.*
2. ***Πρώτο*** *αν δεν είναι μηδέν ή αντιστρέψιμο και οποτεδήποτε $p|ab$ τότε είτε $p|a$ είτε $p|b$.*

φανείς.

Η έννοια του πρώτου είναι πιο ισχυρή από αυτήν του ανάγωγου με την έννοια ότι τα **πρώτα στοιχεία είναι ανάγωγα**. Πράγματι, αν $p = ab$ και το p είναι πρώτο τότε είτε $p|a$ είτε $p|b$. Ας υποθέσουμε ότι $p|a$ δηλαδή ότι $a = pd$ για κάποιο d. Τότε $p = (db)p$ και αφού είμαστε σε ακέραια περιοχή θα έχουμε $db = 1$ δηλαδή το b είναι αντιστρέψιμο. Το αντίστροφο δεν ισχύει πάντοτε[30]:

Παράδειγμα 18 *Στο $\mathbb{Z}(\sqrt{-5})$ (και πάλι) δείξτε ότι το $2 + \sqrt{-5}$ είναι ανάγωγο αλλά όχι και πρώτο. (Υπόδειξη: Το $2 + \sqrt{-5}|3 \cdot 3$ αλλά είναι αδύνατον να διαιρεί το 3.)*

Αν ωστόσο η περιοχή μας είναι περιοχή ΜΚΔ (δηλαδή οποιαδήποτε a, b μη μηδενικά στοιχεία έχουν ένα μέγιστο κοινό διαιρέτη) τότε πρώτα και ανάγωγα στοιχεία συμπίπτουν.

Παρακάτω θα χαρακτηρίσουμε τα ανάγωγα και τα πρώτα στοιχεία μίας ακέραιας περιοχής στη γλώσσα των ιδεωδών.

Ορισμός 40
Ένα κύριο ιδεώδες (a) θα λέγεται ***μεγιστικό κύριο ιδεώδες*** *αν είναι γνήσιο ιδεώδες και δεν υπάρχει άλλο γνήσιο κύριο ιδεώδες που να το περιέχει γνήσια.*

Πρόταση 25
Έστω R μία ακέραια περιοχή και p ένα μη μηδενικό, μη αντιστρέψιμο στοιχείο. Τότε:
(1) *Το p είναι ανάγωγο αν και μόνο αν το ιδεώδες (p) είναι μεγιστικό κύριο ιδεώδες.*
(2) *Το p είναι πρώτο αν και μόνο αν το ιδεώδες (p) είναι πρώτο ιδεώδες.*

Απόδειξη:
(1): Ας υποθέσουμε ότι το p είναι ανάγωγο και ότι για κάποιο a ισχύει $(p) \subseteq (a)$. Τότε για κάποιο $r \in R$ θα ισχύει $p = ar$. Τότε είτε το a είτε το r θα είναι αντιστρέψιμο. Αν το a είναι αντιστρέψιμο τότε $(a) = R$. Αν πάλι το r είναι αντιστρέψιμο τότε $a = r^{-1}p$ και συνεπώς $a \in (p)$ οπότε $(a) \subseteq (p)$ δηλαδή $(a) = (p)$. Άρα τα μόνα κύρια ιδεώδη που μπορεί να περιέχουν το (p) είναι το R είτε ο εαυτός του, που σημαίνει ότι το (p) είναι μεγιστικό κύριο ιδεώδες.

[30] Στον δακτύλιο $\mathbb{Z}$ βέβαια η έννοιες αυτές συμπίπτουν

Αντίστροφα, ας υποθέσουμε ότι το (p) είναι μεγιστικό κύριο ιδεώδες και έστω ότι $p = ab$. Τότε θα έχουμε ότι $(p) \subseteq (a)$ και συνεπώς $(a) = (R)$ οπότε το a θα είναι αντιστρέψιμο είτε $(a) = (p)$ οπότε τα a, p θα είναι ομόλογα και το b θα είναι αναγκαστικά αντιστρέψιμο. Συνεπώς το p είναι ανάγωγο.
(2): Ας υποθέσουμε ότι το p είναι πρώτο στοιχείο και έστω $ab \in (p)$. Τότε $p|ab$ οπότε είτε $p|a$ οπότε $a \in (p)$ είτε $p|b$ οπότε $b \in (p)$ και δείξαμε ότι το (p) είναι πρώτο ιδεώδες.
Το αντίστροφο το αφήνουμε σαν άσκηση. □

Ορισμός 41 *Μία ακέραια περιοχή R θα ονομάζεται περιοχή μονοσήμαντης (ή μοναδικής) ανάλυσης αν ισχύουν οι παρακάτω δύο συνθήκες:*

(1) *Κάθε στοιχείο $a \in R$ που δεν είναι ούτε μηδενικό ούτε αντιστρέψιμο γράφεται σαν ένα γινόμενο $a = p_1 \dots p_n$ ανάγωγων στοιχείων του R.*

(2) *Η αναπαράσταση ενός μη αντιστρέψιμου μη μηδενικού στοιχείου a του R έχει μοναδική αναπαράσταση σαν γινόμενο ανάγωγων στοιχείων με την εξής έννοια: Αν $a = p_1 \cdots p_n = q_1 \cdots q_m$ είναι δύο αναπαραστάσεις του a σε γινόμενο πρώτων στοιχείων τότε $m = n$ και υπάρχει μία μετάθεση $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ τέτοια ώστε για κάθε $i \in \{1, \dots, n\}$ ο p_i είναι ομόλογος με τον $q_{\sigma(i)}$, δηλαδή $p_i = eq_{\sigma(i)}$ όπου e αντιστρέψιμο.*

Από τον ορισμό της περιοχής μονοσήμαντης ανάλυσης κάθε στοιχείο $a \in R$ μιας περιοχής μονοσήμαντης ανάλυσης είτε θα είναι το 0 είτε θα είναι αντιστρέψιμο είτε θα γράφεται κατά ουσιαστικά μοναδικό τρόπο σα γινόμενο ανάγωγων στοιχείων της περιοχής. Αν μαζέψουμε τους πρώτους που επαναλάμβονται σε μια αναπαράσταση ενός μη αντιστρέψιμου μη μηδενικού στοιχείου a τότε αυτό θα γράφεται στη μορφή

$$a = p_1^{n_1} \cdots p_k^{n_k} \tag{1.14}$$

όπου οι $p_1, \dots, p_k$ είναι πρώτοι μη ομόλογοι ανά δύο και τα $n_1, \dots, n_k$ θετικοί ακέραιοι αριθμοί.

Σε μια περιοχή μονοσήμαντης ανάλυσης τα ανάγωγα στοιχεία θα είναι και πρώτα. Πράγματι ας υποθέσουμε ότι το $p \in R$ είναι ανάγωγο στοιχείο και ότι διαιρεί το γινόμενο ab με $a, b \in R$. Μπορούμε να παραστήσουμε τα a, b σαν γινόμενα

$$a = up_1^{n_1} \dots p_k^{n_k} \tag{1.15}$$
$$b = vp_1^{m_1} \dots p_k^{m_k} \tag{1.16}$$

όπου:
1. Τα $p_1, \dots, p_k$ είναι ανάγωγα στοιχεία και τα u, v αντιστρέψιμα στοιχεία.

2. Τα $n_1, \ldots, n_k, m_1, dots, m_k$ είναι θετικοί ακέραιοι που μπορούν να πάρουν και την τιμή μηδέν αλλά αν $n_i = 0$ τότε $m_i \neq 0$ και αν $m_i = 0$ τότε $n_i \neq 0$.

Ας υποθέσουμε ότι το p είναι ανάγωγο στοιχείο του R και ότι $p|ab$. Λόγω των προηγουμένων το

$$ab = uvp^{n_1+m_1} \cdots p^{n_k+m_k} = uvp_1^{s_1} \cdots p_k^{s_k}$$

όπου $s_i \geq 1$ για κάθε $i = 1, \ldots, k$. Λόγω της μοναδικότητας της ανάλυσης σε γινόμενο πρώτων ο p πρέπει να είναι ανάλογος με κάποιο p_j από τους $p_1, \ldots, p_k$ που σημαίνει ότι είτε $p|a$ (αν $n_j \geq 1$) είτε $p|b$ (αν $m_j = 1$). Δείξαμε λοιπόν ότι

Καθε ανάγωγο στοιχείο μιας Περιοχής μονοσήμαντης Ανάλυσης είναι και πρώτος

Αν Θέσουμε $t_i = \min\{m_i, n_i\}$ για κάθε $i = 1, \ldots, k$ και

$$d = p_1^{t_1} \cdots p_k^{t_k}$$

φανερά ο t είναι κοινός διαιρέτης των a, b. Αν τώρα d' είναι ένας κοινός διαιρέτης των a, b τότε αν κάποια δύναμη πρώτου πρώτου p^t εμφανίζεται στην ανάλυση του d' θα πρέπει να υπάρχουν i και αντιστρέψιμο στοιχείο e με $p = ep_i$ και

$$\min\{n_i, m_i\} \leq t \tag{1.17}$$

Πράγματι το ότι ο p είναι ομόλογος με κάποιον από τους $p_1, \ldots, p_k$ προκύπτει από το μονοσήμαντο της ανάλυσης του a για παράδειγμα. Αν δεν ήταν κάποιος από αυτούς αφού $a = px$ για κάποιο $x \in R$, αναλύοντας το x θα είχαμε δύο αναλύσεις όπου στην μία εμφανίζεται ένας πρώτος που δεν είναι ομόλογος με κανένα πρώτο της άλλης ανάλυσης. Αν πάλι συνέβαινε -πχ- $p = p_i$ και $t > n_i$ τότε πάλι θα παραβιαζόταν το μονοσήμαντο της ανάλυσης του a ενώ αν $t|m_i$ θα παραβιαζόταν το μονοσήμαντο της ανάλυσης του b. Από την σχέση 1.17 που ισχύει για κάθε i έχουμε προφανώς ότι $d'|d$. Καταλήξαμε συνεπώς στο να δείξουμε την επόμενη:

Πρόταση 26 *Έστω R μία περιοχή μονοσήμαντης ανάλυσης. Τότε:*
(1) *Η R είναι ΜΚΔ-περιοχή.*
(2) *Κάθε ανάγωγο στοιχείο της R είναι πρώτο.*

1.12.1 Ασκήσεις

Ασκηση 68 *Στο $\mathbb{Z}(\sqrt{-5})$ δείξτε ότι τα $\pm(2 \pm \sqrt{-5})$ είναι ανάγωγα αλλά όχι πρώτα.*

Ασκηση 69 *Στο $\mathbb{Z}$ δείξτε ότι τα ανάγωγα στοιχεία είναι ακριβώς τα πρώτα στοιχεία.*

Ασκηση 70 *Να δείξετε ότι σε μία ΜΚΔ-περιοχή ισχύουν τα παρακάτω:*
1. Αν ο d, d' είναι μέγιστοι κοινοί διαιρέτες των a, b και $a = da_1, b = d'b_1$ τότε οι κοινοί διαιρέτες των a_1, b_1 είναι τα αντιστρέψιμα στοιχεία της R και μόνο αυτά.
2. Αν a, b, c μη μηδενικά στοιχεία της R και $a|bc$ και το 1 είναι μέγιστος κοινός διαιρέτης των a, c τότε $a|b$. Δείξτε με ένα παράδειγμα ότι αυτό δεν ισχύει γενικά σε ακέραιες περιοχές.

Ασκηση 71 *Δείξτε ότι το $\mathbb{Z}(\sqrt{-5}) = \{a+b\sqrt{-5} : a, b \in \mathbb{Z}\}$ είναι ακέραια περιοχή που δεν είναι ΜΚΔ-ακέραια περιοχή.*

Ασκηση 72 *Δείξτε ότι σε μία ΜΚΔ-περιοχή τα πρώτα και τα ανάγωγα στοιχεία συμπίπτουν.*

Ασκηση 73 *Ας υποθέσουμε ότι $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, είναι μη μηδενικά στοιχεία μίας ακέραιας περιοχής και ισχύει*

$$a_1b_1 = a_2b_2 = \cdots = a_nb_n = c$$

Να δείξετε τα παρακάτω:
(a) Αν υπάρχει μέγιστος κοινός διαιρέτης των $ra_1, \ldots, ra_n$ για κάθε $r \neq 0$ τότε θα υπάρχει ελάχιστο κοινό πολλαπλάσιο των $b_1, \ldots, b_n$

(a) Αν υπάρχει ελάχιστο κοινό πολλαπλάσιο των $a_1, \ldots, a_n$ τότε θα υπάρχει μέγιστος κοινός διαιρέτης των $b_1, \ldots, b_n$

1.13 Θεωρία διαιρετότητας σε περιοχές κυρίων ιδεωδών

Για να προχωρήσουμε πιο πολύ στην αφηρημένη θεωρία διαιρετότητας θέλουμε να έχουμε ακέραιες περιοχές που να έχουν ιδιότητες ανάλογες με αυτές που συναντάμε στους ακέραιους. Πιο συγκεκριμένα θα θέλαμε να ισχύουν οι παρακάτω δύο ιδιότητες:
1. *Για οποιαδήποτε μη μηδενικά στοιχεία $a_1, \ldots, a_n$, οποιουδήποτε πλήθους n, να υπάρχει μέγιστος κοινός διαιρέτης τους.*
2. Κάθε μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ να είναι ένας συνδυασμός αυτών των στοιχείων ή ισοδύναμα $d \in (a_1, \ldots, a_n)$

Ασκηση 74 *Δείξτε ότι*
(1) *Ο d είναι κοινός διαιρέτης των $a_1, \ldots, a_n$ αν και μόνο αν $(a_1) \cap \cdots \cap (a_n) \subseteq (d)$*
(2) *Ο d είναι συνδυασμός των $a_1, \ldots, a_n$ αν και μόνο αν $(d) \subseteq (a_1, \ldots, a_n)$*

Παρατηρείστε το εξής:

Πρόταση 27
Έστω R μία ακέραια περιοχή, $a_1, \ldots, a_n$ μη μηδενικά στοιχεία της. Αν

$$(a_1) \cap \cdots \cap (a_n) \subseteq (d) \subseteq (a_1, \ldots, a_n)$$

τότε ο d είναι μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$.

Απόδειξη: Η σχέση $(a_1) \cap \cdots \cap (a_n) \subseteq (d)$ μας λέει ότι ο d είναι ένας κοινός διαιρέτης των $a_1, \ldots a_n$ ενώ η $(d) \subseteq (a_1, \ldots, a_n)$, ότι υπάρχουν κάποια $r_1, \ldots, r_n$ με $d = r_1a_1 + \cdots + r_na_n$. Αν τώρα ο d' είναι κάποιος κοινός διαιρέτης των $a_1, \ldots, a_n$ τότε προφανώς θα διαιρεί και τον $d = r_1a_1 + \cdots + r_na_n$. □

Πρόταση 28
Έστω R μία ακέραια περιοχή, $a_1, \ldots, a_n$ μη μηδενικά στοιχεία της. Τότε τα $a_1, \ldots, a_n$ έχουν μέγιστο κοινό διαιρέτη d που είναι συνδυασμός τους δηλαδή που να εκφράζεται στη μορφή

$$d = r_1a_1 + \cdots + r_na_n$$

αν και μόνο αν το το ιδεώδες $(a_1, \ldots, a_n)$ είναι κύριο ιδεώδες.

Απόδειξη: Αν τα $a_1, \ldots, a_n$ έχουν μέγιστο κοινό διαιρέτη d που είναι συνδυασμός τους τότε φανερά $(d) \subseteq (a_1, \ldots, a_n)$. Για να πάρουμε και τον αντίθετο εγκλεισμό, θεωρώ $x = s_1a_1 + \cdots + s_na_n \in (a_1, \ldots, a_n)$. Επειδή ο d είναι κοινός διαιρέτης για κάθε $i = 1, \ldots, n$ θα έχω ότι $a_i = db_i$ για κάποια b_i οπότε $x = (s_1b_1 + \cdots + s_nb_n)d \in (d)$.

Συνεπώς $(a_1, \ldots a_n) = (d)$ είναι κύριο ιδεώδες.
Αντίστροφα αν το $(a_1, \ldots a_n)$ είναι κύριο θα έχουμε ότι για κάποιο r θα ισχύει $(a_1, \ldots a_n) = (d)$. Από την Πρόταση 27 έχουμε άμεσα ότι ο d είναι μέγιστος κοινός διαιρέτης των $a_1, \ldots a_n$ και εκφράζεται σαν συνδυασμός τους. □

Περνάμε τώρα σε μία σημαντική κατηγορία ακέραιων περιοχών.

Ορισμός 42
Μία ακέραια περιοχή θα λέγεται ***περιοχή κύριων ιδεωδών*** *αν κάθε ιδεώδες της είναι κύριο ιδεώδες.*

Σκοπός μας είναι να δείξουμε ότι μία περιοχή κύριων ιδεωδών έχει σημαντικές ιδιότητες, όπως για παράδειγμα ότι υπάρχει πάντοτε ο μέγιστος κοινός διαιρέτης δύο στοιχείων της (είναι δηλαδή ΜΚΔ-περιοχή) και ότι κάθεμη μηδενικό στοιχείο της που δεν είναι αντιστρέψιμο γράφεται μονοσήμαντα σαν γινόμενο ανάγωγων στοιχείων (είναι δηλαδή περιοχή μονοσήμαντης ανάλυσης). Επίσης δεν χρειάζεται να ανησυχούμε αν τα στοιχεία της ανάλυσης είναι ανάγωγα ή πρώτα αφού, όπως θα δούμε, σε περιοχές κύριων ιδεωδών.

Η Πρόταση 28 μας δίνει ένα άμεσο συμπέρασμα για τις περιοχές κύριων ιδεωδών:

Πρόταση 29
Αν R είναι περιοχή κύριων ιδεωδών τότε για οποιαδήποτε μη μηδενικά στοιχεία της $a_1, \ldots, a_n$ υπάρχει μέγιστος κοινός διαιρέτης τους d [31] που εκφράζεται πάντοτε σαν συνδυασμός των $a_1, \ldots, a_n$. Ειδικότερα κάθε περιοχή κύριων ιδεωδών είναι ΜΚΔ-περιοχή.

Ξεκινάμε με μία σημαντική ιδιότητα των περιοχών κύριων ιδεωδών:

Θεώρημα 21 *Έστω R μία περιοχή κύριων ιδεωδών και $(I_n)_{n=1}+\infty$ μία αύξουσα ακολουθία ιδεωδών της R δηλαδή*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \ldots$$

Τότε υπάρχει ένα n_0 τέτοιο ώστε

$$Αν \;\; n \geq n_0 \;\; τότε \;\; I_n = I_{n_0}$$

Απόδειξη: Έστω $(I_n)_{n=1}^{+\infty}$ μία αύξουσα ακολουθία ιδεωδών της R και $I = \bigcup_{n=1}^{+\infty} I_n$ η ένωσή τους. Τότε το I είναι ένα ιδεώδες και αφού είμαστε σε περιοχή κύριων ιδεωδών θα υπάρχει $a \in R$ με $I = (a)$. Έστω κάποιο n_0 με $a \in I_{n_0}$. Τότε $I = (a) \subseteq I_0 \subseteq I$, άρα $I_{n_0} = I$ και προφανώς όταν $n \geq n_0$ αφού $I_{n_0} \subseteq I_n$ θα έχουμε ότι $I_n = I_{n_0} = I = (a)$. □

Πρόταση 30
Σε μία περιοχή κύριων ιδεωδών κάθε μεγιστικό ιδεώδες είναι πρώτο ιδεώδες.

Απόδειξη: Έστω I να είναι μεγιστικό ιδεώδες και $p \in R$ με $I = (p)$. Φανερά το p δεν είναι ούτε μηδέν ούτε αντιστρέψιμο, αφού τα μεγιστικά ιδεώδη είναι γνήσια. θα δείξουμε ότι το p είναι πρώτο.
Πράγματι ας υποθέσουμε ότι $p|ab$ και έστω $J = (a, p) = \{xa + yp : x \in R, y \in B.$
Το $J \supseteq I$, και αφού το I είναι μεγιστικό είτε $J = I$ είτε $J = R$.
Στην πρώτη περίπτωση θα έχουμε ότι $a \in (p)$ δηλαδή $p|a$.
Στη δεύτερη περίπτωση θα έχουμε ότι $1 \in (a, p)$ δηλαδή για κάποια $x, y \in R$ θα συμβαίνει $1 = ax + py$, οπότε $b = abx + pby$ και αφού $p|ab$ θα έχουμε ότι $p|b$. □

Από τις Προτάσεις 30 και 25 έχουμε άμεσα:

Πρόταση 31 *Ένα ιδεώδες μίας περιοχής κύριων ιδεωδών είναι μεγιστικό αν και μόνο αν είναι πρώτο. Ειδικότερα, σε μία περιοχή κύριων ιδεωδών τα ανάγωγα και τα πρώτα στοιχεία της συμπίπτουν.*

Ας κάνουμε το πρώτο βήμα για να δείξουμε ότι οι περιοχές πρώτων ιδεωδών είναι περιοχές μονοσήμαντης ανάλυσης.

[31] άρα και το ελάχιστο κοινό πολλαπλάσιό τους

Πρόταση 32 *Κάθε μη μηδενικό μη αντιστρέψιμο στοιχείο a μίας περιοχής κύριων ιδεωδών εκφράζεται σα γινόμενο $a = pb$ όπου p πρώτος της περιοχής.*

Απόδειξη: Ας υποθέσουμε ότι αυτό δεν μπορεί να συμβεί δηλαδή υπάρχει μηδενικό μη αντιστρέψιμο στοιχείο a μίας περιοχής κύριων ιδεωδών δεν εκφράζεται σα γινόμενο $a = pb$ όπου p πρώτος της περιοχής. Τότε αυτό δεν είναι ανάγωγο (θυμόμαστε ότι τα ανάγωγα στοιχεία είναι οι πρώτοι) γιατί τότε θα το γράφαμε $a = 1 \cdot a$. Συνεπώς υπάρχουν a_1, b_1 με το a_1 μη αντιστρέψιμο και $a = a_1 b_1$, οπότε[32] $(a) \subseteq (a_1)$ Εφαρμόζοντας τον ίδιο συλλογισμό για το a_1 θα καταλήξουμε επαγωγικά σε μία άπειρη γνήσια αύξουσα ακολουθία ιδεωδών

$$(a) \subset (a_1) \subset (a_2) \subset \dots$$

και έρχόμαστε σε αντίφαση με το Θεώρημα 21. □

Πρόταση 33 *Κάθε μη μηδενικό μη αντιστρέψιμο στοιχείο a μίας περιοχής κύριων ιδεωδών εκφράζεται σα γινόμενο πρώτων.*

Απόδειξη: Από την προηγούμενη Πρόταση το a γράφεται σαν $a = p_1 a_1$ με p_1 πρώτος. Αν το a_1 είναι αντιστρέψιμο έχουμε τελειώσει αφού το $a_1 p_1$ είναι πρώτος. Αν όχι τότε το $a_1 = p_2 a_2$ με το p_2 πρώτος. Συνεχίζουμε την διαδικασία αυτή που πρέπει να τερματίζεται σε ένα πεπερασμένο αριθμό βημάτων. Πράγματι, αν μπορούσαμε να συνεχίζαμε επ άπειρον θα υπήρχε μία άπειρη ακολουθία $(p_n)_n$ από πρώτους ώστε $a = a_1 p_1 = a_2 p_1 p_2 = a_3 p_1 p_2 p_3 = \dots$ και θα ερχόμαστε πάλι σε αντίφαση με το Θεώρημα 21 γιατί τότε θα παίρναμε μία γνήσια αύξουσα ακολουθία ιδεωδών:

$$(a) \subset (p_1) \subset (p_2) \subset \dots$$

Αν η ακολουθία αυτή τερματιστεί σε n βήματα τότε έχουμε ότι το a γράφεται σαν $a = p_1 \cdots p_n$ με τα $p_1, \dots, p_n$ πρώτους. □

Θεώρημα 22 *Κάθε περιοχή κύριων ιδεωδών είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη: Από την προηγούμενη πρότση έχουμε ότι κάθε στοιχείο a μίας περιοχής κύριων ιδεωδών που δεν είναι ούτε μηδέν ούτε αντιστρέψιμο θα αναλύεται σε ένα γινόμενο πρώτων:

$$a = p_1 p_2 \cdots p_n \tag{1.18}$$

Αρκεί να δείξουμε ότι η ανάλυση αυτή είναι μονοσήμαντη. Με άλλα λόγια πρέπει να δείξουμε πως αν

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \tag{1.19}$$

με τα $p_1, p_2, \dots, p_n, q_1, q_2 \dots, q_m$ πρώτους, τότε
1) $m = n$ και

[32] Το σύμβολο $\subset$ εννοεί **γνήσιο** υποσύνολο

2) Υπάρχει μία 1-1 συνάρτηση $\sigma : \{1, \dots n\} \to \{1, \dots n\}$ τέτοια ώστε ο p_i να είναι ομόλογος με τον $q_{\sigma(i)}$ για κάθε $i \in \{1, \dots n\}$

Για να διευκολυνθούμε στην παρουσίαση μας αν $J \subseteq \{1, \dots, n\} = \{j_1, \dots, j_k\}$ το γινόμενο $p_{j_1} \cdots p_{j_k}$ όλων των p_j με δείκτη $j \in J$ θα συμβολίζεται εν συντομία

$$\prod_{j \in J} p_j$$

Ανάλογο νόημα θα έχει και η έκφραση $\prod_{j \in J} q_j$ όταν $J \subseteq \{1, \dots, m\}$. Έτσι, αν θέσουμε

$$A_1 = \{1, 2, \dots, n\}, \quad B_1 = \{1, 2, \dots, m\}$$

η εξίσωση 2.19 γράφεται

$$\prod_{i \in A_1} p_i = \prod_{j \in B_1} q_j \tag{1.20}$$

Υποθέτουμε ότι $n \leq m$.

Επειδή ο p_1 είναι πρώτος και διαιρεί το γινόμενο $q_1 q_2 \cdots q_m$ θα διαιρεί κάποιον από τους $q_1, \dots, q_m$. Θέτουμε $\sigma(1)$ να είναι ο μικρότερος i από τους $\{1, \dots, m\}$ ώστε $p_1 | q_i$. Θα έχουμε λοιπόν ότι $p_1 | q_{\sigma(1)}$, δηλαδή $q_{\sigma(1)} = p_1 a_1$. Αλλά ο $q_{\sigma(1)}$ είναι πρώτος και σε κάθε ανάλυσή τους σε γινόμενο δύο παραγόντων ο ένας είναι μοναδιαίος. Ο p_1 δεν είναι μοναδιαίος άρα θα είναι ο a_1 και έτσι έχουμε ότι ο $q_{\sigma(1)}$ είναι ομόλογος με τον p_1. Αν θέσουμε

$$A_2 = \{2, 3, \dots, m\}, \quad B_2 = B_1 \setminus \{\sigma(1)\}$$

η εξίσωση 1.20 γράφεται $p_1 \prod_{i \in A_2} p_i = a_1 p_1 \prod_{j \in B_2} q_j$ και με απαλειφή του p_1 θα έχουμε

$$\prod_{i \in A_2} p_i = a_1 \prod_{j \in B_2} q_j \tag{1.21}$$

όπου το a_1 είναι μοναδιαίο και προφανώς δεν μπορεί να διαιρείται από κανέναν πρώτο. Επειδή το $p_2 | a_1 \prod_{j \in B_2} q_j$ είτε διαιρεί το a_1 είτε διαιρεί το $\prod_{j \in B_2} q_j$. Αλλά το a_1 δεν γίνεται να το διαιρεί αφού οι πρώτοι δεν είναι μοναδιαία και μόνο τα μοναδιαία διαιρούν μοναδιαία συνεπώς

$$p_2 | \prod_{j \in B_2} q_j$$

Με τον ίδιο συλλογισμό όπως και πρίν θα υπάρχει ένα $j \in B_2$ με $p_2 | q_j$ και θέτουμε

$$\sigma(2) = \min\{j \in B_2 : p_2 | q_j\}$$

Θέτουμε

$$A_3 = \{3, \dots, n\}, \quad B_3 = B_2 \setminus \{\sigma(2)\}$$

και καταλήγουμε στο ότι

$$p_3 | \prod_{j \in B_3} q_j$$

Σε n βήματα θα έχουμε ορίσει μία 1-1 συνάρτηση

$$\sigma : \{1, \ldots, n\} \to \{1, \ldots, m\}$$

όπου ο p_i θα είναι ομόλογος με τον $q_{\sigma(i)}$. Παρατηρούμε ακόμα πως αν $m \neq n$ δηλαδή αν $n < m$ τότε το σύνολο $B_n \neq \emptyset$ και θα καταλήγαμε σε μία σχέση

$$1 = e \prod_{j \in B_n} q_j$$

με e μοναδιαίο που είναι αδύνατο γιατί τότε κάποιος πρώτος θα διαιρούσε τη μονάδα. Άρα $m = n$ και η πρότασή μας αποδείχτηκε πλήρως. □

1.14 Ευκλείδιες Περιοχές

Ευκλείδιες περιοχές θα ονομάζουμε εκείνες τις ακέραιες περιοχές στις οποίες έχουμε ένα ανάλογο της ταυτότητας της διαίρεσης (Θεώρημα 4) η οποία μας επέτρεπε να γράψουμε ένα αλγόριθμο με τον οποίο βρίσκουμε το μέγιστο κοινό διαιρέτη δύο μη μηδενικών ακέραιων. Με τον αλγόριθμο αυτό δείξαμε ότι ο μέγιστος κοινός διαιρέτης δύο ακέραιων είναι ένας ακέραιος συνδυασμός τους. Το βασικό σημείο στην ταυτότητα της διαίρεσης είναι ότι το υπόλοιπο της διαίρεσης έχει απόλυτη τιμή μικρότερη από την απόλυτη τιμή του διαιρέτη. Αυτό μας επιτρέπει με συνεχείς διαιρέσεις να έχουμε μια ακολουθία από υπόλοιπα που το κάθε ένα έχει απόλυτη τιμή μικρότερη από του προηγούμενου δηλαδή οι απόλυτες τιμές τους φθίνουν. Αλλά οι απόλυτες τιμές ακέραιων είναι φυσικοί αριθμοί και γνήσια φθίνουσα ακολουθία φυσικών δεν υπάρχει (Αρχή της Καλής Διάταξης). Καταλήγαμε έτσι ότι κάποιο υπόλοιπο θα μηδενιστεί και σε αυτό το στάδιο βρίσκαμε τον μέγιστο κοινό διαιρέτη. Στις Ευκλείδιες περιοχές θέλουμε να έχουμε μία ανάλογη έννοια με αυτή της απόλυτης τιμής, την οποία σε γενικούς δακτύλιους ονόμαζουμε Ευκλείδια εκτίμηση και ο ορισμός της δίνεται αμέσως παρακάτω:

Ορισμός 43 *Έστω R μία ακέραια περιοχή. Μία συνάρτηση*

$$N : R \to \mathbb{N}$$

*θα λέγεται **Ευκλείδια εκτίμηση** αν έχει τις παρακάτω ιδιότητες:*
(1)
Αν $a \neq 0$ τότε $N(a) \neq 0$.
(2) *Για οποιαδήποτε μη μηδενικά $a, b \in R$ $N(ab) \geq \max\{N(a), N(b)\}$.*

Παραδείγματα

1. Θεωρούμε ένα οποιοδήποτε μη μηδενικό ακέραιο m και θεωρούμε τον υποδακτύλιο του σώματος των μιγαδικών:

$$\mathbb{Z}(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in \mathbb{Z}\}$$

Αν $m = 1$ και γενικά αν ο m είναι τέλειο τετράγωνο τότε απλώς παίρνουμε το $\mathbb{Z}$. Αν $m = -1$ παίρνουμε το δακτύλιο των ακέραιων του Gauss και αν $m < 0$ και το $|m|$ είναι τέλειο τετράγωνο πάλι τον δακτύλιο των ακέραιων του Gauss θα έχουμε. Θα θεωρούμε όλους δακτύλιους $\mathbb{Z}(\sqrt{m})$ όπου $m = \pm 1$ είτε ο $|m|$ δεν είναι τέλειο τετράγωνο. Σε αυτούς ορίζουμε

$$N(a + b\sqrt{m}) = |(a + b\sqrt{m})(a - b\sqrt{m}) = |a^2 - mb^2|$$

Είναι εύκολο να δείξουμε ότι:
1. $N(a + b\sqrt{m}) = 0$ αν και μόνο αν $a = b = 0$.
2. Αν $x, y \in \mathbb{Z}(\sqrt{m})$ τότε $N(xy) = N(x)N(y)$.
Που δείχνει ότι ειδικότερα οι συναρτήσεις N είναι Ευκλείδιες εκτιμήσεις σε όλους αυτούς τους δακτύλιους.

2. Ας θεωρήσουμε μία οποιαδήποτε ακέραια περιοχή R και το δακτύλιο $R[x]$ όλων των πολυωνύμων μίας μεταβλητής x με συντελεστές από το R. Για κάθε πολυώνυμο $f(x) \in R[x]$ ορίζουμε $N(f)$ να είναι ο βαθμός του πολυωνύμου. Τότε είναι εύκολο να δούμε ότι αφού για πολυώνυμα f, g μη μηδενικού βαθμού ισχύει

$$N(fg) = N(f) + N(g)$$

η N είναι μία Ευκλείδια εκτίμηση στις ακέραιες περιοχές πολυωνύμων.

Δίνουμε τώρα τον ορισμό της έννοιας της Ευκλείδιας Περιοχής:

Ορισμός 44 *Μία ακέραια περιοχή R θα λέγεται* ***Ευκλείδια περιοχή*** *αν μπορεί να οριστεί μία Ευκλείδια εκτίμηση $N : R \to \mathbb{N}$ τέτοια ώστε για οποιαδήποτε $a, b \in R$ με $a \neq 0$ υπάρχουν[33] k, υ ώστε*

$$N(\upsilon) < N(a), \qquad b = ka + \upsilon$$

Θα τελειώσουμε δείχνοντας ότι οι Ευκλείδιες περιοχές είναι περιοχές κύριων ιδεωδών που σημαίνει ότι σε Ευκλείδιες περιοχές έχουμε όλα τα πλεονεκτήματα που ισχύουν στους συνηθισμένους ακέραιους: Τα ανάγωγα στοιχεία είναι και πρώτα, υπάρχει ο μέγιστος κοινός διαιρέτης και το ελάχιστο κοινό πολλαπλάσιο όποιωνδήποτε μη μηδενικών στοιχείων τους, ο μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$ εκφράζεται σαν συνδυασμός των $a_1, \ldots, a_n$ και τέλος κάθε μη μηδενικό μη αντιστρέψιμο στοιχείο εκφράζεται κατά ουσιαστικά μοναδικό τρόπο σαν γινόμενο ανάγωγων στοιχείων της περιοχής.

[33] όχι απαραίτητα μοναδικά

Θεώρημα 23 *Κάθε Ευκλείδια περιοχή είναι περιοχή πρώτων ιδεωδών.*

Απόδειξη: Έστω R μία ευκλείδια περιοχή με συνάρτηση εκτίμησης N και I ένα οποιοδήποτε ιδεώδες της. Αν $I = (0)$ είναι κύριο και υποθέτουμε έτσι ότι $I \neq (0)$. Θεωρούμε το παρακάτω υποσύνολο του $\mathbb{N}$:

$$M = \{N(x) : x \in I, x \neq 0\}$$

Το M είναι μη κενό υποσύνολο των φυσικών, $0 \notin M$ και συνεπώς έχει ένα ελάχιστο στοιχείο $N(b)$ με $b \neq 0$.

Παρατηρείστε τώρα ότι αν $x \in I$ τότε $N(x) < N(b)$ μπορεί να συμβαίνει μόνο αν $x = 0$.

Θα δείξουμε ότι

$$I = (b)$$

Πράγματι, έστω $x \in I$. Επειδή η R είναι Ευκλείδια περιοχή θα υπάρχουν k, υ με

$$N(\upsilon) < N(b), \qquad x = bk + \upsilon$$

Επειδή $x, b \in I$ θα έχουμε ότι $\upsilon \in I$ και από την προηγούμενη παρατήρηση θα έχουμε ότι $\upsilon = 0$ άρα $b|x$ άρα

$$I \subset (b)$$

Αλλά $b \in I$ άρα και

$$(b) \subset I$$

και η απόδειξη του θεωρήματος μας ολοκλήρώθηκε. $\square$

Πόρισμα 1 *Κάθε ευκλείδια περιοχή είναι περιοχή μονοσήμαντης ανάλυσης.*

Κεφάλαιο 2

Εφαρμογές της Γενικής Θεωρίας Ειδικές Ακέραιες Περιοχές

2.1 Δακτύλιοι Πολυωνύμων μίας μεταβλητής

Έστω F να είναι μία ακέραια περιοχή, $n \geq 0$ ένας φυσικός αριθμός και x ένα σύμβολο που $x \notin F$. Θα ονομάζουμε **πολυώνυμο βαθμού** n (ως προς τη μεταβλητή x) με συντελεστές από το F κάθε παράσταση της μορφής

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{2.1}$$

όπου $n \geq 0$ $a_n \neq 0$. Συχνά θα γράφουμε αντί της 2.1 ένα πολυώνυμο $f(x)$ σαν

$$f(x) = \sum_{i=0}^{n} a_i x^i \tag{2.2}$$

Με $R[x]$ θα συμβολίζουμε το σύνολο όλων των πολυωνύμων κάθε βαθμού με ένα επιπλέον στοιχείο 0 το οποίο θα ονομάζουμε το μηδενικό πολυώνυμο και το οποίο θα θεωρούμε διαφορετικό από κάθε άλλο πολυώνυμο. Γενικά αν $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = \sum_{j=0}^{m} b_i x^i = b_0 + a_1 x + \cdots + a_m x^m$ είναι δύο μη μηδενικά πολυώνυμα θα τα θεωρούμε ίσα αν και μόνο αν έχουν τον ίδιο βαθμό και τους ίδιους ομοιόβαθμους συντελεστές, συγκεκριμένα:

$$f(x) = g(x) \quad \Leftrightarrow \quad m = n, \quad a_0 = b_0, a_1 = b_1, \ldots a_n = b_n$$

Το $R[x]$ γίνεται ακέραια περιοχή με τις ακόλουθες πράξεις:

1. $0 \cdot f(x) = f(x) \cdot 0 = 0, 0 + f(x) = f(x) + 0 = f(x)$ για οποιοδήποτε $f(x) \in R[x]$.
2. Αν $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$,
$g(x) = \sum_{j=0}^{m} b_i x^i = b_0 + a_1 x + \cdots + a_m x^m$

είναι δύο μη μηδενικά πολυώνυμα τότε

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k x^k \tag{2.3}$$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \tag{2.4}$$

3. Η πρόσθεση ορίζεται με το να προσθέσουμε τους συντελεστές των ομοιόβαθμων όρων. Επειδή όμως είναι δυνατόν, αν τα πολυώνυμα έχουν τον ίδιο βαθμό, να κατέβει ο βαθμός του αθροίσματος πρέπει να ορίσουμε λίγο προσεκτικά το άθροισμα. Έστω $f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$,
$g(x) = \sum_{j=0}^{m} b_i x^i = b_0 + a_1 x + \cdots + a_m x^m$
είναι δύο μη μηδενικά πολυώνυμα. θα διακρίνουμε δύο περιπτώσεις:
(α) **Τα πολυώνυμα έχουν τον ίδιο βαθμό :** $m = n$. Σε αυτή την περίπτωση θέτουμε

$$N = \max\{0 \geq i \geq n : a_i - b_i \neq 0\}$$

Αν ο N δεν υπάρχει τότε θέτουμε $f(x) + g(x) = 0$ ενώ αν υπάρχει τότε

$$f(x) + g(x) = \sum_{i=0}^{N} (a_i + b_i) x^i$$

(β) **Τα πολυώνυμα έχουν διαφορετικό βαθμό :** $m < n$. Σε αυτή την περίπτωση θέτουμε

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

όπου θεωρούμε $b_i = 0$ αν $i > m$.

Οι προηγούμενοι ορισμοί φαίνονται κάπως περίπλοκοι και ο λόγος είναι ότι πρέπει να αναφερόμαστε κάθε φορά στους βαθμούς των πολυωνύμων. Υπάρχει όμως και ένας πιο σύντομος ορισμός του δακτύλιου $R[x]$. Η ιδέα είναι να ταυτίσουμε στη σκέψη μας ένα πολυώνυμο

$$a_0 + a_1 x + \cdots + a_n x^n$$

με την ακολουθία

$$(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$$

Ορισμός 45 *Έστω R ένας δακτύλιος. Μία* ***τελικά μηδενική ακολουθία*** *στοιχείων του R είναι μία ακολουθία $(a_n)_{n=0}^{+\infty}$ που με $a_n \in R$ για κάθε n και όλα τα*

στοιχεία της-εκτός από πεπερασμένο πλήθος - είναι ίσα με 0. Με άλλα λόγια υπάρχει ένα $n_0 \in \mathbb{N}$ τέτοιο ώστε για κάθε $n \geq n_0$ ισχύει $a_n = 0$.
Με 0 θα συμβολίζουμε την ακολουθία στοιχείων του R που όλα τα μέλη της είναι ίσα με 0.
Αν $(a_n)_{n=0}^{+\infty}$ είναι μία τελικά μηδενική σκολουθία διαφορετική από την 0 θα ονομάζουμε ***βαθμό*** *της $(a_n)_{n=0}^{+\infty}$ το μεγαλύτερο αριθμό n με την ιδιότητα $a_n \neq 0$.*
Τις τελικά μηδενικές ακολουθίες στοιχείων ενός δακτυλίου R θα τις ονομάζουμε και ***πολυώνυμα*** *με συντελεστές από το R. Ο θαθμός μίας μη μηδενικής ακολουθίας θα λέγεται ο* ***βαθμός*** *του πολυωνύμου.*
Το σύνολο όλων των πολυωνύμων στο R θα συμβολίζεται με $R[x]$.

Ορισμός 46 *Το $R[x]$ θα θεωρείται δακτύλιος με πράξεις:*

$$(a_n)_{n=0}^{+\infty} + (b_n)_{n=0}^{+\infty} = (a_n + b_n)_{n=0}^{+\infty}$$

$$(a_n)_{n=0}^{+\infty} \cdot (b_n)_{n=0}^{+\infty} = (a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0)_{n=0}^{+\infty} = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_{n=0}^{+\infty}$$

Για κάθε πολυώνυμο $f \in R[x]$ θα θέτουμε

$$N(f) = \begin{cases} 0 & \text{αν } f = 0 \\ (\text{βαθμός του } f) + 1 & \text{αν } f \neq 0 \end{cases}$$

Η παρακάτω πρόταση αφήνεται σαν άσκηση:

Πρόταση 34 *Αν R είναι ακέραια περιοχή και f, g είναι δύο μη μηδενικά πολυώνυμα στην $R[x]$ τότε*

$$N(f) = 0 \text{ αν και μόνο αν } f = 0 \tag{2.5}$$
$$N(f+g) = \max\{N(f), N(g)\} \tag{2.6}$$
$$N(fg) = N(f) + N(g) - 1 \tag{2.7}$$

Ειδικά η N είναι μία Ευκλείδια εκτίμηση.

Το βασικό αποτέλεσμα αυτής της παραγράφου είναι το ακόλουθο:

Θεώρημα 24 *Έστω R να είναι ένα σώμα. Τότε Για οποιαδήποτε πολυώνυμα $f, g \in R$ με $g \neq 0$ υπάρχουν δύο πολυώνυμα k, υ με $N(\upsilon) < N(g)$ και*

$$f = kg + \upsilon$$

Με άλλα λόγια το $R[x]$ είναι μία Ευκλείδια Περιοχή.

Απόδειξη: Αν $f = 0$ ή $N(f) < N(g)$ αρκεί να θέσουμε $k = 0$ και $\upsilon = f$ και τελειώσαμε. Άρα **μπορούμε εξαρχής να υποθέτουμε** πως $f \neq 0$ και $N(f) \geq N(g)$.
Θα αποδείξουμε το Θεώρημα με επαγωγή στο βαθμό $N(f) - 1$ του f.
Αν $N(f) = 1$ τότε $N(g) = 1$ και αφού $f, g \neq 0$ θα έχουμε $f = a_0 \neq 0$, $g = b_0 \neq 0$. **Επειδή το R είναι σώμα** το b_0 αντιστρέφεται και αρκεί να θέσουμε $k = b_0^{-1}a_0$ οπότε $\upsilon = 0$ και $N(\upsilon) = 0 < 1 = N(g)$.
Ας υποθέσουμε ότι γνωρίζουμε το θεώρημα για κάθε f, g με $N(f) \leq n + 1$ και $N(g) \leq N(f)$.
Θεωρώ δύο f, g με $N(f) = n + 1$ και $N(g) \leq N(f)$ όπου $f = a_0 + a_1x + \cdots + a_nx^n + a_{n+1}x^n$, $g = b_0 + \cdots + b_mx^m$ με $m \geq n$, $a_{n+1}b_m \neq 0$.
Θέτουμε[1]

$$h = a_nb_m^{-1}x^{n-m}, \qquad f' = f - gh$$

Παρατηρείστε ότι $N(f') < N(g)$. Αν $N(f') < N(h)$ έχουμε τελειώσει λόγω της παρατήρησης που κάναμε στην αρχή της απόδειξης. Αν πάλι $N(g) \leq N(f')$ τότε μπορούμε να χρησιμοποιήσουμε την επαγωγική υπόθεση για τα f', h και να βρούμε k', υ με $N(\upsilon) < N(g)$ και

$$f' = f - gh = k'g + \upsilon$$

Αλλά τότε

$$f = (k + h)g + \upsilon = kg + \upsilon$$

και το Θεώρημά μας αποδείχτηκε πλήρως. □

Είδαμε στην προηγούμενη παράγραφο ότι κάθε Ευκλείδια Περιοχή είναι περιοχή κύριων ιδεωδών και ειδικότερα περιοχή μονοσήμαντης ανάλυσης. Δεν είναι δύσκολο να δούμε ότι αν το F είναι σώμα τα μόνα αντιστρέψιμα στοιχεία του $F[x]$ θα είναι τα σταθερά μη μηδενικά πολυώνυμα δηλαδή αυτά με βαθμό ίσο με 0 (θυμηθείται ότι το 0 δεν έχει βαθμό). Άρα τα ανάγωγα πολυώνυμα θα έχουν βαθμό ≥ 1 και φανερά τα πολυώνυμα πρώτου βαθμού είναι ανάγωγα. Αυτά μας δίνουν άμεσα το εξής πόρισμα:

Πόρισμα 2 *Αν F είναι σώμα το $F[x]$ είναι περιοχή Περιοχή Κύριων Ιδεωδών και συνεπώς Περιοχή μονοσήμαντης Ανάλυσης.*
Ειδικότερα κάθε ανάγωγο πολυώνυμο είναι πρώτο και κάθε μη μηδενικό μη σταθερό πολυώνυμο $f \in F[x]$ αναλύεται κατά μοναδικό τρόπο σε γινόμενο ανάγωγων πολυωνύμων.

Μπορούμε να δείξουμε και με άμεσο τρόπο ότι το $F[x]$ είναι περιοχή κυρίων ιδεωδών. Πράγματι, ας θεωρήσουμε ένα οποιοδήποτε ιδεώδες I τής ακέραιας περιοχής $F[x]$ όλων των πολυωνύμων μίας μεταβλητής με συντελεστές από το σώμα

[1] Εννοείται ότι $h = 0 + 0x + 0x^2 + \cdots + 0x^{n-m-1} + b_m^{-1}x^{n-m}$ και ότι αν $n = m$ τοτε απλά $h = b_m^{-1}$

F. Υποθέτουμε ότι $I \neq (0)$ και έστω ένα στοιχείο $f \in I$ με τον ελάχιστο δυνατό βαθμό δηλαδή βαθμός$f \leq$ βαθμόςg για οποιοδήποτε $g \in I$. Προφανώς

$$(f) \subset I$$

θα δείξουμε ότι και $I \subset (f)$ οπότε $I = (f)$, δηλαδή το I είναι κύριο ιδεώδες.

Έστω $g \in I$. Αφού το f έχει βαθμό μικρότερο ή ίσο από το g, οπότε $N(f) \leq N(g)$, θα υπάρχουν $k, \upsilon \in F[x]$ με $g = kf + \upsilon$ με $N(\upsilon) < N(f)$. Αλλά $\upsilon = g - kf$, $g, kf \in I$ άρα και $\upsilon \in I$. Αυτό συνεπάγεται ότι το υ δεν μπορεί να είναι πολυώνυμο διαφορετικό από το μηδενικό (ισοδύναμα να έχουμε $N(\upsilon > 0)$, γιατί τότε θα είχε βαθμό που θα ήταν μικρότερος από από αυτόν του f, το οποίο αποκλείεται λόγω της εκλογής του f. Άρα $\upsilon = 0$ και συνεπώς $g \in (f)$. Άρα

$$I \subset (f)$$

και καταλήγουμε ότι

$$I = (f)$$

Από όσα έχουμε δεί μέχρι τώρα ένας δακτύλιος πολυωνύμων $F[x]$ είναι περιοχή μονοσημάντης ανάλυσης όταν το F είναι σώμα, με άλλα λόγια κάθε πολυώνυμο $f(x) \in F[x]$ θα γράφεται μονοσήμαντα σαν ένα γινόμενο $f(x) = p_1(x) \cdots p_n(x)$ με $p_1(x), \ldots, p_n(x)$ ανάγωγα πολυώνυμα.
Αλλά ποιά είναι τα ανάγωγα στοιχεία του $F[x]$;
Κατ΄ αρχήν παρατηρούμε ότι τα πολυώνυμα μηδενικού βαθμού δεν είναι (αφού είναι τα αντιστρέψιμα στοιχεία του $F[x]$). Επίσης, όλα τα πολυώνυμα πρώτου βαθμού είναι ανάγωγα, γιατί αν ένα πολυώνυμο πρώτου βαθμού αναλυόταν σε γινόμενο περισσότερων από ένα ανάγωγων πολυωνύμων τότε αυτά θα είχαν άθροισμα των βαθμών τους ίσο με 1, που δεν γίνεται. Το αν υπάρχουν πολυώνυμα βαθμού μεγαλύτερου από ένα που να είναι ανάγωγα αυτό εξαρτάται από το σώμα F. Αν για παράδειγμα $F = \mathbb{Q}$ τότε το $x^2 - 2$ είναι ανάγωγο ενώ το ίδιο πολυώνυμο στο $\mathbb{R}$ δεν είναι. Επίσης το $x^2 + 1$ σαν στοιχείο του $\mathbb{R}[x]$ είναι ανάγωγο ενώ αν το δούμε σαν στοιχείο του $\mathbb{C}[x]$ δεν είναι. Όπως θα δούμε το $\mathbb{C}[x]$ έχει την ιδιότητα που επιθυμούμε, δηλαδή τα ανάγωγα στοιχεία του να είναι τα πολυώνυμα πρώτου βαθμού και μόνο αυτά.

Από εδώ και στο εξής θα θεωρούμε πάντοτε ότι ο δακτύλιος των πολυωνύμων $F[x]$ ορίζεται πάνω σε σώμα.

Ας συνοψίσουμε όλα τα αποτελέσματα αυτής της παραγράφου
Αν F είναι ένα σώμα τότε:

(1) Ο δακτύλιος των πολυωνύμων του $F[x]$ είναι μία ακέραια περιοχή στην οποία τα αντιστρέψιμα στοιχεία είναι τα πολυώνυμα μηδενικού βαθμού (δηλαδή τα σταθερά μη μηδενικά πολυώνυμα) και μόνο αυτά.

(2) *Επιπλέον το $F[x]$ είναι Ευκλείδια Περιοχή συνεπώς περιοχή κύριων ιδεωδών και περιοχή μονοσήμαντης ανάλυσης άρα κάθε πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_nx^n$ βαθμού n αναλύεται μοναδικά σε ένα*

$$f(x) = p_1(x) \cdot p_2(x) \dots p_k(x)$$

όπου τα $p_1(x), dots, p_k(x)$ είναι ανάγωγα πολυώνυμα βαθμού ≥ 1 και το άθροισμα των βαθμών τους θα δίνει ακριβώς n.

Το τελευταίο προκύπτει από το γεγονός ότι ο βαθμός του γινομένου μη μηδενικών πολυωνύμων είναι το άθροισμα των βαθμών τους. Η μοναδικότητα σημαίνει ότι σε πιθανόν διαφορετικές αναλύσεις σε γινόμενο ανάγωγων πολυωνύμων οι παράγοντες της μίας ανάλυσης θα είναι ομόλογοι με αυτούς της άλλης. Επειδή ξέρουμε ακριβώς τα αντιστρέψιμα στοιχεία στο $F[x]$ (τα σταθερά μη μηδενικά πολυώνυμα) αυτό σημαίνει ότι οι παράγοντες μιας ανάλυσης έρχονται σε μία 1-1 αντιστοιχία με τους παράγοντες της άλλης ανάλυσης ώστε ο κάθε παράγοντας να είναι πολλαπλάσιο του αντίστοιχού του με σταθερό αριθμό. Πχ στο $\mathbb{R}[x]$

$$x^2 - 1 = (x-1)(x+1) = \frac{1}{2}(2x-2)(x+1) = \frac{1}{6}(2x-2)(3x+3) = \dots$$

Κάθε πολυώνυμο είναι φανερά ομόλογο με κάποιο που έχει συντελεστή του μεγιστοβάθμιου όρου του ίσο με 1. Ένα τέτοιο πολυώνυμο θα το ονομάζουμε «μονικό», αν και ο όρος αυτός δεν φαίνεται τόσο πετυχημένος.

Ορισμός 47
Ένα πολυώνυμο $f(x) \in F[x]$ της μορφής

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$$

*θα λέγεται **μονικό** πολυώνυμο βαθμού n.*

Φανερά θα έχουμε ότι:

Κάθε πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \in F[x]$ βαθμού n θα γράφεται κατά μοναδικό τρόπο σαν γινόμενο

$$f(x) = a_n p_1(x) \cdot p_2(x) \dots p_k(x)$$

όπου τα $p_1(x), dots, p_k(x)$ είναι ανάγωγα μονικά πολυώνυμα βαθμού ≥ 1 και το άθροισμα των βαθμών τους θα δίνει ακριβώς n. Εδώ η μοναδικότητα εννοείται με ισχυρότερο τρόπο από πρίν, δηλαδή αν

$$f(x) = a_n p_1(x) \cdot p_2(x) \dots p_k(x) = a_n q_1(x) \cdot ;_2 (x) \dots q_l(x)$$

με τα $p_1(x) \cdot p_2(x) \dots p_k(x), q_1(x) \cdot q_2(x) \dots q_l(x)$ μονικά πολυώνυμα τότε $k = l$ και υπάρχει μία 1-1 αντιστοιχεία $\sigma : \{1, \dots, k\} \to \{1, \dots, k\}$ με $p_i = q_{\sigma(i)}$ για κάθε $i = 1, \dots, k$.

Μια βασική έννοια για τη μελέτη της διαιρετότητας σε ένα δακτύλιο πολυωνύμων είναι η έννοιας της ρίζας.

Ορισμός 48
Έστω F ένα σώμα και $a \in F$. Η ***τιμή ενός πολυωνύμου*** $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ ***στο*** *a ορίζεται να είναι το στοιχείο $f(a) = a_0 + a_1a + \cdots + a_na^n$ του F.* ***Ρίζα*** *ενός πολυωνύμου $f(x)$ ονομάζεται κάθε $a \in F$ με την ιδιότητα $f(a) = 0$.*

Θεώρημα 25
Ένα μονικό πολυώνυμο πρώτου βαθμού $x - a$ διαιρεί ένα πολυώνυμο $f(x)$ αν και μόνο αν το a είναι ρίζα του $f(x)$.

Απόδειξη: Αν το $x - a$ διαιρεί το $f(x)$ τότε θα συμβαίνει $f(x) = (x - a)g(x)$ για κάποιο πολυώνυμο $g(x)$ και φανερά $f(a) = (a - a)g(a) = 0g(a) = 0$.
Αντίστροφα, αν $f(a) = 0$ τότε εκτελώντας την διαίρεση του $f(x)$ με $x - a$ θα έχουμε ότι $f(x) = g(x)(x - a) + c$ όπου c ένα σταθερό πολυώνυμο και θέτωντας $x = a$ στην προηγούμενη εξίσωση θα έχουμε ότι $c = 0$ άρα $x - a|f(x)$. □

Πόρισμα 3
Αν ένα πολυώνυμο $f(x) = a_0 + \cdots + a_nx^n$ βαθμού n έχει σαν ρίζες τον αριθμό c τότε γράφεται μοναδικά στη μορφή

$$f(x) = a_n(x - c)^m g(x)$$

όπου $1 \leq m \leq n$ και αν $m < n$ τότε το $g(x)$ είναι μονικό πολυώνυμο βαθμού $n - m$, με $g(c) \neq 0$, διαφορετικά $g(x) = 1$.
Ο αριθμός m θα ονομάζεται η ***πολλαπλότητα*** *της ρίζας c.*

Απόδειξη: Παρατηρείστε ότι

$$f(x) = a_n\left(x^n + \frac{a_{n-1}}{a_n} + \cdots + \frac{a_0}{a_n}\right)$$

, το δε πολυώνυμο $h(x) = \frac{a_0}{a_n} + \cdots + \frac{a_{n-1}}{a_n}x^{n-1} + x^n$ είναι μονικό και έχει τις ίδιες ρίζες με το $f(x)$. Από το προηγούμενο θεώρημα θα έχουμε ότι $h(x) = (x-c)g_1(x)$ όπου $g_1(x)$ θα είναι μονικό πολυώνυμο [2]. Αν πάρουμε το μεγαλύτερο δυνατό φυσικό m για τον οποίο θα έχουμε $h(x) = (x - c)^m g(x)$ φανερά $1 \leq m \leq n$ και[3] το $g(c) \neq 0$. Ένας λιγότερο σύντομος τρόπος να δούμε τα πράγματα είναι ο εξής: Από το προηγούμενο Θεώρημα, αφού το c είναι ρίζα του $h(x)$ θα έχουμε ότι $h(x) = (x - c)g_1(x)$. Αν το c δεν είναι ρίζα του $h_1(x)$ τελειώσαμε. Αν είναι τότε εφαρμόζοντας πάλι το προηγούμενο θεώρημα, ότι $g_1(x) = (x - c)g_2(x)$, άρα $h(x) = (x-c)^2 g_2(x)$. Συνεχίζουμε με τον ίδιο τρόπο...Η διαδικασία θα σταματήσει μετά από m φορές όπου βέβαια $1 \leq m \leq n$. □

[2] αυτό φαίνεται εξισώνοντας τους μεγιστοβάθμιους όρους.

[3] Αν $g(c) = 0$ δηλαδή αν ο c ήταν ρίζα του g τότε θα είχαμε από το προηγούμενο Θεώρημα ότι $h(x) = (x - c)^{m+1}g(x)$, το οποίο αποκλείεται λόγω της εκλογής του m.

Πόρισμα 4
Αν ένα πολυώνυμο $f(x) = a_0 + \cdots + a_n x^n$ βαθμού n έχει σαν ρίζες τους $c_1, c_2, \ldots, c_k$ (εννοείται διαφορετικούς ανά δύο) τότε διαιρείται από το $(x-c_1)(x-c_2)\cdots(x-c_k)$ και γράφεται μοναδικά στη μορφή

$$f(x) = a_n(x-c_1)^{m_1}\cdots(x-c_k)^{m_k}g(x)$$

όπου $m_1 + \cdots + m_k \leq n$ και αν $m_1 + \cdots + m_k < n$ τότε το $g(x)$ είναι ανάγωγο μονικό πολυώνυμο βαθμού $m = n - (m_1 + \cdots + m_k)$, διαφορετικά $g(x) = 1$.

Απόδειξη: Επαγωγή στον αριθμό k. Η περίπτωση $k = 1$ είναι το Πόρισμα 3. □

Πόρισμα 5
Αν ένα πολυώνυμο $f(x)$ έχει βαθμό ίσο με n τότε το πλήθος των διαφορετικών ριζών του είναι $\leq n$.

Απόδειξη: Ας υποθέσουμε ότι $f(x)$ είχε περισσότερες από n ρίζες, δηλαδή υπήρχαν $n+1$ διαφορετικές ρίζες του $f(x)$ που συμβολίζουμε με $c_1, \ldots, c_{n+1}$. Από τα προηγούμενα θα είχαμε $f(x) = (x-c_1)\ldots(x-c_{n+1})g(x)$ για κάποιο πολυώνυμο $g(x)$. Αλλά αυτό θα σήμαινε ότι ο βαθμός του $f(x)$ θα ήταν μεγαλύτερος από n, άτοπο. □

Ορισμός 49
Ένα σώμα F θα ονομάζεται:
(α) ***Αλγεβρικά κλειστό*** *αν κάθε πολυώνυμο μη μηδενικού βαθμού σε αυτό έχει ρίζα.*
(β) ***Πραγματικά κλειστό*** *αν κάθε πολυώνυμο περιττού μη μηδενικού βαθμού σε αυτό έχει ρίζα.*

Το παρακάτω Θεώρημα είναι από τα βασικότερα της Άλγεβρας και γι' αυτό ονομάζεται και Θεμελιώδες Θεώρημα. Αποδείχτηκε για πρώτη φορά από τον Gauss. Υπάρχουν πολλές διαφορετικοί μέθοδοι για να το δείξουμε αλλά καμμία δεν είναι απλή. Θα το δείξουμε σε μία ξεχωριστή παράγραφο.

Θεώρημα 26 (Το Θεμελιώδες Θεώρημα της Άλγεβρας)
Το σώμα $\mathbb{C}$ των μιγαδικών αριθμών είναι ένα αλγεβρικά κλειστό σώμα.

Πιο απλό σε απόδειξη είναι το παρακάτω Θεώρημα:

Θεώρημα 27
Το σώμα $\mathbb{R}$ των πραγματικών αριθμών είναι ένα πραγματικά κλειστό σώμα.

Απόδειξη: Έστω $f(x) = a_0 + a_1x + \cdots + a_nx^n$ πολυώνυμο στο $\mathbb{R}$ βαθμό n όπου το $n \geq 1$ είναι περιττός αριθμός. Ας υποθέσουμε ότι $a_n > 0$. Τότε

$$\lim_{x \to +\infty} f(x) = +\infty \tag{2.8}$$

$$\lim_{x \to -\infty} f(x) = -\infty \tag{2.9}$$

Η σχέση 2.8 μας δείχνει ότι θα υπάρχει κάποιο $x_1 > 0$ με $f(x_1) > 0$ και η σχέση 2.9 ότι θα υπάρχει κάποιο $x_2 < 0$ με $f(x_2) < 0$ και από το θεώρημα της ενδιάμεσης τιμής για συνεχείς συναρτήσεις[4] θα έχουμε ότι το $f(x)$ θα έχει μια ρίζα.

Η περίπτωση $a_n < 0$ είναι εντελώς ανάλογη. □

Σε αλγεβρικά κλειστά σώματα (όπως το $\mathbb{C}$) τα μη μηδενικά πολυώνυμα γράφονται σαν γινόμενα πρωτοβάθμιων πολυωνύμων. **Ειδικά σε αυτά τα ανάγωγα στοιχεία τους είναι τα πολυώνυμα πρώτου βαθμού και μόνο αυτά.**

Πόρισμα 6

Αν ένα σώμα F είναι αλγεβρικά κλειστό $f(x) = a_0 + \cdots + a_nx^n \in F$ βαθμού $n \geq 1$ θα γράφεται μοναδικό τρόπο στην μορφή:

$$f(x) = a_n(x - c_1)^{m_1} \cdots (x - c_k)^{m_k}$$

όπου $c_1, \ldots, c_k \in F$ είναι οι ρίζες του $f(x)$ και

$$m_1 + \cdots + m_k = n$$

Ειδικότερα αυτό συμβαίνει όταν $F = \mathbb{C}$.

Απόδειξη: Από το Πόρισμα 4 θα έχουμε ότι

$$f(x) = a_n(x - c_1)^{m_1} \cdots (x - c_k)^{m_k} g(x)$$

όπου $c_1, \ldots, c_k$ είναι όλες οι διαφορετικές ρίζες που έχει το $f(x)$ και το $g(x)$ είναι ανάγωγο μονικό πολυώνυμο. Αλλά τότε θα πρέπει $g(x) = 1$ γιατί από υπόθεση αν είχε βαθμό > 0 θα είχε ρίζα και δεν θα ήταν ανάγωγο. □

Τέλος ισχύει ένα θεώρημα ανάλογο με αυτό του Θεμελιώδους Θεωρήματος της Άλγεβρας για πολυώνυμα με πραγματικούς συντελετές.

Θεώρημα 28

Αν $f(x) = a_0 + \cdots + a_nx^n \in \mathbb{R}[x]$ είναι πολυώνυμο βαθμού n, τότε αυτό θα γράφεται κατά μοναδικό τρόπο στην μορφή:

$$f(x) = a_n(x - c_1)^{m_1} \cdots (x - c_k)^{m_k} \left((x + b_1)^2 + d_1^2\right)^{s_1} \cdots \left((x + b_l)^2 + d_l^2\right)^{s_l}$$

όπου $c_1, \ldots, c_k \in F$ είναι οι ρίζες του $f(x)$ και

$$m_1 + \cdots + m_k + 2s_1 + \cdots + 2s_l = n$$

.

[4] Αν $f : \mathbb{R} \to \mathbb{R}$ είναι μια συνεχής συνάρτηση και υπάρχουν $a, b \in \mathbb{R}$ με $f(a)f(b) < 0$ τότε θα υπάρχει και c μεταξύ των a, b με $f(c) = 0$. Επίσης τα πολυώνυμα είναι συνεχείς συναρτήσεις.

Αφού κάθε πολυώνυμο σε οποιοδήποτε σώμα γράφεται **μοναδικά** στην μορφή

$$f(x) = ap_1(x)\dots p_k(x)$$

με a να είναι ο συντελεστής του μεγιστοβάθμιου όρου και $p_1(x)\dots p_k(x)$ **μονικά και ανάγωγα** πολυώνυμα φανερά το προηγούμενο Θεώρημα είναι ισοδύναμο με το εξής:

Θεώρημα 29 *Τα ανάγωγα μονικά πολυώνυμα του $\mathbb{R}[x]$ είναι τα πολυώνυμα της μορφής*

$$x-a, \quad (x-a)^2+b^2, \;\; a,b\in\mathbb{R}, b\neq 0 \tag{2.10}$$

και μόνο αυτά.

Απόδειξη: Είναι σαφές ότι κάθε πολυώνυμο της μορφής 2.10 είναι ανάγωγο στο $\mathbb{R}$. Αν θεωρήσουμε ένα μονικό ανάγωγο πολυώνυμο $f(x)$ με βαθμό ≥ 2. Αν δούμε το $f(x)$ σαν στοιχείο του $\mathbb{C}[x]$ τότε από το Θεμελιώδες Θεώτημα θα έχει μια τουλάχιστον μιγαδική ρίζα ρ. Επειδή το $f(x)$ είναι ανάγωγο δεν μπορεί να είναι το ρ πραγματικός αριθμός δηλαδή θα πρέπει

$$\rho = a+b\mathrm{i}, \;\; b\neq 0 \tag{2.11}$$

Επειδή το $f(x)$ έχει πραγματικούς συντελεστές θα πρέπει για κάθε $c\in\mathbb{C}$

$$\begin{aligned}
\overline{f(a)} &= \overline{a_0+a_1c+a_2a^2+\dots+a_nc^n} = \\
&= \overline{a_0}+\overline{a_1c}+\overline{a_2a^2}+\dots+\overline{a_nc^n} = \\
&= \overline{a_0}+\overline{a_1}\,\overline{c}+\overline{a_2}\,\overline{a}^2+\dots+\overline{a_n}\,\overline{c}^n = \\
&= a_0+a_1\overline{c}+a_2\overline{c}^2+\dots+a_n\overline{c}^n = \\
&= f(\overline{a})
\end{aligned}$$

Συνεπώς αφού $f(\rho)=0$ θα έχουμε ότι $f(\overline{\rho})=0$ και λόγω της 2.11 θα έχουμε ότι

$$f(x) = (x-a-b\mathrm{i})(x-a+b\mathrm{i})g(x) = \left((x-a)^2+b^2\right)g(x)$$

Για κάποιο πολυώνυμο $g(x)$ που θα πρέπει να έχει **πραγματικούς συντελεστές**. Αλλά το $f(x)$ είναι ανάγωγο και μονικό, συνεπώς θα πρέπει $g(x)=1$ και το Θεώρημα μας αποδείχτηκε. □

Αν γνωρίζουμε ότι αληθεύει το Θεώρημα 28 τότε εύκολα προκύπτει το Θεμελιώδες Θεώρημα. Στην πραγματικότητα ο Gauss απέδειξε το Θεμελιώδες Θεώρημα στη μορφή του Θεωρήματος 28.

Από το Θεμελιώδες Θεώρημα θα έχουνε το ασθενέστερο φαινομενικά αποτέλεσμα:

Θεώρημα 30 *Κάθε πολυώνυμο με πραγματικούς συντελεστές έχει μία τουλάχιστον μιγαδική ρίζα.*

Φανερά το το Θεμελιώδες Θεώρημα συνεπάγεται το Θεώρημα 30. Ας υποθέσουμε ότι ισχύει το Θεώρημα 30. Θα δείξουμε από αυτό πως προκύπτει το Θεμελιώδες Θεώρημα.
Αν

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

είναι ένα πολυώνυμο με μιγαδικούς συντελεστές και θεωρήσουμε το συζυγές πολυώνυμο

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n$$

τότε το πολυώνυμο

$$F(x) = f(x)\overline{f}(x) = b_0 + b_1 x + \cdots + b_{2n-1}x^{2n-1} + b_{2n}x^{2n}$$

θα έχει πραγματικούς συντελεστές, αφού

$$b_k = \sum_{i,j,\ i+j=k} a_i\, \overline{a}_j, \quad k = 0\ldots, 2n$$

και συνεπώς με χρήση των ιδιοτήτων των συζυγών μιγαδικών θα πάρουμε

$$\overline{b}_k = \sum_{i,j,\ i+j=k} \overline{a}_i\, a_j = b_k$$

Από το Θεώρημα 30 το $F(x)$ θα έχει μία ρίζα ρ, δηλαδή

$$F(\rho) = f(\rho)\overline{f}(\rho) = 0$$

Αν $f(\rho) = 0$ τότε βρήκαμε μια ρίζα του $f(x)$. Αν πάλι $\overline{f}(\rho) = 0$ τότε

$$\overline{f}(\rho) = \overline{a}_0 + \overline{a}_1\rho + \cdots + \overline{a}_n\rho^n = 0$$

άρα

$$f(\overline{\rho}) = \overline{\overline{f}(\rho)} = a_0 + a_1\overline{\rho} + \cdots + a_n\overline{rho}^n = 0$$

και πάλι βρήκαμε μια ρίζα του $f(x)$.

2.1.1 Η Παράγωγος και ο τύπος του Taylor

Μία πολύ χρήσιμη έννοια είναι αυτή της παραγώγου ενός πολυωνύμου που θα εισάγουμε εδώ με καθαρά αλγεβρικό τρόπο.

Ορισμός 50 *Έστω R ένα σώμα. Ονομάζουμε* ***παράγωγο*** *ενός πολυωνύμου $f(x) = (a_i)_{i=0}\infty \in R[x]$ να είναι το πολυώνυμο*

$$f'(x) = ((i+1)a_{i+1})_{i=0}^{\infty} = (a_1, 2a_2, 3a_3, \ldots)$$

Παρατηρούμε τα εξής:

(α) Αν το πολυώνυμο είναι το μηδενικό πολυώνυμο ή πολυώνυμο μηδενικού βαθμού τότε η παράγωγός του είναι το μηδενικό πολυώνυμο.

(β) Αν το πολυώνυμο $f(x)$ έχει βαθμό $n \geq 1$, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$ τότε η παράγωγός του είναι πολυώνυμο $n-1$ βαθμού, συγκεκριμμένα το

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

Πρόταση 35 *Αν R είναι σώμα και $f(x), g(x) \in R[x]$, $a, b \in R$ τότε*

$$(af(x) + bg(x))' = af'(x) + bg'(x) \tag{2.12}$$

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x) \tag{2.13}$$

Απόδειξη: Αν $f(x) = (a_i)_{i=0}^{\infty}, g(x) = (b_i)_{i=0}^{\infty}$ τότε

$$\begin{aligned} af'(x) + bg'(x) &= ((i+1)(aa_{i+1} + bb_{i+1})) = \\ &= (af(x) + bg(x))' \end{aligned}$$

Για την απόδειξη της 2.13 θα χρησιμοποιήσουμε επαγωγή στο βαθμό του πολυωνύμου $f(x)$. Αν $f(x) = 0$ ή $f(x)$ είναι πολύωνυμο μηδενικού βαθμού και το $g(x)$ οποιοδήποτε πολυώνυμο (δηλαδή το $f(x) = a$) τότε η 2.13 προκύπτει από την 2.12. Ας υποθέσουμε ότι γνωρίζουμε την ισχύ της 2.13 όταν το $f(x)$ είναι πολυώνυμο με βαθμό μικρότερο ή ίσο από n και το $g(x)$ οποιοδήποτε πολυώνυμο. Ας υποθέσουμε τώρα ότι το $f(x)$ είναι πολυώνυμο βαθμού $n+1$, και γράφουμε

$$f(x) = h(x) + a_{n+1} x^{n+1}$$

Παρατηρείστε ότι είναι εύκολο να δούμε ότι για κάθε n:

$$(ax^n)' = anx^{n-1} \tag{2.14}$$

και επίσης ότι για κάθε πολυώνυμο $g(x) = b_0 + b_1 x + \cdots + b_m x^m$:

$$\begin{aligned} (xg(x))' &= (b_0 x + b_1 x^2 + \cdots + b_m x^{m+1})' = \\ &= b_0 + 2b_1 x + 3b_2 x^2 + \cdots + (m+1) b_m x^m \\ &= xg'(x) + g(x) \end{aligned} \tag{2.15}$$

όπου το $h(x)$ έχει βαθμό μικρότερο ή ίσο από n. Τότε με χρήση της επαγωγικής υπόθεσης και των 2.12, 2.14, 2.15:

$$\begin{aligned} (f(x)g(x))' &= (g(x)h(x))' + (a_{n+1}x^{n+1}g(x))' = \\ &= (g(x)h(x))' + (a_{n+1}x^n x g(x))' = \\ &= g'(x)h(x) + g(x)h'(x) + (a_{n+1}x^n)' x g(x) + a_{n+1}(xg(x))' = \\ &= g'(x)h(x) + g(x)h'(x) + n a_{n+1} x^{n-1} x g(x) + a_{n+1} x^n (xg(x))' = \\ &= g'(x)h(x) + g(x)h'(x) + n a_{n+1} x^n g(x) + a_{n+1} x^{n+1} g(x) + a_{n+1} x^n g'(x) = \\ &= g(x)\left(h'(x) + (n+1)a_{n+1}x^n\right) + g'(x)(h(x) + a_{n+1}x^{n+1}) = \\ &= g(x)f'(x) + g'(x)f(x) \end{aligned}$$

και η σχέση 2.13 αποδείχτηκε. □

Λήμμα 4 *Για κάθε $n \geq 1$*

$$((x+a)^n)' = n(x+a)^{n-1} \tag{2.16}$$

Απόδειξη: Για $n = 1$ η σχέση είναι προφανής. Επαγωγικά, με χρήση της 2.13:

$$\begin{aligned}((x+a)^{n+1})' &= ((x+a)^n(x+a))' = \\ &= ((x+a)^n)'(x+a) + (x+a)^n(x+a)' = \\ &= n(x+a)^{n-1}(x+a) + (x+a)^n = \\ &= (n+1)(x+a)^n\end{aligned}$$

□

Από τα προηγούμενα μπορούμε να πάρουμε σχετικά εύκολα μια σημαντική ταυτότητα γνωστή με το όνομα **τύπος του Taylor**. Πρίν διατύπωσουμε το θεώρημα θα εισάγουμε ένα συμβολισμό. Αν $f(x)$ είναι ένα πολυώνυμο τότε $f'(x)$ συμβολίζει την παράγωγό του, $f^(2)(x)$ την παράγωγο του $f'(x)$ και επαγωγικά $f^(i)(x)$ την παράγωγο του $f^{(i-1)}(x)$ που λέγεται και **παράγωγος $i-$τάξης** του $f(x)$ και είναι το πολυώνυμο που προκύπτει αν παραγωγίσουμε i φορές διαδοχικά το $f(x)$. φανερά αν το $f(x)$ είναι βαθμού n τότε το $f^{(i)}(x)$ είναι το μηδενικό πολυώνυμο όταν $i \geq n+1$.
Αν $a \in R$ με $f^{(i-1)}(a)$ συμβολίζουμε την τιμή του $f^{(i-1)}(x)$ για $x = a$. Επίσης σε οποιοδήποτε σώμα με μονάδα 1 όταν γράφουμε n με n φυσικός αριθμός θα εννοούμε το στοιχείο $1 + \cdots + 1$ (n-φορές) του σώματος και με $\frac{a}{n}$ το an^{-1}.

Θεώρημα 31 (Ο τύπος του Taylor για πολυώνυμα) *Έστω R οποιοδήποτε σώμα. Για κάθε πολυώνυμο $f(x) \in R[x]$ βαθμού $n \geq 1$ και κάθε $a \in R$ ισχύει*

$$f(x+a) = f(a) + \frac{f'(a)}{1!}x + \cdots + \frac{f^{(i)}(a)}{i!}x^i + \cdots + \frac{f^{(n)}(a)}{n!}x^n \tag{2.17}$$

Μια άμεση εφαρμογή του τύπου του Taylor είναι το δυωνυμικό ανάπτυγμα του Newton. Αν πάρουμε για $f(x) = x^n$, τότε αν $1 \leq i \leq n$ με επαγωγή δείχνουμε ότι:

$$f^{(i)}(x) = n(n-1)\ldots(n-i+1)x^{n-i}$$

και συνεπώς

$$\frac{f^(i)(a)}{i!} = \frac{n(n-1)\ldots(n-i+1)}{i!}a^{n-i} = \binom{n}{i}a^{n-i}$$

και ο τύπος του Taylor γίνεται

$$(x+a)^n = \sum_{i=0}^{n} \binom{n}{i} x^i a^{n-i}$$

δηλαδή ο τύπος του δυωνύμου του Newton.

Η απόδειξη του τύπου του Taylor γίνεται ως εξής. Αν $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ τότε θα έχουμε:

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ f'(x) &= a_1 + 2a_2 x \cdots + n a_n x^{n-2} \\ &\cdots \\ f^{(i)}(x) &= i! a_i + \cdots + n(n-1)\cdots(n-i+1) x^{n-i+1} \end{aligned}$$

που δίνει θέτοντας $x = 0$

$$\begin{aligned} f(0) &= a_0 \\ f'(0) &= a_1 \\ &\cdots \\ f^{(i)}(0) &= i! a_i \end{aligned}$$

για $i = 0, \ldots, n$, όπου θεωρούμε $0! = 1$.
Με αυτό τον τρόπο καταλήγουμε άμεσα στην ταυτότητα:

$$f(x) = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} \frac{f^{(i)}(0)}{i!} x^i \tag{2.18}$$

Αν θέσουμε

$$g(x) = f(x+a)$$

εφαρμόζουμε το Λήμμα 4 και τον τύπο 2.12 και έχουμε:

$$\begin{aligned} g'(x) &= (\sum_{i=0}^{n} a_i (x+a)^i)' = \\ &= \sum_{i=0}^{n-1} a_{i+1}(i+1)(x+a)^i = \\ &= f'(x+a) \end{aligned}$$

και γενικότερα:

$$g^{(i)}(x) = f^{(i)}(x+a) \tag{2.19}$$

Από τις εξισώσεις 2.18, 2.19 θα έχουμε

$$f(x+a) = g(x) = \sum_{i=0}^{n} \frac{g^{(i)}(0)}{i!} x^i = \sum_{i=0}^{n} \frac{f^{(i)}(a)}{i!} x^i$$

Μια από τις εφαρμογές της παραγώγου είναι ότι μπορούμε να ελέγξουμε αν μία ρίζα έχει πολλαπλότητα ≥ 2.

Πρόταση 36 *Έστω R ένα σώμα. Ένα $a \in R$ είναι ρίζα πολλαπλότητας μεγαλύτερης ή ίσης του 2 για το πολυώνυμο $f(x) \in R[x]$ αν και μόνο αν είναι ρίζα των $f(x), f'(x)$*

Απόδειξη: Αν το a είναι ρίζα πολλαπλότητας μεγαλύτερης ή ίσης του 2 τότε θα έχουμε ότι

$$f(x) = (x-a)^2 g(x)$$

και συνεπώς

$$f'(x) = (x-a)\left(2g(x) + (x-a)g'(x)\right)$$

άρα το a είναι και ρίζα του $f'(x)$. Αντίστροφα, αν το a είναι κοινή ρίζα των $f(x), f'(x)$ τότε θα υπάρχουν πολυώνυμα $g(x), h(x)$ με

$$f(x) = (x-a)g(x) \tag{2.20}$$
$$f'(x) = (x-a)h(x) \tag{2.21}$$

Παραγωγίζοντας την 2.20

$$f'(x) = (x-a)g'(x) + g(x) \tag{2.22}$$
$$\tag{2.23}$$

και συνδυάζοντας τις 2.20, 2.21, 2.22,

$$f(x) = (x-a)g(x) = (x-a)\left(f'(x) - (x-a)g'(x)\right) = \tag{2.24}$$
$$= (x-a)\left((x-a)h(x) - (x-a)g'(x)\right) = \tag{2.25}$$
$$= (x-a)^2\left(h(x) - g'(x)\right) \tag{2.26}$$

□

2.2 Το Θεμελιώδες Θεώρημα της Άλγεβρας

Όπως υποσχεθήκαμε δύο παράγραφους πιο πριν θα δείξουμε ένα βασικό Θεώρημα, ότι το σώμα των μιγαδικών αριθμών είναι αλγεβρικό κλειστό σώμα δηλαδή κάθε μη μηδενικό πολυώνυμο στο $\mathbb{C}[x]$ έχει ρίζα ή ισοδύναμα αναλύεται σε γινόμενο πολυωνύμων πρώτου βαθμού ή ισοδύναμα τα ανάγωγα στοιχεία του $\mathbb{R}[x]$ είναι ακριβώς τα πολυώνυμα πρώτου βαθμού.

Θεώρημα 32 *[Το Θεμελιώδες Θεώρημα της Άλγεβρας]*
Κάθε πολυώνυμο μη μηδενικού βαθμού με συντελεστές στο $\mathbb{C}$ έχει μία ρίζα στο $\mathbb{C}$.

Θα χρειαστούμε πρώτα ένα βοηθητικό Θεώρημα από την ανάλυση. Στα μαθήματα της ανάλυσης είδαμε ότι αν X, Y είναι μετρικοί χώροι και $f : X \to Y$ μια συνεχής συνάρτηση τότε για οποιοδήποτε $K \subset X$ συμπαγές σύνολο η εικόνα του $f(K)$ είναι επίσης συμπαγές υποσύνολο του Y. Αυτό είναι το **Θεώρημα Bolzano-Weierstrass**.

Εμείς θα περιοριστούμε στην περίπτωση που $X = \mathbb{C}$ και $Y = \mathbb{R}$. Σε αυτή την περίπτωση (και γενικά αν οι χώροι μας είναι οι Ευκλείδιοι χώροι $\mathbb{R}^n$ οποιαδήποτε διάστασης) τα συμπαγή υποσύνολα είναι τα κλειστά και φραγμένα. Θα έχουμε λοιπόν σαν άμεσο πόρισμα του Θεωρήματος Bolzano-Weierstrass το

Θεώρημα 33 *Αν $f : \mathbb{C} \to \mathbb{R}$ είναι μια συνεχής συνάρτηση τότε σε κάθε κλειστο κύκλο $C_M = \{x \in \mathbb{C} : |x| \leq M\}$, $M > 0$ θα λαμβάνει ελάχιστη τιμή (και μέγιστη βέβαια), δηλαδή θα υπάρχει ένα $x_0 \in C_M$ με $f(x_0) \leq f(x)$ για κάθε $x \in C_M$.*

Το επόμενο είναι σχεδόν άμεσο:

Πρόταση 37 *Αν $f(x) = a_0 + \cdots + a_n x^n$ είναι ένα πολυώνυμο με μιγαδικούς συντελεστές τότε αυτό είναι συνεχής συνάρτηση $f : \mathbb{C} \to \mathbb{C}$ και η συνάρτηση $g(x) = |f(x)|$ είναι μια συνεχής συνάρτηση από το $\mathbb{C}$ στο $\mathbb{R}$.*

Απόδειξη: θεωρείστε ένα $x_0 \in \mathbb{C}$ και $\epsilon > 0$. Έστω $x \in \mathbb{C}$ και $h = x - x_0$. Χρησιμοποιώντας το ανάπτυγμα του Taylor (μπορείτε να το δείξετε και άμεσα αν θέλετε) θα υπάρχουν σταθεροί αριθμοί[5] $c_1, \ldots, c_n$ με

$$f(x) = f(x_0) + c_1 h + \cdots + c_n h^n$$

και συνεπώς αν πάρουμε $|h| < 1$

$$|f(x) - f(x_0)| \leq |h|(|c_1| + \cdots + |c_n|)$$

Αν διαλέξουμε

$$|h| = |x - x_0| < \min\left\{1, \frac{\epsilon}{|c_1| + \cdots + |c_n|}\right\}$$

θα έχουμε άμεσα ότι

$$|f(x) - f(x_0)| < \epsilon$$

που δείχνει τη συνέχεια της $f(x)$ στο σημείο x_0. Επειδή επιλέξαμε το x_0 στη τύχη θα έχουμε ότι η $f(x)$ είναι συνεχής σε κάθε σημείο x του μιγαδικού επιπέδου. Επειδή:

$$|\ |f(x)| - |f(x_0)|\ | \leq |f(x) - f(x_0)|$$

θα έχουμε άμεσα και την συνέχεια της $|f(x)|$ από το $\mathbb{C}$ στο $\mathbb{R}$. □

[5] Τους οποίους μπορείτε να υπολογίσετε συναρτήσει των συντελεστών του πολυωνύμου. Συγκεκριμμένα $c_i = \frac{f^{(i)}(x_0)}{i!}$.

Αν το πολυώνυμο $f(x) = a_0 + \cdots + a_n x^n$ έχει βαθμό $n \geq 1$ τότε

$$\begin{aligned} |f(x)| &= |a_0 + \cdots + a_n x^n| = \\ &= |x|^n \left| \frac{a_0}{|x|^n} + \cdots + a_n \right| \geq \\ &\geq |x|^n \left(\left| |a_n| - \frac{a_{n-1}}{|x|} - \cdots - \frac{|a_0|}{|x|^n} \right| \right) \end{aligned} \tag{2.27}$$

Αν τώρα μας δώσουν έναν οσοδήποτε μεγάλο θετικό αριθμό N και διαλέξουμε το x να έχει μεγάλο μέτρο, πχ

$$|x| > \max \left\{ 1, \frac{2n\ |a_i|}{|a_n|}, N, \quad i = 0, \ldots, n-1 \right\}$$

τότε

$$|f(x)| > N$$

και έτσι δείξαμε πως:

Πρόταση 38 *Αν $f(x)$ είναι ένα μιγαδικό πολυώνυμο βαθμού ≥ 1 (δηλαδή μη σταθερό) , για οποιοδήποτε $N > 0$ μπορούμε να βρούμε ένα $M > 0$ τέτοιο ώστε αν $|x| > M$ τότε $|f(x)| > N$.*

Θα χρειαστούμε και μια τελευταία πρόταση γνωστή σαν το **Λήμμα του d' Alembert**.

Πρόταση 39 *Αν $f(x)$ είναι ένα μιγαδικό πολυώνυμο βαθμού ≥ 1 (δηλαδή μη σταθερό) και $x_0 \in \mathbb{C}$ με $f(x_0) \neq 0$ τότε μπορούμε να βρούμε ένα $h \in \mathbb{C}$ με $|f(x_0 + h)| < |f(x_0)|$.*

Απόδειξη: Από τον τύπο του Taylor θα έχουμε ότι για οποιαδήποτε $x_0, h \in \mathbb{C}$, θα υπάρχουν $b_1, \ldots, b_n \in \mathbb{C}$ ανεξάρτητα από το h με

$$f(x_0 + h) = f(x_0) + b_1 h + \cdots + b_n h^n$$

και αν $f(x_0) \neq 0$ και το πολυώνυμο έχει βαθμό ≥ 1 θα έχουμε ότι

$$\frac{f(x_0 + h)}{f(x_0)} = (1 + c_k h^k) + c_k h^k \left(\frac{c_{k+1}}{c_k} h + \cdots + \frac{c_n}{c_k} h^{n-k} \right)$$

όπου $c_k \neq 0$, και τα $c_k, \ldots, c_n$ είναι ανεξάρτητα του h.

Αν διαλέξουμε το h να έχει αρκετά μικρό μέτρο για παράδειγμα[6]

$$|h| < \epsilon_1 = \min \left\{ \frac{|c_k|}{2n|c_i|}, \quad i = k+1, \ldots, n \right\} \tag{2.28}$$

[6] Αν $c_i = 0$ τότε θεωρούμε $\frac{|c_k|}{2n|c_i|} = +\infty$.

τότε

$$\left|\frac{c_{k+1}}{c_k}h+\cdots+\frac{c_n}{c_k}h^{n-k}\right|<\frac{1}{2} \tag{2.29}$$

και θα έχουμε ότι για όλα αυτά τα h

$$\frac{|f(x_0+h)|}{|f(x_0)|}<|1+c_kh^k|+\frac{1}{2}|c_kh^k| \tag{2.30}$$

Αν επιπλέον διαλέξουμε

$$|h|<\epsilon_2=\frac{1}{\sqrt[k]{|c_k|}} \tag{2.31}$$

τότε

$$|c_kh^k|<1 \tag{2.32}$$

Κάθε μιγαδικός αριθμός x γράφεται σαν

$$x=|x|(\cos\theta+\mathrm{i}\sin\theta)$$

όπου $|x|$ είναι το μέτρο του και θ ένας πραγματικός αριθμός με $0\leq\theta<2\pi$ που συμβολίζεται με

$$\theta=\arg(x)$$

Επειδή για οποιουσδήποτε μιγαδικούς αριθμούς x,y ισχύει

$$\arg(xy)=\arg(x)+\arg(y)$$

θα έχουμε

$$\arg(c_kh^k)=\arg(c_k)+k\arg(h)$$

Αν συνεπώς διαλέξουμε

$$\arg(h)=\frac{\pi-\arg(c_k)}{k} \tag{2.33}$$

τότε

$$\arg(c_kh^k)=\pi$$

που σημαίνει ότι ο c_kh^k θα είναι αρνητικός πραγματικός αριθμός και συνεπώς θα έχουμε αν επιπλέον $|c_kh^k|<1$, ότι

$$|1+c_kh^k|=1-|c_kh^k| \tag{2.34}$$

Συνδυάζοντας όλα τα προηγούμενα θα έχουμε ότι αν h είναι μιγαδικός αριθμός που να ικανοποιεί τις σχέσεις 2.28, 2.31, 2.34 τότε θα έχουμε από την εξίσωση 2.30 και τις 2.32, 2.34:

$$\frac{|f(x_0+h)|}{|f(x_0)|}<|1+c_kh^k|+\frac{1}{2}|c_kh^k|=1-|c_kh^k|+\frac{1}{2}|c_kh^k|=1-\frac{1}{2}|c_kh^k|<1 \tag{2.35}$$

και η πρόταση μας αποδείχτηκε. Για την ακρίβεια δείξαμε ότι αν $f(x_0) \neq 0$ τότε για κάθε $\epsilon > 0$ υπάρχει μιγαδικός h με $|h| < \epsilon$ και $|f(x_0 + h)| < f(x_0)$. $\square$

Τώρα είμαστε σε θέση να δώσουμε μια απόδειξη του Θεμελιώδους θεωρήματος.

Ας θεωρήσουμε ένα οποιοδήποτε μη σταθερό πολυώνυμο $f(x)$. Από την Πρόταση 38 υπάρχει ένα $M > 0$ ώστε $|f(x)| > |f(0)|$ όταν $|x| > M$. Από το Θεώρημα του Weierstrass υπάρχει ένα $x_0 \in C_M = \{x : |x| \leq M\}$ με $|f(x_0)| \leq |f(x)|$ όταν $x \in C_M$. Ειδικότερα $|f(x_0)| \leq |f(0)|$. Αλλά και όταν $x \notin C_M$ δηλαδή όταν $|x| > M$ θα έχουμε ότι $|f(x)| > |f(0)| \leq |f(x_0)|$ και συνεπώς

$$\text{Για κάθε } x \in \mathbb{C}, \quad |f(x_0)| \leq |f(x)| \tag{2.36}$$

Αλλά τότε $f(x_0) = 0$ διαφορετικά η 2.36 θα ερχόταν σε αντίφαση με το Λήμμα του d' Alembert (Πρόταση 39).

2.3 Το σώμα των πηλίκων μιας ακέραιας περιοχής

Σε αυτή την παράγραφο θα κατασκευάσουμε ξεκινώντας από μία οποιαδήποτε ακέραια περιοχή R ένα σώμα $\mathcal{Q}(R)$ που είναι το «μικρότερο» σώμα που περιέχει (ισομορφικά) μέσα του την R. Το σώμα αυτό θα το ονομάζουμε το σώμα των πηλίκων (κλασμάτων) της ακέραιας περιοχής γιατί η κατασκευή του είναι εντελώς ανάλογη με αυτή αυτή του σώματος των ρητών αριθμών που είναι το σύνολο των κλασμάτων (πηλίκων) των ακέραιων αριθμών, δηλαδή το σύνολο των $\frac{a}{b}$ με $a, b \in \mathbb{Z}$.

Θεώρημα 34 *Έστω R μία ακέραια περιοχή. Τότε υπάρχει ένα σώμα $F = \mathcal{Q}(R)$ με τις εξής ιδιότητες:*
(1) *Υπάρχει ένας μονομορφισμός $j : R \to F$ ώστε για κάθε $x \in F$ να υπάρχουν $a, b \in R$ με $b \neq 0$ και*

$$x = \frac{ja}{jb}$$

(2) *Για κάθε σώμα F' που επεκτείνει το R δηλαδή υπάρχει ένας μονομορφισμός $f : R \to F'$ θα θα υπάρχει μοναδικός μονομορφισμός $g : F \to F'$ με $f = g \circ j$ δηλαδή το F' θα είναι μια επέκταση του F.*

Η απόδειξη του Θεωρήματος αυτού είναι η ίδια η κατασκευή του $F = \mathcal{Q}(R)$. Για να φανεί η αναλογία με την κατασκευή των ρητών θα χρησιμοποιούμε το συμβολισμό

$$\frac{a}{b}$$

αντί του

$$(a, b)$$

για ένα διατεταγμένο ζευγάρι στοιχείων a, b ενός συνόλου.

Θεωρούμε τώρα το σύνολο

$$\mathfrak{F} = R \times R \setminus \{0\} = \left\{ \frac{a}{b} : a, b \in R, \ \ b \neq 0 \right\}$$

στο οποίο ορίζουμε μια σχέση ισοδυναμίας

$$\frac{a}{b} \sim \frac{a'}{b'} \ \ \Leftrightarrow \ \ ab' = a'b$$

Ορίζουμε:

$$F = \mathcal{Q}(R) = \mathfrak{F}/_{\sim}$$

Θα συμβολίζουμε με

$$\left[\frac{a}{b}\right]$$

τη κλάση ισοδυναμίας του στοιχείου $\frac{a}{b} \in \mathfrak{F}$. Στο F ορίζουμε τις πράξεις:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right] \tag{2.37}$$

$$\left[\frac{a}{b}\right] \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right] \tag{2.38}$$

Επίσης θα ορίσουμε $j : R \to F$ από την

$$j(a) = \left[\frac{a}{1}\right] \tag{2.39}$$

Απομένει να ελέγξουμε τα παρακάτω:
Οι πράξεις είναι καλά ορισμένες στο F. Το F είναι σώμα με αυτές τις πράξεις. Η απεικόνιση $j : R \to F$ είναι μονομορφισμός. Ικανοποιούνται οι επιπλέον συνθήκες (1), (2) του Θεωρήματος.

Για να δείξουμε ότι οι πράξεις είναι καλά ορισμένες αρκεί να δείξουμε πως αν

$$\frac{a}{b} \sim \frac{a'}{b'}, \ \ \frac{c}{d} \sim \frac{c'}{d'}$$

τότε

$$\frac{ad + bc}{bd} \sim \frac{a'd' + b'c'}{b'd'}, \ \ \frac{ac}{bd} \sim \frac{a'c'}{b'd'}$$

το οποίο είναι θέμα στοιχειωδών πράξεων και το αφήνουμε στον αναγνώστη.

Επίσης είναι άμεσο ότι το F είναι σώμα με τις προηγούμενες πράξεις. Αφού επαληθεύσουμε ότι είναι αντιμεταθετικός δακτύλιος με μηδέν και μονάδα τα

$$0_F = \left[\frac{0}{1}\right], \quad 1_F = \left[\frac{1}{1}\right]$$

βλέπουμε αμέσως πως αν

$$x = \left[\frac{a}{b}\right] \neq 0$$

τότε $a \neq 0$ και

$$x^{-1} = \left[\frac{b}{a}\right]$$

αφού

$$xx^{-1} = \left[\frac{ab}{ab}\right] = \left[\frac{1}{1}\right]$$

δηλαδή κάθε μη μηδενικό στοιχείο αντιστρέφεται.

Επίσης αφού ορίσαμε την $j : R \to F$ με $j(a) = \left[\frac{a}{1}\right]$ είναι προφανές ότι η j είναι 1-1 και ότι

$$\begin{aligned} j(a+b) &= \left[\frac{a+b}{1}\right] = \left[\frac{a1+b1}{1\cdot 1}\right] = \left[\frac{a}{1}\right] + \left[\frac{b}{1}\right] = \\ &= j(a) + j(b) \end{aligned}$$

$$\begin{aligned} j(ab) &= \left[\frac{ab}{1}\right] = \left[\frac{ab}{1\cdot 1}\right] = \left[\frac{a}{1}\right]\left[\frac{b}{1}\right] = \\ &= j(a)j(b) \end{aligned}$$

Δηλαδή η j είναι μονομορφισμός. Επίσης αν $x = \left[\frac{a}{b}\right] \in F$ τότε

$$\begin{aligned} x &= \left[\frac{a}{1}\right]\left[\frac{1}{b}\right] = \left[\frac{a}{1}\right]\left(\left[\frac{b}{1}\right]\right)^{-1} = \\ &= j(a)(j(b))^{-1} = j(a)/j(b) \end{aligned}$$

Ας υποθέσουμε τώρα ότι η ακέραια περιοχή R περιέχεται ισομορφικά μέσα σε ένα άλλο σώμα F' δηλαδή υπάρχει ένας μονομορφισμός

$$f : R \to F'$$

Κάθε στοιχείο $x \in F$ γράφεται σαν

$$x = j(a)(j(b))^{-1}, a, b \in R, b \neq 0$$

και ορίζουμε

$$g : F \to F'$$

με

$$g(x) = j(f(a))(j(f(b)))^{-1}$$

Τότε η g είναι μονομορφισμός και

$$f = g \circ j$$

Με όλα αυτά το Θεώρημά μας αποδείχτηκε. Ας σημειώσουμε ότι μπορούμε να βλέπουμε το σώμα των πηλίκων μιας ακέραιας περιοχής ακριβώς με τον ίδιο τρόπο που βλέπουμε και το σύνολο των ρητών αριθμών σαν πηλίκα ακέραιων με τον παρανομαστή όχι 0. Δηλαδή, αν R μια ακέραια περιοχή μπορούμε να βλέπουμε το σώμα των πηλίκων της $\mathcal{Q}(R)$ σαν το σύνολο

$$\mathcal{Q}(R) = \left\{ \frac{a}{b} : a, b \in R, b \neq 0 \right\}$$

με τις συνηθισμένες πράξεις των κλασμάτων **Θεωρώντας** όμως ότι

$$\frac{a}{b} = \frac{c}{d}$$

οποτεδήποτε

$$ac - bd = 0$$

2.4 Δακτύλιοι πολυωνύμων σε περιοχές μονοσήμαντης ανάλυσης.

Αν μία ακέραια περιοχή είναι σώμα, τότε ο αντίστοιχος δακτύλιος των πολυώνύμων της $R[x]$ είναι Ευκλείδια Περιοχή και συνεπώς περιοχή μονοσήμαντης ανάλυσης. Αν όμως το R δεν είναι σώμα δεν μπορούμε να δείξουμε την ύπαρξη ενός αλγορίθμου διαίρεσης για τα πολυώνυμα στο $R[x]$.

Παρ'ολα αυτά είναι δυνατόν να έχουμε μονοσήμαντη ανάλυση ενός πολυωνύμου σε γινόμενο ανάγωγων πολυωνύμων ακόμα και αν ο δακτύλιος δεν είναι σώμα· Αν για παράδειγμα θεωρήσουμε τα πολυώνυμα με ακέραιους συντελεστές και μόνο υπάρχει μονοσήμαντη ανέλυση·

Στην παράγραφο αυτή θα δείξουμε ότι αν το R είναι περιοχή μονοσήμαντης ανάλυσης τότε το ίδιο θα συμβαίνει και για το $R[x]$. Αυτό είναι ένα σημαντικό αποτέλεσμα όχι μόνο γιατί μας εξασφαλίζει το μονοσήμαντο της ανάλυσης στο $\mathbb{Z}[x]$.

Ας ξεκινήσουμε από ένα σώμα και ας θεωρήσουμε τα πολυώνυμα **δύο** μεταβλητών x, y με συντελεστές από το σώμα R. Αυτά αποτελούν μία ακέραια περιοχή που συμβολίζεται με $R[x, y]$ και μπορούμε να την ταυτίσουμε (ισομορφικά) με την περιοχή $R[x][y]$ (δες και επόμενη παράγραφο για μια αυστηρή παρουσίαση). Αν για παράδειγμα $R = \mathbb{R}$ τότε τη έκφραση

$$1 + 2x + \sqrt{2}x^2y + x^5y^{13}$$

είναι ένα πολυώνυμο δύο μεταβλητών βαθμού 18=5+13. Όπως θα δούμε παρακάτω το $R[x, y]$ δεν είναι περιοχή κύριων ιδεωδών και συνεπώς δεν μπορεί να είναι Ευκλείδια περιοχή, με άλλα λόγια δεν μπορούμε να βρούμε **κανενός είδους** αλγόριθμο της διαίρεσης. Επειδή όμως το $R[x]$ είναι Ευκλείδια περιοχή άρα και περιοχή

μονοσήμαντης ανάλυσης τότε συμπεραίνουμε από το Θεώρημα που θα δείξουμε σε αυτή την παράγραφο ότι το $R[x,y]$ είναι περιοχή μονοσήμαντης ανάλυσης, και συνεπώς κάθε πολυώνυμο δύο μεταβλητών θα αναλύεται με ουσιαστικά μοναδικό τρόπο σε γινόμενο ανάγωγων πολυωνύμων (δύο μεταβλητών) και έτσι θα υπάρχει και μέδιστος κοινός διαιρέτης δύο ή περισσότερων πολυωνύμων. Προφανώς το αποτέλεσμα αυτό επακτείνεται (επαγωγικά) και για τους δακτύλιους πολυωνύμων n μεταβλητών για οποιοδήποτε πλήθος n μεταβλητών.

Σε αυτή την παράγραφο θα μελετήσουμε το δακτύλιο των πολυωνύμων μιας περιοχής μονοσήμαντης ανάλυσης R. Θυμίζουμε ότι σε μια τέτοια περιοχή τα ανάγωγα και τα πρώτα στοιχεία συμπίπτουν και ότι υπάρχει μέγιστος κοινός διαιρέτης για οποιοδήποτε πεπερασμένο πλήθος μη μηδενικών στοιχείων της.

Ορισμός 51 *Έστω R μια περιοχή μονοσήμαντης ανάλυσης και $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. Το $f(x)$ θα ονομάζεται* ***πρωταρχικό πολυώνυμο*** *αν έχει βαθμό $n\geq 1$ και η μονάδα είναι μέγιστος κοινός διαιρέτης των συντελεστών του.*
Με άλλα λόγια αν $f(x)=cg(x)$ με $c\in R$ τότε θα πρέπει το c να είναι αντιστρέψιμο στοιχείο της ακέραιας περιοχής.

Ένα βασικό Θεώρημα είναι το ακόλουθο:

Θεώρημα 35 (Το Λήμμα του Gauss)
Το γινόμενο δύο πρωταρχικών πολυωνύμων είναι πρωταρχικό πολυώνυμο.

Θα δείξουμε το Θεώρημα με δύο τρόπους. Ο πρώτος είναι άμεσος αλλά κάπως πιο περίπλοκος:

Πρώτη Απόδειξη του Θεωρήματος 35: Ας υποθέσουμε ότι $f(x)=a_0+\cdots+a_nx^n$, $g(x)=b_0+\cdots+b_mx^m$ είναι δύο πρωταρχικά πολυώνυμα. Θα θεωρούμε τα $f(x)=(a_i)_{i=0}^{\infty}$, $g(x)=(b_i)_{i=0}^{\infty}$, σαν δύο τελικά μηδενικές ακολουθίες. Αν $a_i=0$ και $p\in R$ θα θεωρούμε ότι $p|a_i$. Αυτό που πρώτα πρέπει να παρατηρήσει κανείς είναι ότι αν p είναι ανάγωγο (=πρώτο) στοιχείο του R τότε αναγκαστικά για κάποιο i, $p\not| a_i$ οπότε $a_i\neq 0$. Η ίδια παρατήρηση ισχύει και για την τελικά μηδενική ακολουθία $(b_i)_{i=0}^{+\infty}$.

$$f(x)g(x)=(c_i)_{i=0}^{+\infty}$$

με

$$c_0 = a_0b_0 \quad (0)$$
$$c_1 = a_0b_1 + a_1b_0 \quad (1)$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0 \quad (2)$$
$$\dots$$
$$c_i = \sum_{j+k=i} a_jb_k \quad (i)$$
$$\dots$$

Αν το $f(x)g(x)$ δεν ήταν πρωταρχικό θα υπήρχε ένας πρώτος $p \in R$ ο οποίος θα διαιρούσε τα $c_0, c_1, \dots c_i \dots$. Επειδή $p|a_0b_0 = c_0$ τότε είτε $p|a_0$ είτε $p|b_0$.
1η περίπτωση: $p|a_0$. Σε αυτή την περίπτωση θα υπάρχει ένα $i = 1, \dots, n$ με $p \not| a_i$ αφού το $f(x)$ είναι πρωταρχικό και έστω $i \geq 1$ να είναι τέτοιο ώστε $p|a_0, \dots p|a_{i-1}, p \not| a_i$. Αφού $p|c_i = a_0b_i + \dots + a_{i-1}b_1 + a_ib_0$ θα έχουμε ότι $p|a_ib_0$ οπότε αναγκαστικά $p|b_0$. Ας υποθέσουμε τώρα ότι έχουμε δείξει πως $p|b_0, \dots, p|b_{j-1}$. Επειδή $p|c_{i+j} = (a_0b_{i+j} + \dots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \dots + a_{i+j}b_0)$ και από υπόθεση το p διαιρεί τα εντός παρενθέσεων αθροίσματα θα έχουμε ότι $p|a_ib_j$ οπότε αναγκαστικά $p|b_j$. Αλλά αυτό σημαίνει ότι το $p|b_j$ για κάθε $j = 0, 1, \dots$ που σημαίνει ότι το $g(x)$ δεν είναι πρωταρχικό. Άτοπο.

2η περίπτωση: $p \not| a_0$. Σε αυτή την περίπτωση $p|b_0$ και ακριβώς όπως στην προηγούμενη περίπτωση δείχνουμε ότι $p|a_i$ για κάθε $i = 0, 1, \dots$ που επίσης είναι άτοπο αφού το $f(x)$ είναι πρωταρχικό. □

Η δεύτερη απόδειξη που θα κάνουμε είναι λιγότερο στοιχειώδης αλλά πιο απλή. Αν R είναι μια ακέραια περιοχή και I ένα ιδεώδες του R τότε το R_I είναι επίσης ακέραια περιοχή. Ο δακτύλιος $R/_I[x]$ αποτελείται από τα στοιχεία της μορφής $(a_i+I)_{i=0}^{\infty}$ με $a_i = 0$ όταν $i \geq i_0$ για κάποιο i_0. Ας ξεκινήσουμε με έναν φυσιολογικό ορισμό :

Ορισμός 52 *Έστω R μια περιοχή μονοσήμαντης ανάλυσης και $I \subset R$ ένα ιδεώδες: Η απεικόνιση*

$$\nu : R[x] \to R/I[x]$$

που ορίζεται από την σχέση

$$\nu_I(a_0 + \dots + a_nx^n) = (a_0 + I) + \dots + (a_n + I)x^n$$

θα ονομάζεται ***φυσικός επίμορφισμός*** *του $R[x]$ επί του $R/I[x]$*

Είναι άμεσο ότι η ν είναι πράγματι επιμορφισμός δακτυλίων.

Πρόταση 40 *Έστω R περιοχή μονοσήμαντης ανάλυσης και $f(x) = a_0 + \cdots + a_n x^n$ πολυώνυμο στην R βαθμού ≥ 1. Το $f(x)$ είναι πρωταρχικό αν και μόνο αν για κάθε πρώτο p ισχύει*

$$\nu_{(p)}(f) \neq 0$$

Απόδειξη: Ας υποθέσουμε ότι το $f(x) = a_0 + \cdots + a_n x^n$ είναι πρωταρχικό. Αν για κάποιο p πρώτο συνέβαινε $\nu_{(p)}(f) \neq 0$ τότε για κάθε i θα είχαμε πως $a_i + (p) = (p)$ δηλαδή πως $a_i \in (p)$ ή ισοδύναμα $p|a_i$, το οποίο είναι αδύνατο αν το $f(x)$ είναι πρωταρχικό πολυώνυμο.

Αντίστροφα, αν το $f(x)$ δεν είναι πρωταρχικό θα υπήρχε κάποιος πρώτος p ο οποίος θα διαιρούσε κάθε συντελεστή του a_i που θα σήμαινε πως $a_i + (p) = (p)$, ή ισοδύναμα $\nu_{(p)}(f) = 0$ $\square$

Δεύτερη Απόδειξη του Θεωρήματος 35: Ας υποθέσουμε ότι το γινόμενο δύο πολυωνύμων $f(x), g(x)$ βαθμού ≥ 1 δεν είναι πρωταρχικό. Από την προηγούμενη πρόταση θα υπάρχει κάποιος πρώτος $p \in R$ με την ιδιότητα

$$\nu_{(p)}(f(x)g(x)) = \nu_{(p)}(f(x))\nu_{(p)}(g(x)) = 0$$

Αλλά το $R/_{(p)}[x]$ είναι ακέραια περιοχή και συνεπώς θα έχουμε πως $\nu_{(p)}(f(x)) = 0$ είτε $\nu_{(p)}(g(x)) = 0$.
Σε κάθε περίπτωση, πάλι από των προηγούμενη Πρόταση είτε το $f(x)$ δεν θα είναι πρωταρχικό είτε το $g(x)$ δεν θα είναι πρωταρχικό, και οδηγούμαστε σε άτοπο. $\square$

Ας υποθέσουμε ότι έχουμε δύο ακέραιες περιοχές R, R' με την R να περιέχεται ισομορφικά μέσα στην R', δηλαδή υπάρχει κάποιος μονομορφισμός $j : R \to R'$. Τότε και το $R[x]$ θα περιέχεται φυσιολογικά μέσα στο $R'[x]$ και θα βλέπουμε κάθε πολυώνυμο $f(x) = a_0 + \cdots + a_n x^n \in R[x]$ και σαν πολυώνυμο του $R'[x]$ ταυτίζοντάς το με το $jf(x) = j(a_0) + \cdots + j(a_n)x^n \in R'[x]$. Αν το $jf(x)$ είναι ανάγωγο στην R' τότε αναγκαστικά και το $f(x)$ θα είναι ανάγωγο στην R αλλά αναγκαστικά δεν θα ισχύει το αντίστροφο[7]. Το παρακάτω σημαντικό Θεώρημα (που ουσιαστικά οφείλεται επίσης στον Gauss) μας λέει ότι ένα ανάγωγο πολυώνυμο σε μια περιοχή μονοσήμαντης ανάλυσης παραμένει ανάγωγο αν το δούμε μέσα στο σώμα των πηλίκων του.

Ας δείξουμε πρώτα ένα απλό αλλά ιδιαίτερα χρήσιμο λήμμα που προκύπτει από το Λήμμα του Gauss:

Λήμμα 5 *Αν R είναι μια περιοχή μονοσήμαντης ανάλυσης και F το σώμα των πηλίκων της R τότε για κάθε $f(x) \in F[x]$ υπάρχουν $a, b \in R$ και ένα πρωταρχικό πολυώνυμο $g(x) \in R[x]$ με*

$$f(x) = ab^{-1}g(x)$$

[7] Αν ένα πολυώνυμο είναι ανάγωγο σε μια περιοχή R είναι πιθανόν να μην είναι αν το δούμε σε μια «μεγαλύτερη» περιοχή ενώ σίγουρα θα είναι ανάγωγο σε μια «μικρότερη». Για παράδειγμα το $f(x) = x^2 - 2$ είναι ανάγωγο σαν στοιχείο του $\mathbb{Q}[x]$ αλλά όχι σαν στοιχείο του $\mathbb{R}[x]$.

Επιπλέον, Αν ένα πολυώνυμο $f(x) = cg(x) = c_1 g_1(x)$ όπου $c, c_1 \in F$ και τα $g(x), g_1(x)$ πρωταρχικά πολυώνυμα του $R[x]$ θα υπάρχει αντιστρέψιμο στοιχείο $u \in D$ με $c_1 = uc$ και $g(x) = ug_1(x)$.

Απόδειξη: Ας ξεκινήσουμε με ένα παράδειγμα. Ας υποθέσουμε ότι $R = \mathbb{Z}$ οπότε $F = \mathbb{Q}$ και ας πάρουμε

$$f(x) = \frac{3}{5} + 3x + \frac{3}{7}x^2$$

αν πάρουμε σαν $b = 35$ το ελάχιστο κοινό πολλαπλάσιο των παρανομαστών τότε

$$f(x) = b^{-1}bf(x) = 35^{-1}(21 + 105x + 15x^2)$$

Αν $a = 3$ είναι ο μέγιστος κοινός διαιρέτης των $21, 105, 15$ τοτε

$$f(x) = 3 \cdot 35^{-1}(7 + 35x + 5x^2)$$

όπου το $7 + 35x + 5x^2$ είναι ανάγωγο. Η απόδειξη στη γενική περίπτωση είναι εντελώς ανάλογη. Ένα στοιχείο $f(x) \in F[x]$ θα γράφεται στη μορφή[8]:

$$f(x) = \frac{a_0}{b_0} + \cdots + \frac{a_n}{b_n}x^n$$

με $a_0, \ldots, a_n, b_0, \ldots, b_n \in R$ με όλα τα b_i διαφορετικά από 0. Αν $b = b_0 \cdots b_n$ τότε $bf(x) \in R[x]$ και θεωρώντας το μέγιστο κοινό διαιρέτη a των συντεστών του $bf(x)$ θα έχουμε ότι $bf(x) = ag(x)$ με $g(x)$ **πρωταρχικό** πολυώνυμο του $R[x]$. Τελικά

$$f(x) = ab^{-1}g(x).$$

Ας υποθέσουμε τώρα ότι για κάποιο $f(x) \in R[x]$ έχουμε ότι

$$f(x) = cg(x) = c_1 g_1(x)$$

με $c, c_1 \in F$ και $g(x), g_1(x)$ πρωταρχικά πολυώνυμα του $R[x]$. Τα c, c_1 σαν στοιχεία του σώματος των πηλίκων μπορούν να γραφτούν σαν

$$c = \frac{a}{b}, \quad c_1 = \frac{a_1}{b}$$

με $a, a_1, binR$ και έτσι

$$ag(x) = a_1 g_1(c)$$

Επειδή το $g(x)$ είναι πρωταρχικό το a είναι μέγιστος κοινός διαιρέτης των συντελεστών του $ag(x)$. Όμως και το $g_1(x)$ είναι πρωταρχικό και ο μέγιστος κοινός διαιρέτης των συντελεστών του $a_1 g_1(x)$ που είναι ίδιος με με τον μέγιστο κοινό διαιρέτη των συντελεστών του $ag(x)$ θα είναι a_1. Άρα τα a, a_1 θα είναι και τα

[8] Για λόγους απλότητας, το τυπικό στοιχείο του F που είναι $j(a)/j(b)$, $a, b \in R, b \neq 0$ το γράφουμε $\frac{a}{b}$ με $a, b \in R$ και $b \neq 0$.

δύο μέγιστοι κοινοί διαιρέτες των συντελεστών του $ag(x)$ και συνεπώς ομόλογοι, δηλαδ••η θα υπάρχει ένα αντιστρέψιμο $u \in R$ με $a = ua_1$. Αν τώρα το $f(x)$ συντελεστές στο R και αν d είναι ένας μέγιστος κοινός διαιρέτης των συντελεστών του τότε $f(x) = dg_1(x)$ με $g_1(x)$ πρωταρχικό πολυώνυμο στο $R[x]$ και έτσι αν $f(x) = cg(x)$ με $c \in F$ και $g_1(x)$ πρωταρχικό πολυώνυμο στο $R[x]$ θα έχουμε ότι για ένα αντιστρέψιμο στοιχείο $u \in R$, $d = uc$ άρα $c \in R$. □

Θεώρημα 36

Έστω R μια περιοχή μονοσήμαντης ανάλυσης και F να είναι το σώμα των πηλίκων της R. Ένα πολυώνυμο $f(x) \in R[x]$ που είναι ανάγωγο στο R είναι και ανάγωγο μέσα στο $F[x]$.

Απόδειξη: Ας υποθέσουμε ότι το πολυώνυμο $f(x) = a_0 + \cdots + a_n x^n \in R[x]$ είναι ανάγωγο στο R αλλά δεν είναι ανάγωγο μέσα στο $F[x]$, δηλαδή υπάρχουν $g(x), h(x) \in F[x]$ με $f(x) = g(x)h(x)$. Από το προηγούμενο λήμμα θα έχουμε ότι $g(x) = ab^{-1}g_1(x), h(x) = cd^{-1}h_1(x)$ για κάποια $a, b, c, d \in R$ και $g_1(x), h_1(x)$ ανάγωγα πολυώνυμα του $R[x]$ και θα έχουμε ότι

$$(bd)f(x) = (ac)g_1(x)h_1(x)$$

Τα $g_1(x), h_1(x)$ είναι πρωταρχικά πολυώνυμα του $R[x]$ και από το Λήμμα του Gauss και το γινόμενό τους θα είναι πρωταρχικό. Αν διαιρέσουμε με το μέγιστο κοινό διαιρέτη των bd, ac θα καταλήξουμε σε μια σχέση

$$uf(x) = vG(x)$$

με τα $u, v \in R$ πρώτα μεταξύ τους και το $G(x)$ πρωταρχικό πολυώνυμο στο R. Ισχυριζόμαστε ότι το u είναι αντιστρέψιμο στοιχείο του R.
Πράγματι, σε διαφορετική περίπτωση θα υπήρχε ένας πρώτος p με $p|u$ και αφού $p \not| v$ θα έπρεπε ο p να διαιρεί όλους τους συντελεστές του $G(x)$ πράγμα αδύνατο αφού το $G(x)$ είναι πρωταρχικό. Συνεπώς θα έχουμε ότι

$$f(x) = v^{-1}uh_1(x)g_1(x)$$

με $v, u^{-1} \in R$ και $h_1(x), g_1(x)$ όχι σταθερά πολυώνυμα του $R[x]$ που αντιφάσκει στην αρχική υπόθεση ότι το $f(x)$ είναι ανάγωγο στο R. □

Πριν συνεχίσουμε την πορεία μας να δείξουμε ότι το $R[x]$ είναι περιοχή μονοσήμαντης ανάλυσης όταν είναι και το R ας δούμε πρώτα ποια είναι τα ανάγωγα στοιχεία του $R[x]$ τα οποία θα κατατάξουμε σε δύο κατηγορίες στην επόμενη πρόταση:

Πρόταση 41 *Αν R είναι μια περιοχή μονοσήμαντης ανάλυσης τότε τα ανάγωγα πολυώνυμα στο $R[x]$ είναι είτε*
(1) *Οι πρώτοι του R.*
(2) *Τα πρωταρχικά πολυώνυμα του $R[x]$ που είναι ανάγωγα σαν στοιχεία του $F[x]$ όπου F είναι το σώμα των πηλίκων του R.*

Απόδειξη: Έστω $f(x)$ ένα ανάγωγο πολυώνυμο στο $R[x]$. Διακρίνουμε δύο περιπτώσεις: Είτε το $f(x)$ είναι μηδενικού βαθμού δηλαδή ίσο με μια σταθερά c οπότε θα αντιστρέφεται αν και μόνο αν το c είναι αντιστρέψιμο στοιχείο του R και δείξαμε την περίπτωση (1) είτε θα έχει βαθμό ≥ 1. Σε αυτή την περίπτωση το γράφουμε σαν $f(x) = dg(x)$ όπου το $g(x)$ είναι πρωταρχικό και το d είναι ένας μέγιστος κοινός διαιρέτης των συντελεστών του $f(x)$. Φανερά το d θα είναι αντιστρέψιμο διαφορετικά από την περίπτωση (1) δεν θα ήταν ανάγωγο και έτσι μπορούμε να πάρουμε $d = 1$ δηλαδή το $f(x)$ είναι πρωταρχικό. Επίσης είναι και ανάγωγο στο $F[x]$ λόγω του Θεωρήματος 36. □

Με όσα έχουμε αποδείξει σε αυτή την παράγραφο έχουμε αρκετά για να αποδείξουμε το κύριο απότελεσμα αυτής της παραγράφου:

Θεώρημα 37

Αν R είναι μια περιοχή μονοσήμαντης ανάλυσης τότε και το $R[x]$, η περιοχή όλων των πολυωνύμων της, θα είναι επίσης. Ειδικά το $\mathbb{Z}[x]$ είναι περιοχή μονοσήμαντης ανάλυσης.

Απόδειξη: [9]

Έστω R να είναι μια περιοχή μονοσήμαντης ανάλυσης και F να είναι το σώμα των πηλίκων της. Κατ' αρχήν ας δείξουμε ότι κάθε πολυώνυμο $f(x) \in R[x]$ έχει μια ανάλυση σαν γινόμενο ανάγωγων πολυωνύμων. Αν δούμε το $f(x)$ στοιχείο του $F[x]$ τότε αυτό θα έχει μια και μοναδική ανάλυση

$$f(x) = g_1(x) \cdots g_k(x)$$

σε γινόμενο ανάγωγων πολυωνύμων **με συντελεστές από** F, αφού το F είναι σώμα και έχουμε ταυτότητα της διαίρεσης.

Όπως και στο Λήμμα 5 κάθε ένα από τα πολυώνυμα αυτά θα γράφεται

$$g_i(x) = ab^{-1} f_i(x)$$

όπου $a, b \in R$ και $f_i(x)$ πρωταρχικό πολυώνυμο στο $R[x]$ και προφανώς ανάγωγο στο $F[x]$ και συνεπώς και στο $R[x]$ Καταλήγουμε έτσι ότι

$$f(x) = cf_1(x) \cdots f_k(x) \tag{2.40}$$

με τα $f_1(x), \ldots, f_k(x)$ πρωταρχικά πολυώνυμα του $R[x]$, ανάγωγα και στο $R[x]$ και στο $F[x]$, και $c \in F$. Αν δείξουμε πως $c \in R$ θα έχουμε δείξει και την δυνατότητα της ανάλυσης σε γινόμενο ανάγωγων πολυωνύμων στο $R[x]$ γράφοντας το $c = p_1 \cdots p_m$ οπότε η

$$f(x) = p_1 \cdots p_m f_1(x) \cdots f_k(x) \tag{2.41}$$

[9] Αν κάποιος δυσκολεύται στις τεχνικές λεπτομέρειες της απόδειξης μπορεί να φαντάζεται ότι το R είναι η ακέραια περιοχή $\mathbb{Z}$ και το σώμα των πηλίκων της το $\mathbb{Q}$.

θα είναι η ζητούμενη ανάλυση. Αλλά αυτό είναι άμεσο πόρισμα του Λήμματος του Gauss, ειδικότερα του Λήματος 5. Ας υποθέσουμε τώρα ότι κάποιο πολυώνυμο $f(x) \in R[x]$ το αναλύαμε με δύο διαφορετικούς τρόπους σε γινόμενο ανάγωγων στοιχείων:

$$f(x) = p_1 \cdots p_m f_1(x) \cdots f_k(x) = q_1 \cdots q_n g_1(x) \cdots g_l(x) \tag{2.42}$$

όπου -κατά τα προηγούμενα-τα p_i, q_j είναι πρώτοι του R και τα $f_i(x), g_j(x)$ είναι πρωταρχικά πολυώνυμα ανάγωγα στο $F[x]$. Από το Λήμμα 5 θα έχουμε ότι για κάποιο αντιστρέψιμο στοιχείο $u \in R$ θα έχουμε

$$p_1 \cdots p_k = u q_1 \cdots q_l$$

και αφού το R είναι περιοχή μονοσήμαντης ανάλυσης θα έχουμε ότι $k = l$ και υπάρχει $\sigma_1 : \{1, \ldots, k\}$ ώστε το p_i να είναι ομόλογο με το $q_{\sigma_1(i)} = p_i$ για κάθε $i = 1, \ldots, k$.
Αν δούμε την σχέση 2.42 σαν ανάλυση του $f(x)$ στο σώμα F τότε από το μονοσήμαντο της ανάλυσης στο $F[x]$ θα πάρουμε ότι ότι $m = n$ και υπάρχει $\sigma_2 : \{1, \ldots, n\}$ ώστε το $f_j(x)$ να είναι ομόλογο με το $g_{\sigma_2(j)(x)} = f_j$ για κάθε $j = 1, \ldots, n$. Το θεώρημά μας αποδείχτηκε πλήρως. □

Θα κλείσουμε την παράγραφο αυτήν διατυπώνοντας ένα κριτήριο, γνωστο και σαν **Κριτήριο του Eisenstein**,για το πότε ένα πολυώνυμο σε μια περιοχή μονοσήμαντης ανάλυσης είναι ανάγωγο και παρουσιάζοντας μερικές εφαρμογές του.

Θεώρημα 38 *[Το κριτήριο του Eisenstein]*
Έστω R να είναι μια περιοχή μονοσήμαντης ανάλυσης και F το σώμα των πηλίκων της. Ας υποθέσουμε ακόμα ότι μας δίνεται ένα μη σταθερό πολυώνυμο

$$f(x) = a_0 + \cdots + a_n x^n, \;\; a_n \neq 0$$

στο $R[x]$ και ότι μπορούμε να βρούμε ένα πρώτο $p \in R$ με τις εξής ιδιότητες:
(1) *Ο p διαιρεί τους $a_0, \ldots, a_{n-1}$.*
(2) *Ο p δεν διαιρεί τον a_n.*
(3) *Ο p^2 δεν διαιρεί τον a_0.*
Τότε το $f(x)$ είναι ανάγωγο στο $F[x]$.

Απόδειξη: Μπορούμε να υποθέσουμε ότι το $f(x)$ είναι πρωταρχικό. Αν δεν είναι γράφουμε το $f(x) = dg(x)$ με $g(x)$ ανάγωγο και οι συνθήκες θα ικανοποιούνται για το $g(x)$, όπως εύκολα βλέπουμε. Αν λοιπόν δείξουμε ότι το $g(x)$ είναι ανάγωγο στο $F[x]$ τότε το έχουμε δείξει και για το $f(x)$.

Θα δείξουμε πρώτα ότι -με την υπόθεση ότι είναι πρωταρχικό- το $f(x)$ είναι ανάγωγο στο R οπότε από το Θεώρημα 36 θα είναι και ανάγωγο σαν στοιχείο του

$F[x]$. Αν δεν ήταν ανάγωγο θα είχαμε ότι $f(x) = g(x)h(x)$ με τα $g(x), h(x)$ μη σταθερά πολυώνυμα. Ας υποθέσουμε ότι

$$f(x) = a_0 + \cdots + a_n x^n$$
$$g(x) = b_0 + \cdots + b_k x^k$$
$$h(x) = c_0 + \cdots + c_l x^l$$

όπου $k, l \geq 1$ και $k+l = n$. Επειδή $a_0 \neq 0$ (η συνθήκη (2» θα έχουμε $b_0 \neq 0, c_0 \neq 0$. Επειδή $p|a_0 = b_0 c_0$ θα διαιρεί είτε τον b_0 είτε τον c_0 αλλά όχι και τους δύο γιατί θα παραβιαζόταν η συνθήκη (3).

Ας υποθέσουμε λοιπόν ότι διαιρεί τον c_0 και δεν διαιρεί τον b_0. Θα δείξουμε επαγωγικά ότι διαιρεί και κάθε c_i, $i = 0, \ldots, l$. Πράγματι, ας υποθέσουμε ότι διαιρεί τους $c_0, \ldots, c_{i-1}$. Τότε $a_i = (c_0 b_i + c_1 b_{i-1} + \cdots + c_{i-1} b_1) + c_i b_0$. Αφού $i \leq l < n$ θα έχουμε από τις υποθέσεις μας ότι $p|a_i$ και αφού $p|c_0, \ldots, p|c_{i-1}$ θα έχουμε ότι $p|c_i b_0$. Όμως ο p δεν διαιρεί τον b_0 και συνεπώς θα διαιρεί τον c_i και τελικά θα διαιρεί τον c_l. Όμως $a_n = c_l b_k$ και θα έχουμε ότι ο p θα διαιρεί τον a_n που αντιφάσκει στην συνθήκη (2). □

Πρόταση 42 *Αν ένας ρητός $\frac{a}{b}$ με $(a,b) = 1$ είναι ρίζα του πρωταρχικού πολυωνύμου $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ με ακέραιους συντελεστές τότε $a|a_0,\ b|a_n$*

Απόδειξη: Αν ο $\frac{a}{b}$ με $(a,b) = 1$ είναι ρίζα του πρωταρχικού πολυωνύμου $f(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$ τότε πολλαπλασιάζοντας με b^n θα έχουμε:

$$a_0 b^n + a_1 a b^{n-1} + \cdots + a_{n-1} b a^{n-1} + a_n a^n = 0$$

Που δίνει άμεσα ότι $b|a^n a_n$. Αφού οι a, b είναι πρώτοι μεταξύ τους θα πρέπει $b|a_n$. Όμοια $a|b^n a_0$ και πάλι θα πρέπει $a|a_0$. □

Από το Κριτήριο του Eisenstein θα πάρουμε εύκολα τα επόμενα:

Πρόταση 43 *Αν a είναι φυσικός αριθμός για τον οποίο υπάρχει ένας πρώτος p με $p|a$ και $p^2 \not| a$ τότε για κάθε $n \geq 1$ το πολυώνυμο $x^n - a$ θα είναι ανάγωγο στους ρητούς. Ειδικά ο $\sqrt[n]{a}$ θα είναι άρρητος αριθμός για $n \geq 2$.*

Πρόταση 44 *Έστω p πρώτος φυσικός αριθμός. Το πολυώνυμο $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$ είναι ανάγωγο.*

Υπόδειξη: Γράφουμε

$$f(x) = \frac{x^p - 1}{x - 1}.$$

Με το Κριτήριο του Eisenstein δείχνουμε ότι το $f(x+1) = p + \binom{p}{1} x + \binom{p}{2} x^2 + \cdots + x^{p-2}$ είναι ανάγωγο, οπότε αναγκαστκά θα είναι και το $f(x)$.

2.5 Δακτύλιοι Πολυωνύμων πολλών μεταβλητών

Ας υποθέσουμε ότι R είναι ένας δακτύλιος. Αυτός ορίζει έναν άλλο δακτύλιο $R[x]$ που είναι όλες οι τελικά μηδενικές ακολουθίες στοιχείων του τις ταυτίζουμε με όλα τα πολυώνυμα μιας μεταβλητής x. Αν πάρουμε όλες τις τελικά μηδενικές ακολουθίες του $R[x]$ τότε κατασκευάζεται ένας νέος δακτύλιος $R[x,y]$ που μπορούμε να τον ταυτίσουμε με τα πολυώνυμα δύο μεταβλητών x, y πάνω στον R. Ίσως αυτό να μη φαίνεται με την πρώτη ματιά.
Ας θεωρήσουμε λοιπόν μια οποιαδήποτε πεπερασμένη ακολουθία

$$f_0, f_1, \ldots, f_n$$

από στοιχεία του $R[x]$. Τότε αυτή μπορούμε να την ταυτίσουμε με το πολυώνυμο

$$F(x,y) = f_0 + f_1 y + f_2 y^2 + \cdots + f_n y^n$$

Για να έχουμε μία σαφέστερη εικόνα ας υποθέσουμε ότι

$$\begin{aligned} f_0 &= a_0 x^{k_0} \\ f_1 &= a_1 x^{k_1} \\ f_2 &= a_2 x^{k_2} \\ &\cdots\cdots \\ f_n &= a_n x^{k_n} \end{aligned}$$

Τότε

$$F(x,y) = a_0 x^{k_0} + a_1 x^{k_1} y + a_2 x^{k_2} + \cdots + a_n x^{k_n} y^n$$

Δεν είναι δύσκολο να δούμε πως τα στοιχεία του $R[x,y]$ μπορούμε γενικά να τα θέσουμε στη μορφή:

$$F(x,y) = a_0 + a_1 x^{k_1} y^{m_1} + a_2 x^{k_2} y^{m_2} + \cdots + a_n x^{k_n} y^{m_n}$$

Ένας άλλος τρόπος να δούμε τα πολυώνυμα δύο μεταβλητών είναι σαν τελικά μηδενικές διπλές ακολουθίες

$$(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$$

Ας προσπαθήσουμε έναν αυστηρό ορισμό:

Ορισμός 53 *Διπλή ακολουθία με στοιχεία από ένα δακτύλιο R είναι μία απεικόνιση $a : \mathbb{N}\times\mathbb{N} \to R$, που θα συμβολίζεται και με*

$$(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$$

*Μία διπλή ακολουθία $(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$ θα λέγεται **τελικά μηδενική** αν υπάρχουν δύο $i_0, j_0 \in \mathbb{N}$ με $a_{ij} = 0$ για οποιαδήποτε $i \geq i_0, j \geq j_0$.*
*Ο **βαθμός** μίας τελικά μηδενικής ακολουθίας διαφορετικής από την μηδενική (δηλαδή αυτή που είναι ταυτοτικά ίση με 0) ορίζεται σαν*

$$\max\{i+j : a_{ij} \neq 0\}$$

Η τελικά μηδενική ακολουθία $(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$ θα ταυτίζεται με το πολυώνυμο

$$F(x,y)=\sum_{i=0,j=0}^{i=n,j=m} a_{ij}x^iy^j$$

που έχει **βαθμό** $n+m$.

Για παράδειγμα τα

$1+x+x^2+x^3+x^4$
$1+y+x^2+y^3+x^4$
y^2x^2
$1+xy+x^2y^2+x^3y+x^4$
$1+x+x^2y^2+x^3+x^4+y^4$
$1+(\sqrt{2}+5i)x+x^2+x^3+x^4+y+y^2+y^3+y^4$
$1+x+x^2+x^3+x^4+y+y^2+y^3+y^4+xy+ixy^2+x^2y+\sqrt{-10}x^2y^2+xy^3+x^3y$

Είναι όλα πολυώνυμα στο $\mathbb{C}[x,y]$.

Τώρα είμαστε σε θέση να ορίσουμε αυστηρά τις πράξεις στο $R[x,y]$ σαν πράξεις σε διπλές ακολουθίες[10]:

$$(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}+(b_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}=(a_{ij}+b_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$$

$$(a_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}\cdot(b_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}=(c_{ij})_{(i,j)\in\mathbb{N}\times\mathbb{N}}$$

όπου

$$c_{ij}=\sum_{k=0,l=0}^{k=i,l=j} a_{kl}b_{i-k,j-l}$$

Ας ορίσουμε όπως στην περίπτωση πολυωνύμων μίας μεταβλητής μία εκτίμηση για τα πολυώνυμα δύο μεταβλητών

$$N:R[x,y]\to\mathbb{N}$$

ακριβώς όπως και στα πολυώνυμα μίας μεταβλητής:

$$N(f)=\begin{cases}0 & \text{αν } f=0\\ (\text{βαθμός του } f)+1 & \text{αν } f\neq 0\end{cases}$$

[10] Για τον αναγνώστη που πιθανόν να ανησυχήσει από τον σχετικά πολύπλοκο τρόπο που ορίζεται ο πολλαπλασιασμός αναφέρουμε ότι μπορεί να τον αγνοήσει και να πολλαπλασιάζει πολυώνυμα πολλών μεταβλητών σαν αλγεβρικές εκφράσεις με τον τρόπο που ξέρει

Και εδώ θα έχουμε για $f \in R[x,y]$ με R να είναι ένα σώμα:

$$\begin{aligned} &N(f) = 0 \text{ αν και μόνο αν } \quad f = 0 \\ &N(f+g) = \max\{N(f), N(g)\} \\ &N(fg) = N(f) + N(g) - 1 \end{aligned}$$

άρα έχουμε μία Ευκλείδια εκτίμηση και έτσι μπορούμε να αναρωτηθούμε αν μπορούμε να έχουμε και Άλγόριθμο της Διαίρεσης δηλαδή αν είμαστε σε Ευκλείδια Περιοχή.
Η απάντηση είναι ΟΧΙ.

Πρόταση 45 *Έστω R ένα μη τετριμμένο σώμα*[11] *τότε το υποσύνολο*

$$I = \{f(x,y) \in R[x,y] : f(0,0) = 0\}$$

είναι ένα γνήσιο ιδεώδες με δύο γεννήτορες και δεν είναι κύριο ιδεώδες. Συνεπώς το $R[x,y]$ δεν είναι Περιοχή Κύριων Ιδεωδών και συνεπώς ούτε Ευκλείδια Περιοχή.

Απόδειξη: Το

$$I = \{f(x,y) \in R[x,y] : f(0,0) = 0\}$$

ειναι το σύνολο των πολυωνύμων με δύο συντελεστές που ο σταθερός τους όρος είναι ίσο με 0. Είναι άμεσο ότι αυτό είναι ένα ιδεώδες και μάλιστα

$$I = (x,y)$$

Το I δεν μπορεί να παράγεται από ένα μόνο στοιχείο $f \in R[x,y]$. Πράγματι ας υποθέσουμε ότι

$$I = (f) = \{gf : g \in R[x,y]\}$$

Αφού $x, y \in I$ θα έχουμε

$$x = g_1 f, \qquad y = g_2 f$$

για κάποια πολυώνυμα $g_1, g_2 \in R[x,y]$. Άλλά τα x, y είναι πρώτου βαθμού και η μόνη περίπτωση για να συμβαίνουν τα προηγούμενα είναι

$$f = ax = by$$

για κάποια $a, b \in R$ μη μηδενικά στοιχεία του σώματος πράγμα προφανώς αδύνατον. □

Ας υποθέσουμε ότι έχουμε μια περιοχή μονοσήμαντης ανάλυσης R τότε από το Θεώρημα 37 το $R[x]$ θα είναι περιοχή μονοσήμαντης ανάλυσης αλλά τότε και το $R[x,y] = R[x][y]$ θα είναι επίσης, οπότε το ίδιο θα συμβαίνει και για το $R[x,y,z]$ το δακτύλιο των πολυωνύμων τριών μεταβλητών. Αποδείξαμε λοιπόν ότι:

[11] να έχει τουλάχιστον 2 στοιχεία

Θεώρημα 39 *Αν R είναι μια περιοχή μονοσήμαντης ανάλυσης τότε για κάθε n η περιοχή $R[x_1, \ldots, x_n]$ των πολυωνύμων n μεταβλητών θα είναι περιοχή μονοσήμαντης ανάλυσης.*

Το $R[x, y]$ από τα προηγούμενα δεν είναι περιοχή κυρίων ιδεωδών, ακόμα και αν το R είναι σώμα, ωστόσο θα είναι από το προηγούμενο Θεώρημα περιοχή μονοσήμαντης ανάλυσης. Έχουμε λοιπόν,

Υπάρχουν Περιοχές μονοσήμαντης Ανάλυσης που δεν είναι Περιοχές Κύριων ιδεωδών