Θεωρία Δακτυλίων-2η Πρόοδος

1. Να δείξετε ότι σε μια περιοχή κύριων ιδεωδών δύο οποιαδήποτε μη μηδενικά στοιχεία a, b έχουν μέγιστο κοινό διαιρέτη d που γράφεται στην μορφή $d = ax + by$.

Λύση: Θεωρούμε το ιδεώδες $J = (a, b)$ που παράγεται από τα στοιχεία a, b. Επειδή το R είναι περιοχή κύριων ιδεωδών θα υπάρχει ένα $d \in R$ με

$$J = \{ax + by : x, y \in R\} = (d) = \{xd : x \in R\}$$

Επειδή $a \in J$ θα έχουμε ότι $a \in (d)$ δηλαδή $d|a$.

Όμοια $d|b$, και συνεπώς το d είναι κοινός διαιρέτης και επειδή $d \in J$, ο d θα γράφεται στην μορφή

$$d = ax + by \tag{1}$$

για κάποια $x, y \in R$.

Έστω τώρα d' ένας κοινός διαιρέτης των a, b. Τότε θα υπάρχουν $m, n \in R$ με

$$a = md', \quad b = nd' \tag{2}$$

Από τις εξισώσεις 1, 2 θα έχουμε ότι

$$d = ax + by = md'x + nd'y = d'(mx + ny)$$

Συνεπώς $d'|d$ δηλαδή ο d είναι ένας κοινός διαιρέτης των a, b διαιρείται από οποιονδήποτε κοινό διαιρέτη των a, b, που σημαίνει ότι είναι ένας μέγιστος κοινός διαιρέτης.

2. Σε μια περιοχή κύριων ιδεωδών R ένα ιδεώδες είναι μεγιστικό αν και μόνο αν παράγεται από πρώτο.

Λύση: Ας υποθέσουμε ότι ένα ιδεώδες J είναι μεγιστικό. Αφού είμαστε σε περιοχή κύριων ιδεωδών το J παράγεται από κάποιο στοιχείο $p \in R$. Το p δεν είναι ούτε αντιστρέψιμο ούτο το μηδέν γιατί το J δεν είναι τετριμμένο ιδεώδες. Θα δείξουμε ότι είναι πρώτος. Αρκεί να δείξουμε ότι είναι ανάγωγο, αφού σε μια περιοχή κύριων ιδεωδών τα πρώτα και τα ανάγωγα στοιχεία συμπίπτουν. Ας υποθέσουμε ότι το p δεν είναι πρώτος, τότε το $p = ab$ για κάποια μη μηδενικά και μη αντιστρέψιμα στοιχεία του R. Τότε $J = (p) \subset (a)$. Τό $(a) \neq R$ αφού το a δεν είναι αντιστρέψιμο, συνεπώς θα πρέπει $(a) = J = (p)$, γιατί υποθέτουμε ότι το J είναι μεγιστικό. Αλλά τότε $a = xp$ για κάποιο $x \in R$, οπότε $p = ab = bxp$ που συνεπάγεται ότι $1 = bx$ δηλαδή το b είναι αντιστρέψιμο, άτοπο.

Αντίστροφα, Ας υποθέσουμε ότι p είναι πρώτος και $J = (p)$. Θα δείξουμε ότι το J είναι μεγιστικό. Πράγματι, $J \neq (0), J \neq R$ γιατί το p σαν πρώτος δεν είναι ούτε το μηδέν ούτε αντιστρέψιμο στοιχείο. Άρα το J είναι μη τετριμένο ιδεώδες.

Αν τώρα $J \subset I$ με I ιδεώδες, αφού είμαστε σε περιοχή κύριων ιδεωδών θα έχουμε ότι $I = (a)$ για κάποιο $a \in R$. Η σχέση $(p) \subset (a)$ μας λέει ότι $a|p$ και επειδή το p είναι πρώτος είτε $a = pu$ για κάποιο αντιστρέψιμο $u \in R$ οπότε $J = I$ είτε το a θα είναι αντιστρέψιμο οπότε $I = R$, που δείχνει την μεγιστικότητα του J.

3. Το $\mathbb{Z}[x]$ είναι περιοχή μονοσήμαντης ανάλυσης (Gauss). Δείξτε ότι δεν είναι περιοχή κύριων ιδεωδών.

Λύση: Ας θεωρήσουμε το ιδεώδες $I = (2, x)$ που παράγεται από τα πολυώνυμα $x, 2 \in \mathbb{Z}[x]$. Αν το $\mathbb{Z}[x]$ ήταν περιοχή κύριων ιδεωδών ο μέγιστος κοινός διαιρέτης των $x, 2$, που είναι το 1, θα γραφόταν

$$1 = 2f + xg \tag{3}$$

για κάποια πολυώνυμα $f = a_0 + \cdots + a_k x^k, g = b_0 + \cdots + b_k x^k$ με ακέραιους συντελεστές. Από την εξίσωση (3) θα είχαμε ότι $2a_0 = 1$ που είναι αδύνατον.

4.Να δείξετε ότι το υπόλοιπο της διαίρεσης ενός πολυωνύμου $f(x) \in \mathbb{R}[x]$ με $x^2 + a^2$ είναι το

$$v(x) = \frac{f(ai) + f(-ai)}{2} + \frac{f(ai) - f(-ai)}{2ai}\, x$$

όπου όμως το $f(x)$ το θεωρούμε σαν στοιχείο του $\mathbb{C}[x]$ και i είναι η φανταστική μονάδα (i^2=-1). Δικαιολογείστε επίσης γιατί $v(x) \in \mathbb{R}[x]$.

Λύση: Αν θεωρήσουμε το $f(x)$ σαν στοιχείο του $\mathbb{C}[x]$ και $v(x) = kx + l$ το υπόλοιπο της διαίρεσης του $f(x)$ με $x^2 + a^2$ θα έχουμε ότι $f(x) = (x^2 + a^2)g(x) + kx + l$. Θέτοντας $x = ai$, $x = -ai$ στην προηγούμενη εξίσωση θα έχουμε

$$f(ai) = aki + l \tag{4}$$
$$f(-ai) = -aki + l \tag{5}$$

και λύνοντας το προηγούμενο σύστημα ως πρός k, l έχουμε το επιθυμητό αποτέλεσμα.

Επειδή το $f(x)$ έχει πραγματικούς συντελεστές θα έχουμε ότι $f(-ai) = \overline{f(ai)}$ και τα ak, l θα είναι το πραγματικό και φανταστικό μέρος του αριθμού $f(ai)$ (μπορείτε να το δείτε άμεσα και από τις εξισώσεις 4, 5) δηλαδή θα είναι πραγματικοί αριθμοί.

5.Να βρείτε το υπόλοιπο της διαίρεσης του $x^n + 1$ με $x^2 + 1$.

Λύση: Αρκεί από το προηγούμενο ερώτημα να βρούμε το παραγματικό και φανταστικό μέρος του $in+1$ για τις διάφορες τιμές του n. Επειδή $i^2=-1, i^3=-i, i^4=1$ θα έχουμε άμεσα

$$i^n+1=\begin{cases}2+0i & \text{αν το } n \text{ είναι της μορφής } 4k\\ 1+i & \text{αν το } n \text{ είναι της μορφής } 4k+1\\ 0+0i & \text{αν το } n \text{ είναι της μορφής } 4k+2\\ 1-i & \text{αν το } n \text{ είναι της μορφής } 4k+3\end{cases}$$

και το υπόλοιπο της διαίρεσης θα είναι:

$$v(x)=\begin{cases}2 & \text{αν το } n \text{ είναι της μορφής } 4k\\ 1+x & \text{αν το } n \text{ είναι της μορφής } 4k+1\\ 0 & \text{αν το } n \text{ είναι της μορφής } 4k+2\\ 1-x & \text{αν το } n \text{ είναι της μορφής } 4k+3\end{cases}$$

6. Να δείξετε ότι για κάθε $a\in\mathbb{R}$ το $\mathbb{R}/(x-a)$ είναι ισόμορφο με το $\mathbb{R}$. (Να δείξετε ότι η απεικόνιση $T:\mathbb{R}[x]\to\mathbb{R}$ με $T(f)=f(a)$ είναι επιμορφισμός και να βρείτε τον πυρήνα της. Μετά θυμηθείτε ότι για κάθε επιμορφισμό $T:R\to S$ ισχύει $R/_{\mathrm{Ker}T}\cong S$)

Λύση: Επαληθεύουμε ότι ο $T:\mathbb{R}[x]\to\mathbb{R}$ με $T(f)=f(a)$ είναι ομομορφισμός: $T(f+g)=(f+g)(a)=f(a)+g(a)=Tf+Tg$, $T(fg)=(fg)(a)=f(a)g(a)=Tf\,Tg$. Για να δείξουμε ότι είναι επί, παρατηρούμε ότι πάρουμε οποιοδήποτε $r\in\mathbb{R}$. και $f=x+(r-a)$ τότε $T(f))=r$.

Ο πυρήνας του T είναι

$$\mathrm{Ker}T=\{f:Tf=0\}=\{f:f(a)=0\}=\{f:x-a|f=0\}=(x-a)$$

και από το θεώρημα ομομορφισμού:

$$\mathbb{R}[x]/\mathrm{Ker}T=\mathbb{R}[x]/(x-a)\cong\mathbb{R}$$

7. Ας υποθέσουμε ότι έχουμε δύο πολυώνυμα $f,g\in\mathbb{R}$ τα οποία διαιρούμενα με x^2+1 αφήνουν υπόλοιπα $x+1$ και $x-1$ αντίστοιχα. Ποιά θα είναι τα υπόλοιπα της διαίρεσης των $f+g$, fg με x^2+1; (1.5)

Λύση: Ας δούμε κάτι πιο γενικό: Ας υποθέσουμε ότι έχουμε δύο πολυώνυμα $f,g\in\mathbb{R}$ τα οποία διαιρούμενα με h αφήνουν υπόλοιπα v και w αντίστοιχα. Δηλαδή $f=hP+v$, $g=hQ+w$ που τα v,w έχουν βαθμό μικρότερο από του h. Πολλαπλασιάζοντας, $fg=h(PQ+v+w)+vw$. Το vw ΔΕΝ είναι πάντοτε το υπόλοιπο της διαίρεσης με h άφού μπορεί να έχει βαθμό μεγαλύτερο ή ίσο. Αν

όμως διαιρέσουμε το vw με h και $vw = Rh + u$ με το u να έχει βαθμό μικρότερο από αυτόν του h τότε $fg = h(PQ + v + w + R) + u$ και το u είναι το υπόλοιπο της διαίρεσης του fg με το h.

Στην συγκεκριμένη περίπτωση, $f = (x^2+1)P + x + 1$, $g = (x^2+1)Q + x - 1$ και άρα :

$$\begin{aligned} fg &= (x^2+1)(PQ + xP - P + xQ + Q) + x^2 - 1 = \\ &= (x^2+1)(PQ + xP - P + xQ + Q) + (x^2+1) - 2 = \\ &= (x^2+1)(PQ + xP - P + xQ + Q + 1) - 2 \end{aligned}$$

δηλαδή το υπόλοιπο είναι -2. Για το άθροισμα προφανώς το υπόλοιπο είναι το άθροισμα των υπολοίπων, δηλαδή $2x$.

8. Δείξτε ότι για κάθε $a \in \mathbb{R}, a \neq 0$ το $\mathbb{R}[x]/(x^2 + a^2)$ είναι ισόμορφο με το $\mathbb{C}$.

Λύση: Έστω $a \in \mathbb{R}$, $a \neq 0$. Θεωρούμε την $T : \mathbb{R}[x] \to \mathbb{C}$ με $T(f) = f(ai)$ που είναι προφανώς ομομορφισμός. Είναι και επιμορφισμός αφού για κάθε $k + il \in \mathbb{C}$ και $f = \frac{k}{a}x + l$ θα έχουμε ότι $T(f) = k + li$. Ο πυρήνας της T είναι το σύνολο όλων των πολυωνύμων f με $f(ai) = 0$ το οποίο από το Θέμα 4 συμβαίνει όταν και μόνο όταν το $x^2 + a^2$ διαιρεί το f. Με άλλα λόγια, $\mathrm{Ker}f = (x^2 + a^2)$ και τελικά (δες και το Θέμα 6)

$$\mathbb{R}[x]/\mathrm{Ker}T = \mathbb{R}[x]/(x^2 + a^2) \cong \mathbb{C}$$

9. Έστω $f(x) \in \mathbb{R}[x]$ πολυώνυμο βαθμού ≥ 3. Μπορεί το $\mathbb{R}[x]/(f(x))$ να είναι σώμα; (Δες και το Θέμα 2).

Λύση: Από το Θεμελιώδες Θεώρημα της Άλγεβρας τα μόνα ανάγωγα πολυώνυμα στο $\mathbb{R}[x]$ είναι της μορφής $c(x-a), c((x-a)^2 + b^2)$ με $a, b, c \in \mathbb{R}$ και $b \neq 0$. Συνεπώς κάθε πολυώνυμο βαθμού ≥ 3 δεν είναι ανάγωγο και επειδή το $\mathbb{R}[x]$ είναι Ευκλείδια Περιοχή (και συνεπώς περιοχή κύριων ιδεωδών) το $(f(x))$ δεν είναι μεγιστικό ιδεώδες και συνεπώς το $\mathbb{R}[x]/(f(x))$ δεν θα είναι σώμα.

10. Δείξτε ότι για κάθε $n \geq 1$ μπορούμε να βρούμε άπειρα μη ομόλογα ανά δύο πολυώνυμα βαθμού n στο $\mathbb{Q}[x]$ που είναι ανάγωγα (=πρώτοι) στο $\mathbb{Q}[x]$. (Υπόδειξη: Κριτήριο του Eisenstein) Ισχύει το ίδιο για τα $\mathbb{R}[x]$, $\mathbb{C}[x]$;

Λύση: Έστω $n \geq 1$ και p πρώτος. Από το Κριτήριο του Eisenstein το πολυώνυμο $f_p(x) = x^n + p$ είναι ανάγωγο δηλαδή πρώτος του $\mathbb{Q}[x]$. Επειδή το σύνολο των πρώτων είναι άπειρο για κάθε $n \geq 1$ έχουμε βρεί άπειρα ανάγωγα πολυώνυμα του $\mathbb{Q}[x]$ βαθμού n. Στο δεύτερο Ερώτημα η απάντηση είναι αρνητική γιατί αν $n \geq 3$ δεν υπάρχει πολύωνυμο βαθμού n το οποίο να είναι ανάγωγο στο $\mathbb{R}[x]$ και το ίδιο συμβαίνει στο $\mathbb{C}[x]$ για κάθε $n \geq 2$. (Δες και τη λύση του προηγούμενου Θέματος).