140/140

Άλγεβρα Ι(Μ)

Λύσεις Ασκήσεων-Φυλλαδίο 9

Τσάνγκο Ιωσήφ

24 Απριλίου 2017

1. Έχω ότι R δακτύλιος, S υποδακτύλιος και I ιδεώδες του R.

   (**Σχόλιο**:Το πλήθος των απαντήσεων μου είναι ίδιο με αυτό των ερωτήσεων, εξαιτίας όμως της χρήσης του στίγματος, ίσως προκύψει η αντύπωση ότι λείπει κάποια απάντηση.)

   (α′) Λάθος. Έστω F σώμα και θεωρώ τον δακτύλιο πολυωνύμων $S = F[X_1, X_2, ...]$, επιπλέον παίρνω το σώμα πηλίκων του S, έστω $R = F(X_1, X_2, ...)$. Άρα έχω $S \subseteq R$ και R σώμα άρα PID άρα $Noetherian$, ωστόσο ο δακτύλιος S δεν είναι $Noetherian$ αφού η αλυσίδα ιδεωδών του $S < X_1 > \subsetneq < X_1, X_2, ... > \subsetneq ...$ δεν γίνεται ποτέ σταθερή.

   (β′) Σωστό. Αν θεωρήσω τον κανονικό επιμορφισμό $\phi : R \longrightarrow R/I$ έπεται απο θεωρία ότι R/I είναι $Noetherian$

   (γ′) Λάθος. Αν θεωρήσω $R = \mathbb{Q}$, $S = \mathbb{Z}$ τότε προφανώς έχω ότι $S = \mathbb{Z}$ υποδακτύλιος του $R = \mathbb{Q}$, με $\mathbb{Q}$ $Artinian$ (τετριμμένα) αφού είναι σώμα και ως γνωστό απο θεωρία $\mathbb{Z}$ είναι $Noetherian$ αλλά όχι $Artinian$.

   (δ′) Σωστό. Αν Θεωρήσω ξανά τον κανονικό επιμορφισμό $\phi : R \longrightarrow R/I$ για κάθε φθίνουσα αλυσίδα ιδεωδών του R/I προκύπτει απο *correspondence theorem*, μία φθίνουσα αλυσίδα ιδεωδών του R, που από υπόθεση γνωρίζω ότι είναι $Artinian$, άρα τελικά γίνεται σταθερή. Επομένως, αν υποθέσω ότι υπάρχει φθίνουσα αλυσίδα ιδεωδών του R/I που δεν σταθεροποιείται τελικά, θα οδηγηθώ σε άτοπο, άρα R/I είναι $Artinian$.

   (ε′) Λάθος. Έστω $R = \mathbb{Q}[X]$, $S = \mathbb{Z}[X]$ τότε R είναι Ευκλείδια περιοχή, άρα $P.I.D$(αφού $\mathbb{Q}$ σώμα) και S όχι(όπως είδαμε στο μάθημα το ιδεώδες $< 2, X >$ του S δεν είναι κύριο).

   (ϛ′) Λάθος. Έστω ότι R/I $P.I.D$. Τότε πρέπει να ισχύει ότι(κάθε ιδεώδες του R είναι κύριο και) R/I είναι ακεραία περιοχή, που απο θεωρία γνωρίζω ότι είναι ισοδύναμο με ότι το I είναι πρώτο ιδεώδες του R, που δεν υπάρχει στην υπόθεση.

   (ζ′) Λάθος. Έστω $S = \mathbb{Z}[\sqrt{10}]$ και R το σώμα πηλίκων του S. Προφανώς το R είναι $U.F.D$, αλλά, όπως έχουμε δει στις ασκήσεις, ο δακτύλιος $\mathbb{Z}[\sqrt{10}]$ δεν είναι $U.F.D(6 = 2 \times 3 = (4 - \sqrt{10})(4 + \sqrt{10})$ με $2, 3, 4 \pm \sqrt{10}$ ανάγωγα στοιχεία του $\mathbb{Z}[\sqrt{10}]$.

20/20

   (η′) Λάθος.
   Αν είχα ότι R/I είναι $U.F.D$ θα έπρεπε να είναι ακεραία περιοχή, ισοδύναμα το ιδεώδες I του R θα έπρεπε να είναι πρώτο, που δεν υπάρχει στην υπόθεση.

   (θ′) Λάθος. Ακριβώς παρόμοια με την ε′.

2. Θα κάνω δύο λύσεις, θα ήθελα να μετρήσει η 2η, απλά έχω απορία αν μπορώ να καταλήξω δίχως σφάλματα σε σωστή λύση με χρήση τρίτου θεωρήματος Ισομορφ.

1η λύση

Είναι πιο εύκολο αν θεωρήσεις την απεικόνιση $f: Z \to Z[\sqrt{-n}]/<\sqrt{-n}>$ που στέλνει το z στο $z+ <\sqrt{-n}>$. Δες τις λύσεις που μοίρασα.

Θέτω $R = \mathbb{Z}[\sqrt{-n}]/ < \sqrt{-n} >$.

Έχω ότι $\mathbb{Z}[\sqrt{-n}] \cong \mathbb{Z}[X]/ < X^2 + n >$ *:σχέση 1*

Απόδειξη σχέσης 1. Έστω η απεικόνιση $\phi_1 : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{-n}]$ με $\phi(f(X)) = f(\sqrt{-n})$ με $f(X) \in \mathbb{Z}[X]$. Τετριμμένο είναι ότι η ϕ_1 είναι επιμορφισμός δακτυλίων. Αρκεί να δείξω ότι $Ker\phi_1 =< X^2 + n >$. Έχω ότι $Ker\phi_1 = \{f(X) \in \mathbb{Z}[X] : \phi_1(f(X)) = 0\} = \{f(X) \in \mathbb{Z}[X] : f(\sqrt{-n}) = 0\} = \{$τα πολυώνυμα με συντελεστές ακεραίους και ρίζα το $\sqrt{-n}\} =< X^2 + n >$.

Άρα από πρώτο θεώρημα ισομορφισμών δακτυλίων έπεται η *σχέση 1.*

Αντίστοιχα έχω ότι το ιδεώδες $< \sqrt{-n} >$ του $\mathbb{Z}[X]$ είναι ισόμορφο με το πηλίκο

$< X^2+n, X > / < X^2+n >$, αφού $< X^2+n, X > / < X^2+n > \cong < (\sqrt{-n})^2+n, \sqrt{-n} >=< \sqrt{-n} >$.

Επομένως έχω:$\mathbb{Z}[\sqrt{-n}]/ < \sqrt{-n} > \cong (\mathbb{Z}[X]/ < X^2 + n >)/(< X^2 + n, X > / < X^2 + n >)$. Παρατηρώ ότι ικανοποιούνται οι προυποθέσεις του τρίτου θεωρήματος ισομορφισμών, άρα το παραπάνω είναι ισόμορφο με $\mathbb{Z}[X]/ < X^2 + n, X >$. Τώρα θεωρώ το ιδεώδες $< X >$ του $\mathbb{Z}[X]$ και του $< X^2 + n, X >$ και κάνοντας ξανά χρήση του τρίτου θεωρήματος ισομορφισμών έχω ότι:

$\mathbb{Z}[X]/ < X^2 + n, X > \cong (\mathbb{Z}[X]/ < X >)/(< X^2 + n, X > / < X >) \cong \mathbb{Z}/ < n > \cong \mathbb{Z}_n$. (Τετριμμένο είναι να δείξω ότι $< X^2 + n, X > / < X > \cong < n >$, για συντομία δεν έδειξα μέσω απεικόνισεων τις σχέσεις ισομορφιών).

2η Λύση

Οι δύο λύσεις που δίνεις είναι ουσιαστικά η ίδια.....

Θεωρώ ξανά $\phi_1 : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{-n}]$ τον (όπως απέδειξα πριν) επιμορφισμό ο οποίος ¨στέλνει' το $f(X)$ του δακτυλίου $\mathbb{Z}[X]$ στο $f(\sqrt{-n})$ του δακτυλίου $\mathbb{Z}[\sqrt{-n}]$. Έχω επίσης τον πυρήνα του ϕ_1, $Ker\phi =< X^2 + n >$. Επομένως από *correspondence theorem* έχω τα εξής:

$$\begin{array}{ccc} \phi_1 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}[\sqrt{-n}] \\ | & & | \\ < X^2 + n, X > & \longleftrightarrow & < \sqrt{-n} > \\ | & & | \\ < X^2 + n > & \longleftrightarrow & 0 \end{array}$$

Και, προφανώς, έχω ότι τα ιδεώδη $< X^2 + n, X >, < X, n >$ είναι ίσα (αρκεί να δείξω ότι $X^2+n, X \in < X, n >$ και ότι $X, n \in < X^2+n, X >$, για το πρώτο έχω ότι $X^2+n = X \cdot X+n \in < X, n >$ και τετριμμένα $X \in < X, n >$, για το δεύτερο $n = (X^2 + n) - X \cdot X \in < X^2 + n, X >$ και τετριμμένα $X \in < X^2 + n, X >$).

Άρα με χρήση του *Correspondence Theorem* έχω καταλήξει στο εξής:

$$\mathbb{Z}[\sqrt{-n}]/ < \sqrt{-n} > \cong \mathbb{Z}[X]/ < X, n >$$

Θεωρώ τώρα την απεικόνιση $\phi_2 : \mathbb{Z}[X] \longrightarrow \mathbb{Z}$ που στέλνει το $f(X) \in \mathbb{Z}[X]$ στο $f(0) \in \mathbb{Z}$. Όπως έχουμε δει και στο μάθημα η ϕ_2 είναι επιμορφισμός με πυρήνα $Ker\phi_2 =< X >$, επομένως χρησιμοποιώντας το *Correspondence Theorem* όπως πρίν έχω τα εξής:

10/10

$$\begin{array}{ccc} \phi_2 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z} \\ | & & | \\ < X, n > & \longleftrightarrow & < n > \\ | & & | \\ < X > & \longleftrightarrow & 0 \end{array}$$

Και άρα προκύπτει ότι $\mathbb{Z}[X]/ < X, n > \cong \mathbb{Z}/ < n > \cong \mathbb{Z}_n$

3. Έχω ότι $R = \mathbb{Z}[\sqrt{-n}], n \in \mathbb{N}$

   (α′) Προφανώς $2|n(n+1)$ Έστω ότι το 2 είναι πρώτο στοιχείο του δακτυλίου R. Τότε πρέπει να ισχύει το εξής:$(2|n) \vee (2|(n+1))$. Θα οδηγηθώ σε άτοπο. Αν $2|n$ τότε $2|-(\sqrt{-n})(\sqrt{-n})$ τότε $2|\sqrt{-n}$ επομένως υπάρχει $a+b\sqrt{-n} \in R$ τέτοιο ώστε $\sqrt{-n} = 2(a+b\sqrt{-n}) = 2a+2b\sqrt{-n}$ άρα πρέπει $b = 1/2$ άτοπο αφού $b \in \mathbb{Z}$. Αν $2|(n+1)$τότε $2|(1+\sqrt{-n})(1-\sqrt{-n})$ και αφού έχω υποθέσει ότι το $2 \in R$ είναι πρώτο, έπεται $[2|(1+\sqrt{-n})] \vee [2|(1-\sqrt{-n})]$. Θα δείξω ότι δεν γίνεται $2|(1+\sqrt{-n})$. Με τον ίδιο ακριβώς τρόπο καταλήγω σε άτοπο και στην άλλη περίπτωση. Αν $2|(1+\sqrt{-n})$, τότε υπάρχει $c+d\sqrt{-n} \in R$ τέτοιο ώστε $1+\sqrt{-t} = 2(c+d\sqrt{-n}) = 2c+2d\sqrt{-n}$, τότε $c = d = 1/2$, άτοπο αφού $c, d \in \mathbb{Z}$.

   ✓

   (β′) Έχω $-n \leq -3$, άρα $n \geq 3$. Έστω ότι το 2 δεν είναι ανάγωγο στο R, τότε υπάρχει στοιχείο του R, έστω $x = a+b\sqrt{-n}$ με $a, b \in \mathbb{Z}$, που δεν είναι μονάδα ούτε συνεταιρικό του 2 $(*)$, που να διαιρεί το 2, δηλαδή έχω $(a+b\sqrt{-n})|2$ άρα $2 = (a+b\sqrt{-n})(c+d\sqrt{-n})$ με $c, d \in \mathbb{Z}$. Παίρνοντας νόρμες στην σχέση έχω το εξής:$4 = (a^2+nb^2)(c^2+nd^2)$ άρα $a^2+nb^2 = 1$ ή 2 ή 4. Αν $(a^2+nb^2) = 1$ τότε απο γνωστή πρόταση έπεται ότι $a+b\sqrt{-n}$ είναι μονάδα, άρα απορρίπτεται από υπόθεση μου $(*)$. Αν $(a^2+nb^2) = 4$ τότε $a+b\sqrt{-n}, 2$ συνεταιρικά, απορρίπτεται$(*)$. Άρα έχω ότι $(a^2+nb^2) = 2$, τότε, αφού $n \geq 3$, αναγκαστικά $b = 0$ άρα $a^2 = 2$ άτοπο, αφού $a \in \mathbb{Z}$.

   ✓

   10/10

   Επομένως έχω ως άμεσο συμπέρασμα ότι ο δακτύλιος R δεν είναι $U.F.D$ αφού αλλιώς ανάγωγα και πρώτα στοιχεία του R θα ταυτίζονταν, πράγμα που όπως είδα δεν συμβαίνει, επομένως δεν έιναι ούτε $P.I.D$, άρα ούτε ευκλείδια περιοχή. Είναι όμως $Noetherian$ αφού ,όπως είδαμε στην παραπάνω άπόδειξη(της άσκησης 2), υπάρχει επιμορφισμός (ϕ_1 στην άσκηση 2) από τον $\mathbb{Z}[X]$ στον R και $\mathbb{Z}[X]$ είναι $Noetherian$ (είναι γνωστο ότι $\mathbb{Z}$ είναι $Noetherian$, και από θεώρημα βάσης του $Hilbert$, $\mathbb{Z}[X]$ είναι $Noetherian$) άρα απο γνωστή πρόταση έπεται ότι R $Noetherian$.

   ✓

4. Ξανά, $R = \mathbb{Z}[\sqrt{-n}], n \geq 3$, με n ελεύθερος τετραγώνων.

   - Για το $\sqrt{-n} \in R$. Έστω ότι δεν είναι ανάγωγο στο R. Τότε, όπως παραπάνω (για το $2 \in R$) υπάρχει στοιχείο $x = a+b\sqrt{-n} \in R, a, b \in \mathbb{Z}$ που δεν είναι ούτε μονάδα, ουτε συνεταιρικό

του $\sqrt{-n}$ τέτοιο ώστε $x|\sqrt{-n}$, άρα έχω $\sqrt{-n} = (a+b\sqrt{-n})(c+d\sqrt{-n})$ με $c,d \in \mathbb{Z}$. Αν πάρω νόρμες στην σχέση έχω το έξης: $n = (a^2+nb^2)N, N = c^2+nd^2 > 0$. Άρα έχω ότι $n = a^2N + nb^2N$,αρχικά αν $a \neq 0$, πρέπει $b = 0$, άρα $n = a^2N$ που είναι άτοπο, αφου n ειναι ελεύθερο τετραγώνων. Αν έχω $a = 0$ τότε $n = nd^2N$ που είναι προφανώς άτοπο. Άρα σε κάθε περίπτωση καταλήγω σε άτοπο αφού έχω υποθέσει ότι $\sqrt{-n}$ δεν είναι ανάγωγο. Άρα $\sqrt{-n}$ ανάγωγο.

- Για το $1+\sqrt{-n} \in R$. Έστω ότι δεν είναι ανάγωγο στο R. Τότε, όπως παραπάνω υπάρχει στοιχείο $x = a+b\sqrt{-n} \in R, a, b \in \mathbb{Z}$ που δεν είναι ούτε μονάδα, ουτε συνεταιρικό του $1+\sqrt{-n}$ τέτοιο ώστε $x|1+\sqrt{-n}$, άρα έχω $1+\sqrt{-n} = (a+b\sqrt{-n})(c+d\sqrt{-n})$ με $c,d \in \mathbb{Z}$. Παίρνοντας νόρμες στην σχέση αυτή, έχω: $1+n = (a^2+nb^2)N$, με $N = (c^2+nd^2) > 0$, άρα έχω $1+n = (a^2+nb^2)N \Rightarrow 1-a^2N+n-nb^2N = 0 \Rightarrow (1-a^2N)+n(1-b^2N) = 0$.

  δεν χρειάζεται να πάρεις περιπτώσεις για το b

  Όπως πρίν, αν $a \neq 0$, έχω $(1-a^2N) \leq 0$ τότε για $b \neq 0$ έχω $n(1-b^2N) \leq 0$, επομένως για να ισχύει $(1-a^2N)+n(1-b^2N) = 0$, πρέπει $(1-a^2N) = n(1-b^2N) = 0$ άρα $a = b = N = 1$ απορρίπτεται αφου οδηγούμε σε συνεταιρικό του $1+\sqrt{-n}$ (αφού τότε έχω ότι $c+d\sqrt{-n}$ μονάδα του R). Για $b = 0$ έχω $a = N = 1$ άρα έχω ότι x μονάδα του R επομένως απορρίπτεται.

  Ή θα μπορούσες να έχεις a=-1 ή b=-1 πάλι με N=1.....

  Αν υποθέσω ότι $a = 0$ τότε έχω $1+n(1-b^2N) = 0 \Rightarrow 1 = n(b^2N-1)$, προφανώς τότε $b \neq 0$, άρα $(b^2N-1) \geq 0, n \geq 3$, άρα αδύνατο να ισχύει $1 = n(b^2N-1)$.

  Άρα κατέληξα στο ότι δεν υπάρχουν γνήσιοι μη τετριμμένοι διαιρέτες του $1+\sqrt{-n}$ στον δακτύλιο R, επομένως είναι ανάγωγο.

  Τώρα θα βρω ιδεώδες του R που δεν είναι κύριο, αναλόγως το n.

  - Έστω ότι n άρτιος, όπως είδα σε προηγούμενη άσκηση, σε αυτή την περίπτωση έχω $2 \nmid \sqrt{-n}$. Θα χρησιμοποιήσω αυτό το δεδομένο παρακάτω. Θεωρώ το ιδεώδες $I_1 =< 2, \sqrt{-n} >$. Έστω ότι είναι κύριο, τότε έχω $I_1 =< u >$ για κάποιο $u \in R$. Τότε: $2 \in < u > \Longrightarrow u|2$, το 2 είδα ότι είναι ανάγωγο στο R, άρα, είτε $u, 2$ είναι συνεταιρικά, είτε το u είναι μονάδα του R. Στην περίπτωση όπου $u, 2$ είναι συνεταιρικά, καταλήγω σε άτοπο, αφού αλλιώς θα είχα ότι $< 2, \sqrt{-n} >=< 2 >$, που δεν ισχύει ($\sqrt{-n} \notin < 2 >$). Στην περίπτωση όπου το u είναι μονάδα του R έχω ότι $I_1 = R$, ισοδύναμα $1 \in I_1 =< 2, \sqrt{-n} >$, άρα υπάρχουν $x, y \in R$ τέτοια ώστε $1 = 2x+\sqrt{-n}y \Longrightarrow \sqrt{-n} = \sqrt{-n}2x + \sqrt{-n}\sqrt{-n}y \Longrightarrow \sqrt{-n} = \sqrt{-n}2x - ny$, όμως απο υπόθεση έχω ότι n άρτιος, άρα $2|n \Longrightarrow 2|(-ny)$ και $2|\sqrt{-n}2x$, άρα $2|\sqrt{-n}2x - ny \Longrightarrow 2|\sqrt{-n}$, άτοπο. Άρα το ιδεώδες I_1 δεν είναι κύριο.

    Μπράβο Ιωσήφ, πολύ καλά!!

  - Έστω ότι n περιττός, από προηγούμενη άσκηση γνωρίζω ότι $2 \nmid 1+\sqrt{-n}$. Θεωρώ $I_2 =< 2, 1+\sqrt{-n} >$. Θα δείξω ότι δεν είναι κύριο. Αν ήταν, τότε $I_2 =< v >$ για κάποιο $v \in R$. Άρα, $2 \in < v > \Longrightarrow v|2$, όμως έδειξα ότι το 2 είναι ανάγωγο στο R, άρα $v, 2$ συνεταιρικά ή v μοναδα, η πρώτη περίπτωση άμεσα με οδηγεί σε άτοπο (αφού τότε $1+\sqrt{-n} \notin I_2$), στην δεύτερη περίπτωση $I_2 = R$, άρα $1 \in I_2$, άρα $1 = 2z+(1+\sqrt{-n})w$ με $z, w \in R$, άρα $(1+\sqrt{-n}) = (1+\sqrt{-n})2z + (1+\sqrt{-n})(1+\sqrt{-n})w \Longrightarrow (1+\sqrt{-n}) = (1+\sqrt{-n})2z + (2\sqrt{-n}+(1-n))w$ και έχω ότι $2|n-1 \Longrightarrow 2|1-n$, ακόμα

15/15

$2|2\sqrt{-n} \Longrightarrow (2\sqrt{-n}+(1-n))w$, επίσης $2|(1+\sqrt{-n})2z$, άρα $2|(1+\sqrt{-n})$ Άτοπο. Άρα I_2 δεν είναι κύριο.

5. Στην άσκηση θα χρησιμοποιήσω την εξής γνωστή (από το μάθημα) πρόταση. Αν R ακεραία περιοχή και F το σώμα πηλίκων της R, τότε υπάρχει μονομορφισμός $i : R \hookrightarrow F$, με $i(r) = r/1$ και μάλιστα το σώμα F είναι το μικρότερο σώμα στο οποίο εμφυτεύται η R. Έχω ακόμα ότι $h : R \hookrightarrow L$, άρα έχω ως άμεσο συμπέρασμα ότι το F είναι υπόσωμα του L, επομένως, αφού κάθε στοιχείο του R έχει αντίστροφο στο F, έχει αντίστροφο και στο L. Άκόμα γνωρίζω ότι $x \in F \Rightarrow x = ab^{-1}, a, b \in R$. Θεωρώ την επέκταση του μονομοφισμού $h : R \hookrightarrow L$ έστω $H : F \hookrightarrow L$ με $H(rd^{-1}) = h(r)h(d)^{-1}$, με $H|_R = h$. Θα δείξω ότι η απεικόνιση H είναι μονομορφισμός. Αρχικά θα δείξω ότι είναι καλά ορισμένη απεικόνιση. Έστω $rd^{-1} = ab^{-1}$ τότε έχω: $rb = ad \Rightarrow h(r)h(b) = h(a)h(d)$, άρα $H(rd^{-1}) = h(r)h(d)^{-1} = h(a)h(b)^{-1} = H(ab^{-1})$. Είναι προφανές ότι είναι ομομορφισμός δακτυλίων. Έστω τώρα ότι $x \in KerH$, τότε $x = rd^{-1}, r, d \in R$, τότε έχω ότι: $H(rd^{-1}) = 0 \Rightarrow h(r)h(d)^{-1} = 0 \Rightarrow h(r) = 0 \Rightarrow r \in Kerh$, όμως $Kerh = 0$ αφού h μονομορφισμός, άρα $H(rd^{-1}) = 0 \Rightarrow r \in Kerh \Rightarrow r = 0 \in R$, άρα τότε $rd^{-1} = 0$, επομένως $kerH = 0 \in F$. Επομένως, η απεικόνιση H είναι μονομορφισμός. Επιπλέον, έχω ότι για κάθε $r \in R$ ισχύει $(H \circ i)(r) = H(i(r)) = H(r/1) = h(r)h(1) = h(r)$, άρα $H \circ i = h$.

10/10

√

√

Αν έχω ότι η h δεν είναι μονομορφισμός, προφανώς δεν μπορεί να υπάρξει επέκταση H του h ,ώστε $H \circ i = h$ με H μονομορφισμό. Έστω ο κανονικός επιμορφισμός $h : \mathbb{Z} \longrightarrow \mathbb{Z}_2$, έχω ότι $\mathbb{Z} \ni a \longmapsto amod2 \in \mathbb{Z}_2$. Άρα, $h(2) = 0 \in \mathbb{Z}_2$, επομένως δεν υπάρχει τρόπος να ορίσω μονομορφική επέκταση του h έστω $H : Z \longrightarrow \mathbb{Z}_2$ τέτοιο ώστε $H(1/2) = h(1)h(2)^{-1}$ αφού $h(2) = 0$.

6. Θεωρώ την απεικόνιση $\phi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_2[X]$ με $\phi(a_nX^n + .. + a_0) = a_n(mod2)X^n + ... + a_0(mod2)X^n$ Είναι γνωστό ότι η ϕ είναι επιμορφισμός με πυρήνα $Ker\phi =< 2 >$. Άρα έχω από *correspondce theorem* ότι:

$$\begin{array}{ccc} \phi_1 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_2[X] \\ | & & | \\ < 2, X^3+1 > & \longleftrightarrow & < X^3+1 > \\ | & & | \\ < 2 > & \longleftarrow & 0 \end{array}$$

√

Επομένως $\mathbb{Z}[X]/ < 2, X^3 > \cong \mathbb{Z}_2[X]/ < X^3+1 >$. Τώρα παρατηρώ ότι $< X^3+1 >=< (X+1)(X^2-X+1) >=< (X+1) >< (X^2-X+1) >$ Όμως $\mathbb{Z}_2$ σώμα, άρα $\mathbb{Z}_2[X] P.I.D$ άρα $< (X+1) >, < (X^2-X+1) >$ είναι *maximal* ιδεώδη του $\mathbb{Z}_2[X]$ αφού τα πολυώνυμα που τα παράγουν είναι ανάγωγα στο $\mathbb{Z}_2[X]$ άρα ται ιδεώδη αυτά είναι ¨πρώτα μεταξύ τους¨(όλα γνωστά απο θεωρία). Επομένως ικανοποιούνται οι προυποθέσεις του κινέζικου θεωρήματος, άρα έχω ότι $\mathbb{Z}_2[X]/ < X^3+1 > \cong \mathbb{Z}_2[X]/ < X+1 > \times \mathbb{Z}_2[X]/ < X^2-X+1 >$. Οι δακτύλιοι $\mathbb{Z}_2[X]/ < X+1 >, \mathbb{Z}_2[X]/ < X^2-X+1 >$ είναι σώματα, επομένως έχουν μόνο τετριμμένα ιδεώδη, άρα ο δακτύλιος $\mathbb{Z}_2[X]/ < X^3+1 >$ έχει μη τετριμμένα ιδεώδη μόνο τα

$\mathbb{Z}_2[X]/ < X+1 >, \mathbb{Z}_2[X]/ < X^2-X+1 >$, άρα από *Correspondence Theorem* μέσω της ϕ προκύπτει ότι τα μόνα μη τετριμμένα ιδεώδη του πηλίκου $\mathbb{Z}[X]/ < 2, X^3+1 >$ είναι τα $\mathbb{Z}[X]/ < 2, X+1 >, \mathbb{Z}[X]/ < 2, X^2-X+1 >$. Αυτό φαίνεται ποι καθαρά αν δω τα εξής διαγράμματα:

$$\begin{array}{ccc} \phi_1 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_2[X] \\ | & & | \\ < 2, X+1 > & \longleftrightarrow & < X+1 > \\ | & & | \\ < 2, X^3+1 > & \longleftrightarrow & < X^3+1 > \end{array}$$

$$\begin{array}{ccc} \phi_1 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_2[X] \\ | & & | \\ < 2, X^2-X+1 > & \longleftrightarrow & < X^2-X+1 > \\ | & & | \\ < 2, X^3+1 > & \longleftrightarrow & < X^3+1 > \end{array}$$

7. Έχω $< 7, X^2+X+1 > \lhd \mathbb{Z}[X]$. Θα δείξω ότι δεν είναι *maximal*. Ισοδύναμα, αρκεί να δείξω ότι ο δακτύλιος πηλίκο $\mathbb{Z}[X]/ < 7, X^2+X+1 >$ δεν είναι σώμα. Θεωρώ την απεικόνιση $\psi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}_7[X]$ με $\psi(a_nX^n + .. + a_0) = a_n(mod7)X^n + ... + a_0(mod7)X^n$ Είναι γνωστό ότι η ψ είναι επιμορφισμός με πυρήνα $Ker\psi =< 7 >$. Άρα έχω την εξής κατάσταση :

$$\begin{array}{ccc} \phi_1 : \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_7[X] \\ | & & | \\ < 7, X^2+X+1 > & \longleftrightarrow & < X^2+X+1 > \\ | & & | \\ < 7 > & \longleftrightarrow & 0 \end{array}$$

Από *Correspondence Theorem* έπεται ότι $\mathbb{Z}[X]/ < 7, X^2+X+1 > \cong \mathbb{Z}_7[X]/ < X^2+X+1 >$, άρα το πρόβλημά μου ανάγεται στο να δείξω ότι ο δακτύλιος πηλίκο $\mathbb{Z}_7[X]/ < X^2+X+1 >$ δεν είναι σώμα, δηλαδή ότι το ιδεώδες $< X^2+X+1 > \lhd \mathbb{Z}_7[X]$ δεν είναι *maximal*. Όμως είναι γνωστό ότι το $\mathbb{Z}_7$ είναι σώμα, επομένως ο $\mathbb{Z}_7[X]$ είναι *P.I.D*, άρα αρκεί να δείξω ότι το πολυώνυμο X^2+X+1 δεν είναι ανάγωγο στο $\mathbb{Z}_7[X]$ (γνωστές από θεωρία προτάσεις). Παρατηρώ ότι $X^2+X+1 = (X^2+8X+15) = (X+5)(X+3) \in \mathbb{Z}_7[X]$ με κανένα από τα $(X+5), (X+3)$ να μην είναι μονάδα η συνεταιρικό του X^2+X+1 στον δακτύλιο $\mathbb{Z}_7[X]$. Συνεπώς δεν είναι ανάγωγο και άρα ο δακτύλιος πηλίκο $\mathbb{Z}_7[X]/ < X^2+X+1 >$ δεν είναι σώμα, άρα απο ισοδυναμίες, το ιδεώδες $< 7, X^2+X+1 > \lhd \mathbb{Z}[X]$ δεν είναι *maximal*.

8. Θέτω $R = \mathbb{Z}_p[X]$. Γνωρίζω ότι $\mathbb{Z}_p$ σώμα για p πρώτο. Άρα R είναι *P.I.D* για κάθε πρώτο p. Άρα, όπως παραπάνω, για να δείξω ότι το ιδεώδες $< X^4+1 >$ δεν είναι *maximal* στον R, αρκεί να δείξω ότι το X^4+1 δεν είναι ανάγωγο στο R.

- $p=2$
  Προφανώς τότε $X^4+1=(X^2+1)(X^2+1)$, αφού $(X^2+1)(X^2+1)=X^4+2X^2+1\equiv X^4+1\in R$, άρα δεν είναι ανάγωγο του R. (Φυσικά εκεί ισχυει $X^4+1=(X+1)^4$ $(freshman's-dream)$, αφού $2|4$ άρα προκύπτει το συμπέρασμα άμεσα)
- $p=5$
  Τότε $X^4+1\equiv(X^2+2)(X^2+3)=X^4+5X^2+6\equiv X^4+1\in R$,άρα δεν είναι ανάγωγο του R.
- $p=7$
  Εδώ σου ξέφυγε το 7 Τότε $X^4+1\equiv(X^2+2)(X^2+3)=X^4+5X^2+6\equiv X^4+1\in R$,άρα δεν είναι ανάγωγο του R
- $p=11$
  Έπειτα από παρατήρηση έχω ότι : $X^4+1\equiv(X^2+6X+5)(X^2+5X+9)\in R$, άρα δεν είναι ανάγωγο του R.

  Σχόλιο: Θα συμβολίζω $\mathbb{F}_n$ το σώμα με n το πλήθος στοιχεία με $\mathbb{F}_p\cong\mathbb{Z}_p$ αν p είναι πρώτος. Επίσης θα χρειαστώ γνώσεις θεωρίας σωμάτων, όπως για παράδειγμα ότι η πολλαπλασιαστική ομάδα πεπερασμένου σώματος είναι κυκλική που δεν θα αποδείξω. Στην περίπτωση $p=2$ έχω ότι όπως παραπάνω $X^4+1=(X+1)^4$, αφού $2|4$. Άρα θα δω τις περιπτώσεις όπου $p\geq 3$ πρώτος. Τότε έχω ότι $8|p^2-1$. Θεωρώ το σώμα $E=\mathbb{F}_{p^2}$ με p^2 στοιχεία, γνωρίζω ακόμα ότι η επέκταση σωμάτων $E/\mathbb{F}_p$ είναι βαθμού 2 (εύκολο). Τότε η πολλαπλασιαστική του ομάδα E^* είναι κυκλική τάξεως p^2-1. Άρα $c\in E^*\Rightarrow o(c)|p^2-1\Rightarrow c^{p^2-1}=1$ απο θεώρημα $Lagrange$, άρα κάθε στοιχείο της E^* είναι ρίζα του $X^{p^2-1}-1\in\mathbb{F}_p$.

  10/10 Επειδή $8|p^2-1$ έπεται ότι η E^* έχει κυκλική υποομάδα έστω H τάξεως 8. Άρα $e\in H\Rightarrow e^8=1$ άρα το πολυώνυμο X^8-1 εχει όλες τις ρίζες του στην ομάδα $H\subseteq E^*\subseteq E$, άρα όλες οι ρίζες του X^8-1 βρίσκονται στο σώμα E. Όμως $X^8-1=(X^4-1)(X^4+1)\in\mathbb{F}_p$, άρα το πολυώνυμο X^4+1 έχει όλες του τις ρίζες στο σώμα E.

  Αν θεωρήσω ότι το πολυώνυμο X^4+1 είναι ανάγωγο στο $\mathbb{F}_p[X](=\mathbb{Z}_p[X])$, τότε απο γνωστή πρόταση θεωρίας σωμάτων(θεωρημα του $Kronecker$), έπεται ότι υπάρχει επέκταση του σώματος $\mathbb{F}_p$, έστω L, βαθμού $4=deg(X^4+1)$ πάνω από το $\mathbb{F}_p$, στο οποίο το πολυώνυμο έχει ρίζα, αν θεωρήσω a την ρίζα, τότε γνωρίζω ότι $L=\mathbb{F}_p(a)=\{r_0+r_1a+r_2a^2+r_3a^3, r_i\in\mathbb{F}_p\}$.
  Άρα συνοπτικά έχω :
  $\cdot L/\mathbb{F}_p$ επέκταση βαθμού 4
  $\cdot E/\mathbb{F}_p$ επέκταση βαθμού 2
  $\cdot$Το πολυώνυμο πολυώνυμο $X^4+1\in\mathbb{F}_p$ έχει όλες τις ρίζες του στο σώμα E. Άρα $L\subseteq E$, δηλαδή το σώμα E αποτελεί επέκταση του L, άρα $\mathbb{F}_p\subseteq L\subseteq E$, άπο γνωστή πρόταση θ.σωμάτων για τους βαθμούς, έχω ότι $4|2$, άτοπο. Έτσι απέδειξα το ζητούμενο.

9. Έχω $f(X,Y)=X^2+Y^2+1=(X^2+1)+Y^2\in\mathbb{C}[X,Y]=(\mathbb{C}[X])[Y]$ Θέτω $R=\mathbb{C}[X]$. Επειδή $\mathbb{C}$ είναι σώμα (μάλιστα είναι αλγεβρικά κλειστό και απο προπτυχιακή άλγεβρα γνωρίζουμε ότι τα ανάγωγα του $\mathbb{C}[X]$ είναι τα πρωτοβάθμια), άρα R είναι $P.I.D$ (για την ακρίβεια είναι ευκλείδεια περιοχή) άρα είναι $U.F.D$ άρα υπάρχει μονοσήμαντη ανάλυση σε ανάγωγα στο R, επομένως αυτά ταυτίζονται με πρώτα. Επομένως έχω $g(Y)=f(X,Y)=(X^2+1)+Y^2=(X+i)(X-i)+Y^2\in R[Y]$. Απο τα προηγούμενα είναι σαφές ότι $X+i$ είναι ανάγωγο(άρα και πρώτο) στοιχείο του R, με $X+i|(X+i)(X-i)=X^2+1$, επιπλέον το $(X+i)^2=(X+i)(X+i)$ είναι σαφές ότι δεν διαιρεί το $(X+i)(X-i)=X^2+1$, με το στοιχείο $X^2+1\in R$ να αποτελεί τον σταθερό όρο του

10/10

$g(Y)$, και τέλος $X+1$ με το στοιχείο 1 να αποτελεί τον συντελεστή του μεγιστοβάθμιου όρου του $g(Y)$. Ακόμα έχω ότι $c(g)=1$, δηλαδή το g είναι *primitive*, άρα απο κριτήριο *Eisenstein* για τον πρώτο $X+i \in R$, έπεται ότι $g(Y)=f(X,Y)$ ανάγωγο στο $R[Y]=\mathbb{C}[X,Y]$.

10. (α′) Έστω ότι δεν υπάρχει τέτοιο $b \in R$, αφού το f είναι μηδενοδιαιρέτης, υπάρχει $g(X) \in R[X]$ ελαχίστου βαθμού, τέτοιο ώστε $g(X)f(X)=0$, με $g=b_mX^m+...+b_0$, και $b_m \neq 0$. Τότε έχω $g(X)f(X)=(b_mX^m+...+b_0)(a_nX^n+...+a_0)(\star)$, θεωρώ $0 \leq k \leq n$ το μέγιστο τέτοιο ώστε $a_ng \neq 0$, τέτοιο k υπάρχει αφού σε αντίθετη περίπτωση, θα είχα ότι $a_ig(X)=0, i=0,...,n$, άρα $b_mf(X)=0$ με $b_m \neq 0$, που είναι άτοπο απο υπόθεση. Άρα η σχέση $(\star)$ γίνεται $(b_mX^m+...+b_0)(a_kX^k+...+a_0)$, άρα $b_ma_k=0$, άρα ο βαθμός του $h(X)=a_kg(X)$ είναι μικρότερος του m, με $g(X)f(X)=0$, που έρχεται σε αντίθεση με την ελαχιστότητα του m.

(β′) $(\Rightarrow)$
Έστω $f(X)=a_nx^n+...+a_0 \in R[X]$ μονάδα, τότε υπάρχει $g(X)=b_m+...+b_0 \in R[X]$ τέτοιο ώστε $fg=1$, άρα $a_0b_0=1$, άρα $a_0 \in U(R)$. Για να δείξω ότι τα στοιχεία $a_i, i=1,2,...,n$ είναι μηδενοδύναμα θα δείξω ότι ανήκουν σε κάθε πρώτο ιδεώδες του R, που γνωρίζω από θεωρία οτι είναι ισοδύναμα. Έστω I πρώτο ιδεώδες του R, τότε $I[X]$ πρώτο ιδεώδες του $R[X]$, μάλιστα ισχύει $R[X]/I[X] \cong R/I[X]$. Θεωρώ τον κανονικό επιμορφισμό $\phi: R[X] \longrightarrow R/I[X]$ με $\phi(f(X))=\phi(a_nX^n+...+a_0)=(a_n+I)X^n+...+(a_0+I)$. Έχω δεδομένο ότι f είναι μονάδα του $R[X]$, άρα $\phi(f)$ θα είναι μονάδα του $R/I[X]$. Όμως $R/I[X]$ είναι ακεραία περιοχή, άρα αναγκαστικά $\phi(f) \in R/I$, άρα $a_i+I=0+I$ για $i=1,...,n$. Ισοδύναμα $a_i \in I$ για $i=1,...,n$. Επειδή αυτό ισχύει για κάθε πρώτο ίδεώδες του R τα στοιχεία αυτά ανήκουν στο *nilradical* του R και άπο θεωρία έπεται ότι τα $a_i, i=1,...,n$ είναι *nilpotent* στοιχεία του R.

20/20

$(\Leftarrow)$
Έστω ότι a_0 μονάδα και $a_i, i=1,...,n$ *nilpotent*. Έχω $f(X)=a_nX^n+...a_0=a_0+g(X)$, με $g(X)=a_nX^n+...+a_1X \in R[X]$. Επειδή $a_i, i=1,..,n$ είναι *nilpotent*, έπεται ότι $a_nX^n,..,a_1X$ είναι *nilpotent* (εξάλλου το *nilradical* ενός δακτυλίου γνωρίζουμε ότι είναι πάντα ιδεώδες του δακτυλίου), άρα $g(X)$ είναι *nilpotent*. Άπο άσκηση 7a φυλ.6, γνωρίζω ότι: $rnilpotent \Longrightarrow 1-r$ μονάδα. Θα δείξω ότι ισχύει κάτι ποιο γενικό, δηλαδή:
Αν r είναι *nilpotent*, u μοναδα, τότε $r+u$ είναι μονάδα$(*)$,
και έτσι θα έχω δείξω και ότι $f(X)$ μονάδα του $R[X]$. Έχω $u+r=u+uu^{-1}r=u(1+u^{-1}r)$, έχω ότι r είναι *nilpotent* άρα $-u^{-1}r$ είναι *nilpotent*, από την άσκηση 7)a) φυλ.6 έχω ότι $1-(-1)u^{-1}r$ είναι μονάδα, άρα $u(1+u^{-1}r)=u+r$ μονάδα. Άρα $f(X)$ μονάδα του $R[X]$.

σχολιάσαμε στην τάξη πως να το αποφύγεις αν θέλεις.

11. Δεδομένο είναι ότι κάθε πρώτο ιδεώδες του R είναι κύριο. Έστω ότι υπάρχει ιδεώδες του R που δεν είναι κύριο. Θεωρώ το σύνολο $S=\{I \lhd R, \text{το } I \text{ δεν είναι κύριο}\}$. Έστω μία αλυσίδα ιδεωδών του R, $I_1 \subseteq I_2 \subseteq ....$ με $I_i \in S$. Τότε η ένωση $T=\bigcup I_i$ αποτελεί ιδεώδες του R, καθώς και άνω φράγμα της αλυσίδας. Επιπλέον το T ανήκει στο S, αλλιώς θα είχα ότι T κύριο, άρα $T=<t>$ με $t \in \bigcup I_i$ άρα θα υπήρχε $i_0 \in \mathbb{N}$ τέτοιο ώστε $I_{i_0}=<t>$, άτοπο, αφού $I_{i_0} \in S$. Άρα $T \in S$, άρα από λήμμα του *Zorn*, υπάρχει *maximal* στοιχείο του S, έστω P.
Ισχυρίζομαι ότι το P είναι πρώτο ιδεώδες του R.

Απόδειξη. Έστω $ab \in P$ με $(a \notin P) \wedge (b \notin P)$. Τότε $P \subsetneq P+<a>$ και $P \subsetneq P+<b>$, επομένως $P+<a>, P+<b> \notin S$, άρα είναι κύρια με $P+<a>=<p+ra>=<c>$,

$P+ < b >=< p' + r'b >=< d >$, με $p, p' \in P, r, r' \in R$ και $c = p + ra, d = p' + r'b$. Θεωρώ το σύνολο $J = \{x \in R : xa \in P\}$. Το J είναι ιδεώδες του R(αποδεδειγμένο στο μάθημα), και παρατηρώ ότι $da = (p' + r'b)a = p'a + r'ba \in P$, αφού $p', ab \in P$, άρα $d = p' + r'b \in J$, άρα $P \subsetneqq P+ < b > \subseteq J$, άρα $b \in J$ με $J \notin S$, άρα κύριο. Δηλαδή $J =< j >$. Επειδή $P \subsetneqq P+ < a >$, έχω $x \in P \Rightarrow x \in P+ < a >=< c > \Rightarrow x = sc, s \in R$. Επομένως έχω ότι $x = sc \in P$,όμως $a \in < c >$ άρα $a = tc, t \in R$, άρα $sa = stc = t(sc) \in P$, άρα $s \in J$, άρα $s = tj, t \in R$. Άρα, $x = t(jc) \Rightarrow x \in < jc >$, άρα $P \subseteq < jc >$. Τώρα έχω ότι $j \in J$, άρα $ja \in P$. Όμως $jc = j(p + ra) = jp + jra$, με $p, ja \in P$, άρα, $jp, jra \in P$, άρα $jc \in P$, άρα $< jc > \subseteq P$. Άρα για $v = jc \in P$, έχω $P =< v >=< jc >$, άρα P κύριο, άτοπο. Άρα P πρώτο ιδεώδες του R άρα δεν ανήκει στο S.

Κατέληξα στο ότι το *maximal* στοιχείο του S, δηλαδή το P, δεν ανήκει στο S, που είναι αντίφαση. Επομένως το σύνολο S είναι αναγκαστικά το κενό. Άρα η ακεραία περιοχή R είναι $P.I.D.$