Φυλλάδιο 9

Γεωργία Κουρκουνάκη, αμ:330

21 Απριλίου 2017

Άσκηση 1:

α) **Λάθος**: Για παράδειγμα αν $R = K(X_1, X_2, ...)$ και $S = K[X_1, X_2, ...]$, όπου K σώμα και

$$K(X_1, X_2, ...) = \left\{ \frac{f(X_1, X_2, ...)}{g(X_1, X_2, ...)}, \text{ όπου } f(X_1, X_2, ...), g(X_1, X_2, ...) \in K[X_1, X_2, ...], g \neq 0 \right\}$$

τότε S είναι υποδακτύλιος του R. Όμως το R είναι σώμα και άρα Noetherian αλλά το S δεν είναι Noetherian.

β) **Σωστό**: Αν πάρουμε τον φυσικό επιμορφισμό:

$$\pi : R \twoheadrightarrow R/I$$

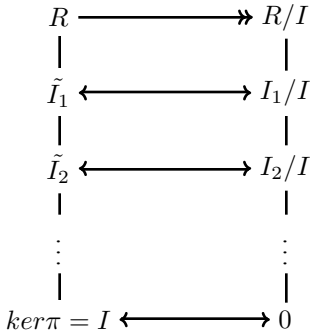
και R Noetherian τότε από γνωστή Πρόταση έχουμε ότι και R/I Noetherian.

γ) **Λάθος**: Για παράδειγμα, αν $R = \mathbb{Q}$ και $S = \mathbb{Z}$, τότε ο R είναι Artinian (αφού είναι σώμα) ενώ ο S δεν είναι Artinian (όπως δείξαμε στο μάθημα).

δ) **Σωστό**: Έστω R Artinian. Αρκεί να δείξουμε ότι η τυχούσα φθίνουσα ακολουθία ιδεωδών του R/I έχει minimal στοιχείο. Θεωρούμε τον φυσικό επιμορφισμό $\pi : R \twoheadrightarrow R/I$ και την φθίνουσα ακολουθία ιδεωδών του R/I:

$$I_1/I \supseteq I_2/I \supseteq ...$$

Τότε από Correspodence theorem για δακτυλίους έχουμε το εξής διάγραμμα:



Άρα έχουμε μία 1-1 αντιστοιχία μεταξύ των ιδεωδών του R που περιέχουν το I και των ιδεωδών του R/I. Οπότε οποιαδήποτε φθίνουσα ακολουθία ιδεωδών του R/I θα έχει minimal στοιχείο και τότε R/I Artinian.

ε) **Λάθος**: Για παράδειγμα, αν $R = \mathbb{Q}[X]$ και $S = \mathbb{Z}[X]$, έχουμε ότι το $\mathbb{Z}[X]$ δεν είναι PID (αφού το $\langle 2, X \rangle$ δεν είναι κύριο) αλλά το $\mathbb{Q}[X]$ είναι PID (αφού $\mathbb{Q}$ σώμα).

ζ) **Σωστό**: Έστω R PID και $I \trianglelefteq R$. Αρκεί να δείξουμε ότι αν $J/I \trianglelefteq R/I$, τότε το J/I είναι κύριο. Παίρνουμε το φυσικό επιμορφισμό $\pi : R \twoheadrightarrow R/I$ με $\pi(r) = r + I$ και από correspodence theorem έχουμε ότι το ιδεώδες J/I αντιστοιχεί σε κάποιο $\tilde{J} \trianglelefteq R$ που περιέχει το I. Αφού R PID έχουμε ότι $\tilde{J} = \langle j \rangle$ για κάποιο $j \in R$. Θα δείξουμε ότι $J/I = \langle j + I \rangle$. Έστω $a + I \in J/I$. Τότε $a + I \in \pi(\tilde{J}) = \tilde{J} + I$, άρα $\exists b \in \tilde{J}$ τέτοιο ώστε $b - a \in I$ και εφ' όσον $I \subseteq \tilde{J}$, έχουμε $b - a \in \tilde{J} \Rightarrow a \in \tilde{J}$. Συνεπώς $a = kj$, για κάποιο $k \in R$, οπότε καταλήγουμε ότι $a + I = kj + I \in \langle j + I \rangle$. Άρα $\langle j + I \rangle \subseteq J/I$. Όμως $\pi(j) \in J/I \Leftrightarrow j + I \in J/I$, άρα $J/I = \langle j + I \rangle$, δηλαδή J/I κύριο ιδεώδες.

η)**Λάθος**: Για παράδειγμα, αν $R = \mathbb{R}$ και $S = \mathbb{Z}[\sqrt{10}]$, τότε το $\mathbb{R}$ είναι UFD (αφού είναι σώμα), ενώ το S, από φυλλάδιο 8, δεν είναι UFD (αφού τα πρώτα ιδεώδη δεν ταυτίζονται με τα ανάγωγα).

θ) **Λάθος**: Έστω R UFD και $I \trianglelefteq R$. Αν R/I UFD τότε θα είναι ακέραια περιοχή και άρα I πρώτο ιδεώδες του R, το οποίο δεν συμβαίνει εν γένει.

18/20

ι) **Λάθος**: Για παράδειγμα αν $R = \mathbb{Q}[X]$ και $S = \mathbb{Z}[X]$, έχουμε ότι το $\mathbb{Z}[X]$ δεν είναι ευκλείδεια περιοχή (αφού δεν είναι PID) αλλά το $\mathbb{Q}[X]$ είναι ευκλείδεια περιοχή (αφού $\mathbb{Q}$ σώμα).

Άσκηση 2: Θεωρούμε τον επιμορφισμό $\phi : \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\sqrt{-n}]$ με $\phi(f(X)) = f(\sqrt{-n})$. Τότε $\ker\phi = \{f(X) \in \mathbb{Z}[X] : f(\sqrt{-n}) = 0\} = \{$όλα τα πολυώνυμα του $\mathbb{Z}[X]$ που έχουν ρίζα το $\sqrt{-n}\} = \langle X^2 + n\rangle$. Άρα από correspodence theorem έχουμε ότι $\langle\sqrt{-n}\rangle$ αντιστοιχεί στο $\langle X, X^2 + n\rangle = \langle X, n\rangle$ και μάλιστα

$$\mathbb{Z}[X]/\langle X, n\rangle \cong \mathbb{Z}[\sqrt{-n}]/\langle\sqrt{-n}\rangle$$

10/10

Αν πάρουμε τώρα τον επιμορφισμό $\psi : \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}$ με $\psi(f(X)) = f(0)$, τότε (όπως έχουμε ξαναδεί σε παλαιότερο φυλλάδιο) $\ker\psi = \langle X\rangle$. Τότε από correspodence theorem έχουμε ότι το ιδεώδες $\langle X, n\rangle$ αντιστοιχεί στο $\langle n\rangle$ και μάλιστα

$$\mathbb{Z}[X]/\langle X, n\rangle \cong \mathbb{Z}/\langle n\rangle$$

Συνεπώς καταλήγουμε ότι

$$\mathbb{Z}[\sqrt{-n}]/\langle\sqrt{-n}\rangle \cong \mathbb{Z}/\langle n\rangle = \mathbb{Z}_n$$

Άσκηση 3: Έστω $n \in \mathbb{N}$ που δεν είναι τέλειο τετράγωνο και $R = \mathbb{Z}[\sqrt{-n}]$.
α) Θα δείξουμε ότι το 2 δεν είναι πρώτο στοιχείο του $\mathbb{Z}[\sqrt{-n}]$. Διακρίνουμε τις εξής περιπτώσεις:

- Αν n άρτιος, τότε
$$2|(-n) \Rightarrow 2|(\sqrt{-n})^2 \Rightarrow 2|(\sqrt{-n})(\sqrt{-n})$$
Όμως $2 \nmid \sqrt{-n}$ (διότι αν $2|\sqrt{-n}$, τότε $\sqrt{-n} = 2(a + b\sqrt{-n})$, για κάποια $a, b \in \mathbb{Z}$ και άρα $\sqrt{-n} = 2a + 2b\sqrt{-n} \Rightarrow 2a = 0, 2b = 1$, άτοπο γιατί $b \in \mathbb{Z}$).

- Αν n περιττός, τότε
$$2|n + 1 \Rightarrow 2|(1 - \sqrt{-n})(1 + \sqrt{-n})$$
Αλλά $2 \nmid 1 \pm \sqrt{-n}$ (διότι αν για παράδειγμα $2|1 + \sqrt{-n}$, τότε $1 + \sqrt{-n} = 2(a + b\sqrt{-n})$, για κάποια $a, b \in \mathbb{Z}$, άρα $1 + \sqrt{-n} = 2a + 2b\sqrt{-n} \Rightarrow 2a = 1, 2b = 1$, άτοπο αφού $a, b \in \mathbb{Z}$).

Συνεπώς το 2 δεν είναι πρώτο στοιχείο του $\mathbb{Z}[\sqrt{-n}]$. Γιατί 2 διαιρεί το γινόμενο n(n+1) αλλά έδειξες ότι δεν διαιρεί κανένα από τους δύο.
β) Έστω $-n \leq -3$. Έστω ότι το 2 δεν είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-n}]$, τότε $\exists a, b, c, d \in \mathbb{Z}$ τέτοια ώστε

$$2 = (a + b\sqrt{-n})(c + d\sqrt{-n})$$

Χρησιμοποιώντας τη νόρμα N του δακτυλίου $\mathbb{Z}[\sqrt{-n}]$, όπου $N(a + b\sqrt{-n}) = a^2 + nb^2$, έχουμε ότι

10/10

$$N(2) = N((a + b\sqrt{-n})(c + d\sqrt{-n})) \Rightarrow (a^2 + nb^2)(c^2 + nd^2) = 4$$

Άρα είτε $N(a + b\sqrt{-n}) = N(c + d\sqrt{-n}) = 2$ ή $N(a + b\sqrt{-n}) = 1$ και $N(c + d\sqrt{-n}) = 4$. Έστω ότι είμαστε στην πρώτη περίπτωση, ότι δηλαδή $N(a + b\sqrt{-n}) = N(c + d\sqrt{-n}) = 2$. Έχουμε $N(a + b\sqrt{-n}) = 2 \Leftrightarrow a^2 + nb^2 = 2$. Όμως $n \in \mathbb{N}$ και $n \geq 3$, άρα η μόνη περίπτωση να ισχύει $a^2 + nb^2 = 2$ είναι όταν $a^2 = 2$. Τότε όμως $a = \sqrt{2}$, άτοπο αφού $a \in \mathbb{Z}$. Οπότε δεν υπάρχουν στοιχεία $a + b\sqrt{-n} \in \mathbb{Z}[\sqrt{-n}]$ με $N(a + b\sqrt{-n}) = 2$. Άρα $N(a + b\sqrt{-n}) = 1$ και $N(c + d\sqrt{-n}) = 4$. Έχουμε $N(a + b\sqrt{-n}) = 1 \Leftrightarrow a^2 + nb^2 = 1$. Όμως $n \geq 3$, άρα αναγκαστικά έχουμε ότι $a^2 = 1$ και $b = 0$, δηλαδή $a + b\sqrt{-n} = \pm 1$. Όμως τα $1, -1$ είναι αντιστρέψιμα στον $\mathbb{Z}[\sqrt{-n}]$, άρα το $2 =$αντιστρέψιμο$\times(c + d\sqrt{-n})$, οπότε το 2 είναι ανάγωγο στο $\mathbb{Z}[\sqrt{-n}]$. Επομένως παρατηρούμε ότι τα ανάγωγα στοιχεία του $\mathbb{Z}[\sqrt{-n}]$ δεν ταυτίζονται με τα πρώτα, άρα ο $\mathbb{Z}[\sqrt{-n}]$ δεν είναι UFD, και άρα ούτε PID, ευκλείδεια περιοχή. Όμως ο $\mathbb{Z}[\sqrt{-n}]$ είναι Noetherian διότι αν πάρουμε τον επιμορφισμό $\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\sqrt{-n}]$, αφού $\mathbb{Z}[X]$ Noetherian έχουμε και ότι $\mathbb{Z}[\sqrt{-n}]$ Noetherian.

Άσκηση 4: Έστω $R = \mathbb{Z}[\sqrt{-n}]$, με $n \geq 3$ ελεύθερο τετραγώνων.
Έστω ότι το $\sqrt{-n}$ δεν είναι ανάγωγο στον R, τότε $\exists a, b, c, d \in \mathbb{Z}$ τέτοια ώστε $\sqrt{-n} = (a + b\sqrt{-n})(c + d\sqrt{-n})$. Άρα, αν πάρουμε τη νόρμα N στον R, όπου $N(a + b\sqrt{-n}) = a^2 + nb^2$, έχουμε ότι $n = m(a^2 + nb^2)$, όπου $m = N(c + d\sqrt{-n}) = c^2 + nd^2$. Οπότε $ma^2 + mb^2n - n = 0 \Leftrightarrow ma^2 + (mb^2 - 1)n = 0$ $(*)$. Προφανώς $m \neq 0$, διότι τότε $c^2 + nd^2 = 0 \Rightarrow c = d = 0$ και τότε $\sqrt{-n} = 0$, άτοπο. Άρα $m \geq 1$. Διακρίνουμε τις εξής περιπτώσεις

Δεν βλέπω λάθος στην απόδειξή σου, αν και δεν χρησιμοποιείς το squarefree.

- Αν $a=0, b\neq 0$, τότε από σχέση $(*)$ παίρνουμε ότι $(mb^2-1)n=0$ και $n\neq 0$, άρα $mb^2=1$. Αφού $m,b\in\mathbb{Z}$ για να ισχύει η παραπάνω σχέση πρέπει $b=1$ και $m=1$. Τότε όμως $N(c+d\sqrt{-n})=1$ και όπως δείξαμε στην Άσκηση 3 έπεται ότι $c+d\sqrt{-n}\in U(R)$ και άρα $\sqrt{-n}$ είναι ανάγωγο.
- Αν $a\neq 0, b=0$, τότε $\sqrt{-n}=a(c+d\sqrt{-n})=ac+ad\sqrt{-n}$, οπότε $ac=0$ και $ad=1$ άρα $a=d=\pm 1$. Συνεπώς $\sqrt{-n}=\pm 1(c+d\sqrt{-n})$, όπου $\pm 1\in U(R)$, άρα $\sqrt{-n}$ ανάγωγο στον R.
- Αν $a,b\neq 0$, τότε $ma^2\geq 0, mb^2-1\geq 0, n\geq 0$, άρα για να ισχύει η $(*)$ στο $\mathbb{Z}$ πρέπει $ma^2=0$ και $(mb^2-1)n=0$. Έχουμε $(mb^2-1)n=0$ και $n\neq 0$, άρα $mb^2-1=0\Rightarrow mb^2=1\Rightarrow m=1$ και $b^2=1$. Τότε όμως $m=1\Leftrightarrow N(c+d\sqrt{-n})=1$ και όπως δείξαμε στην Άσκηση 3 το $c+d\sqrt{-n}\in U(R)$. Άρα $\sqrt{-n}$ ανάγωγο στον R.

Όμοια, έστω ότι το $1+\sqrt{-n}$ είναι ανάγωγο στο R. Τότε $\exists a,b,c,d\in\mathbb{Z}$ τέτοια ώστε $1+\sqrt{-n}=(a+b\sqrt{-n})(c+d\sqrt{-n})\Rightarrow N(1+\sqrt{-n})=N(a+b\sqrt{-n})N(c+d\sqrt{-n})\Rightarrow 1+n=m(a^2+nb^2)$, όπου $m=N(c+d\sqrt{-n})$ και όπως πριν $m\geq 1$. Άρα $(ma^2-1)+(mb^2-1)n=0$ $(**)$. Διακρίνουμε τις εξής περιπτώσεις

10/15

- Αν $a=0, b\neq 0$, τότε από $(**)$ έχουμε ότι $(mb^2-1)n=1\Rightarrow (mb^2-1)=1$ και $n=1$, άτοπο (αφού $n\geq 3$).
- Αν $a\neq 0, b=0$, τότε $1+\sqrt{-n}=a(c+d\sqrt{-n})=ac+ad\sqrt{-n}$. Άρα $ac=1\Rightarrow a=c=\pm 1$ οπότε $1+\sqrt{-n}=\pm 1(c+d\sqrt{-n})$, όπου $\pm 1\in U(R)$, άρα $1+\sqrt{-n}$ ανάγωγο στον R.
- Αν $a,b\neq 0$, τότε έχουμε $ma^2-1\geq 0, mb^2-1\geq 0, n\geq 3$, άρα για να ισχύει η $(**)$ πρέπει $ma^2-1=0$ και $mb^2-1=0$, το οποίο συνεπάγεται ότι $mb^2=1\Rightarrow m=b=1$ και άρα, όπως πριν, $c+d\sqrt{-n}\in U(R)$. Άρα $1+\sqrt{-n}$ ανάγωγο στον R.

Ένα ιδεώδες του R που δεν είναι κύριο είναι το $\langle 2,\sqrt{-n}\rangle$ διότι αν ήταν θα υπήρχαν $a,b\in\mathbb{Z}$ τέτοια ώστε $\langle 2,\sqrt{-n}\rangle=\langle a+b\sqrt{-n}\rangle$. Έτσι όμως $2\in\langle a+b\sqrt{-n}\rangle\Rightarrow 2=(a+b\sqrt{-n})(c+d\sqrt{-n})$ και 2 ανάγωγο. Άρα είτε $c+d\sqrt{-n}\in U(R)$ και $a=\pm 2, b=0$ ή $a+b\sqrt{-n}\in U(R)$ και $c=\pm 2, d=0$. Στην πρώτη όμως περίπτωση έχουμε $\sqrt{-n}\notin\langle a+b\sqrt{-n}\rangle$ και στην δεύτερη περίπτωση έχουμε $\langle 2,\sqrt{-n}\rangle=\mathbb{Z}$, άτοπο. Άρα $\langle 2,\sqrt{-n}\rangle$ δεν είναι κύριο ιδεώδες.

Αυτό συμβαίνει για n πρώτο (σχολιάσαμε στην τάξη). Σε αυτή την περίπτωση το ιδεώδες σου δεν είναι κύριο και πρέπει να δουλέψεις με το 1+\sqrt{-n} στην θέση του \sqrt{-n}

Άσκηση 5: Έστω R ακέραια περιοχή και F το σώμα πηλίκων της. Τότε $F=S^{-1}R$, όπου $S=R\setminus 0$. Έστω μονομορφισμός $h: R\hookrightarrow L$, όπου L σώμα. Όμως το σώμα πηλίκων F του R είναι το μικρότερο σώμα που μπορεί να εμφυτευθεί στον R, άρα το L περιέχει ως υπόσωμα το F (ή κάποια ισομορφική εικόνα του). Άρα για $s\in S$ το s είναι αντιστρέψιμο στον L. Οπότε μπορούμε να επεκτείνουμε τον h σε μονομορφισμό $\overline{h}: F\hookrightarrow L$ ως εξής $\overline{h}\left(\frac{r}{s}\right)=h(r)h(s)^{-1}$, όπου $r\in R, s\in S$.
Η απεικόνιση $\overline{h}$ είναι καλά ορισμένη: Έστω $rs^{-1}=\widehat{r}\widehat{s}^{-1}$, τότε $r\widehat{s}=\widehat{r}s\Rightarrow h(r)h(\widehat{s})=h(\widehat{r})h(s)\Rightarrow h(r)h(s)^{-1}=h(\widehat{r})h(\widehat{s})^{-1}\Rightarrow\overline{h}\left(\frac{r}{s}\right)=\overline{h}\left(\frac{\widehat{r}}{\widehat{s}}\right)$

10/10

Η $\overline{h}$ είναι ομομορφισμός αφού και ο h είναι ομομορφισμός.
Ο $\overline{h}$ είναι 1-1: Έστω $\frac{r}{s}\in\ker\overline{h}$, τότε $\overline{h}\left(\frac{r}{s}\right)=0\Rightarrow h(r)h(s)^{-1}=0$. Όμως $h(s)^{-1}\neq 0$, άρα $h(r)=0\Rightarrow r\in\ker h$ και h μονομορφισμός, οπότε $r=0$. Συνεπώς $\ker\overline{h}=\{0\}$.
Τέλος ο $\overline{h}$ είναι μοναδικός εκ κατασκευής εφ' όσων τα $h(r), h(s)^{-1}$ είναι μοναδικά (αφού h μονομορφισμός).

Αν τώρα ο h δεν ήταν μονομορφισμός τότε δεν θα ίσχυε το παραπάνω αποτέλεσμα. Για παράδειγμα αν $R=\mathbb{Z}, F=\mathbb{Q}$ και $L=\mathbb{R}$, τότε αν $h:\mathbb{Z}\to\mathbb{R}$ με $h(r)=r^2$ η επέκταση $\overline{h}:\mathbb{Q}\to\mathbb{R}$ με $\overline{h}(r)=r^2$ δεν είναι 1-1.

Άσκηση 6: Ψάχνουμε τα ιδεώδη του δακτυλίου

$$\mathbb{Z}[X]/\langle 2, X^3+1\rangle$$

Έστω $f(X)=X^3+1$, τότε από Correspodence Theorem (για τον επιμορφισμό $\mathbb{Z}[X]\twoheadrightarrow\mathbb{Z}[X]/\langle 2,f(X)\rangle$) έχουμε ότι τα ιδεώδη του $\mathbb{Z}[X]/\langle 2,f(X)\rangle$ είναι τα ιδεώδη I του $\mathbb{Z}[X]$ που περιέχουν το $\langle 2,f(X)\rangle$. Εφ' όσων $f(X)=X^3+1=(X+1)(X^2-X+1)$, τότε έχουμε ότι $I_1=\langle 2,f(X)\rangle\trianglelefteq\mathbb{Z}[X]/\langle 2,f(X)\rangle$, $I_2=\mathbb{Z}[X]\trianglelefteq\mathbb{Z}[X]/\langle 2,f(X)\rangle$, $I_3=\langle 2,X+1\rangle\trianglelefteq\mathbb{Z}[X]/\langle 2,f(X)\rangle$ και $I_4=\langle 2,X^2-X+1\rangle\trianglelefteq\mathbb{Z}[X]/\langle 2,f(X)\rangle$. Θα δείξουμε ότι αυτά είναι και τα μόνα ιδεώδη του $\mathbb{Z}[X]/\langle 2,f(X)\rangle$. Έστω κάποιο $g(X)\in\mathbb{Z}[X]\setminus\langle 2,f(X)\rangle$ τέτοιο ώστε $\langle 2,f(X),g(X)\rangle\trianglelefteq\mathbb{Z}[X]/\langle 2,f(X)\rangle$. Τότε διακρίνουμε τις εξής περιπτώσεις:

- Αν $\deg(g(X))=0$, τότε $g(X)=c\in\mathbb{Z}$. Αν c άρτιος τότε $\langle 2,c,f(X)\rangle=\langle 2,f(X)\rangle$. Αν c περιττός τότε $\langle 2,c,f(X)\rangle=\mathbb{Z}[X]$, αφού $\langle 2,c,f(X)\rangle\supseteq\langle 2,c\rangle\ni 1$.

- Αν $\deg(g(X)) > 0$ τότε κοιτάμε τον μκδ$(f(X), g(X))$. Οι διαιρέτες όμως του $f(X)$ είναι οι $f(X), 1, X+1, X^2-X+1$, άρα και ο μκδ$(f(X), g(X))$ είναι κάποιος από τους παραπάνω. Αν μκδ$(f(X), g(X)) = f(X)$, τότε $\langle 2, f(X), g(X)\rangle = \langle 2, f(X)\rangle = I_1$. Αν μκδ$(f(X), g(X) = 1$, τότε $\langle 2, f(X), g(X)\rangle = \mathbb{Z}[X] = I_2$. Αν μκδ$(f(X), g(X)) = X + 1$, τότε $\langle 2, f(X), g(X)\rangle = I_3$. Αν μκδ$(f(X), g(X)) = X^2 - X + 1$, τότε $\langle 2, f(X), g(X)\rangle = I_4$.

10/10

Άρα σε κάθε περίπτωση τα ιδεώδη του $\mathbb{Z}[X]/\langle 2, f(X)\rangle$ είναι τα I_1, I_2, I_3, I_4.

Άσκηση 7:Ξέρουμε ότι σε περιοχές κυρίων ιδεωδών R τα πρώτα ιδεώδη ταυτίζονται με τα maximal ιδεώδη του δακτυλίου (και τα πρώτα με τα ανάγωγα επίσης). Άρα στην περίπτωση ενός σώματος F, το $F[X]$ είναι PID, άρα από την παραπάνω παρατήρηση έχουμε ότι

$$\langle f(X)\rangle \text{ είναι maximal} \Leftrightarrow f(X) \text{ ανάγωγο στο } F[X]$$

√

Από το 3ο Θεώρημα Ισομορφισμών Δακτυλίων έχουμε ότι

10/10

$$\mathbb{Z}[X]/\langle 7, X^2 + X + 1\rangle \cong \mathbb{Z}_7[X]/\langle X^2 + X + 1\rangle$$

όπου $\mathbb{Z}_7$ είναι σώμα και άρα $\mathbb{Z}_7[X]$ είναι PID. Συνεπώς $\langle 7, X^2 + X + 1\rangle$ maximal $\Leftrightarrow \mathbb{Z}[X]/\langle 7, X^2 + X + 1\rangle$ σώμα $\Leftrightarrow \mathbb{Z}_7[X]/\langle X^2 + X + 1\rangle$ σώμα $\Leftrightarrow \langle X^2 + X + 1\rangle$ maximal $\Leftrightarrow X^2 + X + 1$ ανάγωγο στο $\mathbb{Z}_7[X]$. Όμως ένα πολυώνυμο βαθμού 2 πάνω από σώμα είναι ανάγωγο αν και μόνο αν δεν έχει ρίζα στο σώμα. Όμως $2^2 + 2 + 1 = 7 \equiv 0(mod 7)$, άρα το $X^2 + X + 1$ έχει ρίζα στο $\mathbb{Z}_7[X]$, συνεπώς δεν είναι ανάγωγο και άρα καταλήξαμε στο ζητούμενο.

Άσκηση 8: Από την άσκηση 7 έχουμε ότι αν F σώμα τότε

$$\langle f(X)\rangle \text{ είναι maximal} \Leftrightarrow f(X) \text{ ανάγωγο στο } F[X]$$

Άρα για να ελέγξουμε αν το $\langle X^4 + 1\rangle$ είναι maximal στο $\mathbb{Z}_2[X], \mathbb{Z}_5[X], \mathbb{Z}_7[X], \mathbb{Z}_{11}[X]$, αρκεί να ελέγξουμε αν είναι ανάγωγο στις παραπάνω PID's.

10/10

Στο $\mathbb{Z}_2[X]$ έχουμε $(X^2 + 1)(X^2 + 1) = X^4 + 2X^2 + 1 = X^4 + 1$. Άρα το $X^4 + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_2[X]$.
Στο $\mathbb{Z}_5[X]$ έχουμε $(X^2 + 3)(X^2 + 2) = X^4 + 5X^2 + 6 = X^4 + 1$. Άρα το $X^4 + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_5[X]$.
Στο $\mathbb{Z}_7[X]$ έχουμε $(X^2 + 4X + 1)(X^2 + 3x + 1) = X^4 + (3 + 4)X^3 + (1 + 5 + 1)X^2 + (4 + 3)X + 1 = X^4 + 1$.
Άρα το $X^4 + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_7[X]$.
Στο $\mathbb{Z}_{11}[X]$ έχουμε $(X^2 + 5X + 9)(X^2 + 6X + 5) = X^4 + (6 + 5)X^3 + (5 + 30 + 9)X^2 + 45 = X^4 + 1$. Άρα το $X^4 + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_{11}[X]$.

Άσκηση 9: Θέλουμε να δείξουμε ότι το πολυώνυμο $X^2 + Y^2 + 1$ είναι ανάγωγο στο $\mathbb{C}[X, Y]$. Αρκεί να δείξουμε ότι το $h(X) = X^2 + (Y^2 + 1)$ είναι ανάγωγο στο $(\mathbb{C}[Y])[X]$. Έχουμε ότι το πολυώνυμο $Y + i$ είναι ανάγωγο (και άρα πρώτο) στο $\mathbb{C}[Y]$, διότι αν όχι θα υπήρχαν $f(Y), g(Y) \in \mathbb{C}[Y], f, g \neq 0$ τέτοια ώστε $Y + i = f(Y)g(Y)$ και $\deg f, \deg g \leq \deg(Y + i) = 1$. Άρα από ισότητα βαθμών στα δύο μέλη έχουμε ότι αναγκαστικά το f ή το g είναι μηδενικού βαθμού, δηλαδή σταθερά και άρα αντιστρέψιμο στο $\mathbb{C}$. Άρα αν εφαρμόσουμε το κριτήριο αναγωγιμότητας του Eisenstein για το πρώτο $Y + i$ έχουμε

10/10

- $Y + i | Y^2 + 1$ στο $\mathbb{C}[Y]$
- $Y + i \nmid X^2$
- $(Y + i)^2 = Y^2 + 2iY - 1 \nmid Y^2 + 1$

Άρα $X^2 + Y^2 + 1$ ανάγωγο στο σώμα πηλίκων του $\mathbb{C}[X, Y]$ και αφού είναι primitive είναι ανάγωγο και στο $\mathbb{C}[X, Y]$.

Άσκηση 10: 1) Έστω $f(X) = a_n X^n + \cdots + a_0 \in R[X]$ είναι μηδενοδιαιρέτης του $R[X]$. Θα δείξουμε ότι $\exists b \in R$ τέτοιο ώστε $ba_n = ba_{n-1} = ... = ba_0 = 0$. Έστω ότι δεν υπάρχει, δηλαδή για κάθε $b \in R, bf(X) \neq 0$. Έστω πολυώνυμο $g(X) = b_m X^m + \cdots + b_0 \in R[X], g(X) \neq 0, b_m \neq 0$ ελαχίστου βαθμού τέτοιο ώστε $f(X)g(X) = 0$. Θεωρούμε k το μέγιστο δείκτη ώστε $a_k g(X) \neq 0$ (αν δεν υπάρχει τέτοιο k θα είχαμε ότι για κάθε δείκτη $i = 1, \ldots, n$ $a_i g(X) = 0$, άρα $b_0 a_i = 0$ για κάθε $i = 1, ..., n$ συνεπώς $b_0 f(X) = 0$, άτοπο εξ' υποθέσεως). Τότε για δείκτες $i > k$ έχουμε $a_i g(X) = 0$, άρα $0 = f(X)g(X) = (a_n X^n + \cdots + a_0)(b_m X^m + \cdots + b_0) = (a_k X^k + \cdots + a_0)(b_m X^m \cdots + b_0) \Rightarrow$

√

$a_k b_m = 0$. Όμως $f(X)g(X) = 0 \Leftrightarrow a_k f(X)g(X) = 0 \Leftrightarrow f(X)(a_k g(X)) = 0$ και $\deg(a_k g(X)) < \deg g(X)$ επειδή $a_k b_m = 0$, άτοπο λόγω ελαχιστότητας του βαθμού του g.

2) ($\Rightarrow$) Έστω $f(X) = a_n X^n + \cdots + a_0 \in U(R[X])$. Τότε $\exists g(X) = b_m X^m + \cdots + b_0 \neq 0$ τέτοιο ώστε

$$f(X)g(X) = 1 \Leftrightarrow \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k = 1$$

Άρα $a_0 b_0 = 1 \Rightarrow a_0, b_0 \in U(R)$ και $\sum_{i=0}^{k} a_i b_{k-i} = 0$, για $k = 1, \ldots, m+n$. Συνεπώς έχουμε

$$\begin{gathered} a_n b_m = 0 \\ a_{n-1} b_m + a_n b_{m-1} = 0 \Rightarrow a_n a_{n-1} b_m + a_n^2 b_{m-1} = 0 \Rightarrow a_n^2 b_{m-1} = 0 \\ a_{n-2} b_m + a_{n-1} b_{n-1} + a_n b_{m-2} = 0 \Rightarrow a_n^3 b_{m-2} = 0 \\ \vdots \\ a_{n-2} b_2 + a_{n-1} b_1 + a_n b_0 = 0 \Rightarrow a_n^{m+1} b_0 = 0 \end{gathered}$$

Όμως b_0 είναι αντιστρέψιμο άρα $a_n^{m+1} = 0 \Rightarrow a_n \in N(R)$. Άρα δείξαμε ότι το a_n είναι μηδενοδύναμο άρα και το $a_n X^n$ μηδενοδύναμο. Συνεπώς (αν μιμηθούμε την απόδειξη του φυλλαδίου 6, άσκηση 7) έχουμε ότι και το $f(X) - a_n X^n$ είναι αντιστρέψιμο, αφού $f(X)^{m+1} = f(X)^{m+1} - (a_n X^n)^{m+1} = (f(X) - a_n X^n)(f(X)^m + f(X)^{m-1} a_n X^n + \cdots + (a_n X^n)^m) \Leftrightarrow (f(X) - a_n X^n)(f(X)^m + f(X)^{m-1} a_n X^n + \cdots + (a_n X^n)^m)(f(X)^{-1})^{m+1} = 1$ και άρα $f(X) - a_n X^n \in U(R[X])$. Οπότε επαγωγικά έχουμε ότι a_i μηδενοδύναμα στοιχεία του R για $i = 1, \ldots, n$

($\Leftarrow$) Έστω πολυώνυμο $f(X) = a_n X^n + \cdots + a_0 \in R[X]$ με $a_0 \in U(R)$ και a_i nilpotent στοιχεία του R για $i = 1, \ldots, n$. Θα δείξουμε ότι το $f(X) \in U(R[X])$. Έχουμε $f(X) = a_0(1 + a_0^{-1} \sum_{k=1}^{n} a_k X^k)$. Αν $s = \sum_{k=1}^{n} a_k X^k$, αρκεί να δείξουμε ότι $1 + a_0^{-1} s \in U(R[X])$. Έχουμε ότι a_i nilpotent για $i = 1, \ldots, n$, άρα και τα $a_i X^i$ είναι nilpotent και επειδή $N(R[X])$ είναι ιδεώδες, έχουμε και ότι $-a_0^{-1} s$ επίσης nilpotent. Οπότε, από άσκηση 7-φυλλάδιο 6, έχουμε ότι το $1 - (-a_0^{-1} s) = 1 + a_0^{-1} s$ είναι αντιστρέψιμο, το οποίο ολοκληρώνει την απόδειξη.

20/20

Άσκηση 11: Έστω R ακέραια περιοχή όπου κάθε πρώτο ιδεώδες της είναι κύριο. Θα δείξουμε ότι R είναι PID. Έστω ότι δεν είναι. Θεωρούμε $S = \{I \trianglelefteq R : I \text{ δεν είναι κύριο}\}$. Τότε εξ' υποθέσεως, $S \neq \varnothing$. Έστω αλυσίδα A ιδεωδών του S: $I_1 \subseteq I_2 \subseteq \ldots$, τότε $\cup_{i \in \mathbb{N}} I_i$ είναι ιδεώδες του S (διότι αλλιώς αν $\cup_{i \in \mathbb{N}} I_i = \langle a \rangle$ τότε $a \in \cup_{i \in \mathbb{N}} I_i \Rightarrow \exists I_k \in A$ τέτοιο ώστε $a \in I_k$ και $I_k \subseteq \cup_{i \in \mathbb{N}} I_i = \langle a \rangle \Rightarrow I_k = \langle a \rangle$, άτοπο διότι $I_k \in S$) και $\cup_{i \in \mathbb{N}} I_i$ αποτελεί άνω φράγμα της αλυσίδας A. Συνεπώς ικανοποιούνται οι προϋποθέσεις του λήμματος του Zorn, άρα το S έχει maximal στοιχείο, έστω P. Τότε το P δεν γίνεται να είναι πρώτο ιδεώδες, άρα $\exists a, b \in R$ τέτοια ώστε $ab \in P$ και $a, b \notin P$. Κοιτάμε το ιδεώδες $\langle P, a \rangle \supsetneq P$. Από maximal ιδιότητα του P έπεται ότι $\langle P, a \rangle$ είναι κύριο, δηλαδή $\langle P, a \rangle = \langle r \rangle$, για κάποιο $r \in R$. Έστω $K = \{\widehat{r} \in R : \widehat{r} a \in P\}$. Τότε $K \trianglelefteq R$ (όπως είδαμε στο μάθημα) και $P \subsetneq K$, διότι προφανώς $P \subseteq K$ και $b \in K \setminus P$. Άρα το K είναι κύριο ιδεώδες, δηλαδή $K = \langle k \rangle$, για κάποιο $k \in R$. Ισχυρίζομαι ότι $P = \langle rk \rangle$:

15/15

($\subseteq$) Έστω $p \in P$. Τότε $p \in \langle P, a \rangle = \langle r \rangle \Rightarrow p = rx$, για κάποιο $x \in R$. Συνεπώς $rx \in P \Rightarrow x\langle r \rangle \subseteq P$ οπότε $xa \in P \Rightarrow x \in K = \langle k \rangle \Rightarrow x = \widehat{x}k$, για κάποιο $\widehat{x} \in R$. Άρα καταλήγουμε στο ότι $p = \widehat{x}rk \Rightarrow p \in \langle rk \rangle$.

($\supseteq$) Αντίστροφα τώρα έχουμε ότι $k \in K \Rightarrow ka \in P$ άρα το ιδεώδες $k\langle P, a \rangle$ περιέχεται μέσα στο P. Ισοδύναμα $k\langle r \rangle \subseteq P \Rightarrow kr \in P$.

Οπότε συμπεραίνουμε ότι $P = \langle rk \rangle$, δηλαδή P κύριο ιδεώδες, άτοπο. Άρα R είναι PID.