Αριστοτελειο Πανεπιστημιο Θεσσαλονικησ
Σχολη Θετικων Επιστημων
Τμημα Μαθηματικων

Αλγεβρικεσ Δομεσ II

Διδάσκουσα: Χ. Χαραλάμπους

Λυμένες ασκήσεις, Ενότητα 2

1. Έστω $I = \langle 100 \rangle$ ιδεώδες του $\mathbb{Z}$. Να βρεθούν όλα τα ιδεώδη J του $\mathbb{Z}$ έτσι ώστε $I \subset J$. Να βρεθούν όλα τα ιδεώδη K του $\mathbb{Z}$ έτσι ώστε $K \subset I$.

   Απάντηση Έστω $I \subset J$. Όλα τα ιδεώδη του $\mathbb{Z}$ είναι κύρια. Άρα $J = m\mathbb{Z}$ όπου $m \in \mathbb{N}$. Αφού $I \subset J$ έπεται ότι $100 \in m\mathbb{Z} \Rightarrow 100 = mk$, $k \in \mathbb{N}$. Επομένως m πρέπει να είναι διαιρέτης του 100.

   Αντίστροφα, αν $K = s\mathbb{Z} \subset I$ τότε $s = s \cdot 1 \in I$ και $s = 100l$, $l \in \mathbb{Z}$.

2. Έστω R αντιμεταθετικός δακτύλιος και I ιδεώδες του R. Να δείξετε ότι το σύνολο $\sqrt{I} = \{r \in R : \ r^{n_r} \in I, \text{ για κάποιο } n_r \in \mathbb{N}\}$ είναι ιδεώδες του R και ότι $I \subset \sqrt{I}$. Στον δακτύλιο $\mathbb{Z}$ να υπολογίσετε $\sqrt{\langle 3 \rangle}$, $\sqrt{\langle 27 \rangle}$, $\sqrt{\langle 36 \rangle}$.

   Απάντηση Έστω $r, s \in \sqrt{I}$, $f \in R$. Τότε $(r-s)^{n_r+n_s} \in I$ και έτσι $r - s \in \sqrt{I}$. Πράγματι στο δυωνυμικό ανάπτυγμα ο όρος $r^k s^{(n_r+n_s)-k} \in I$ όταν $k \geq n_r$. Επίσης όταν $k < n_r$ τότε $(n_r + n_s) - k > n_s$ και άρα και πάλι $r^k s^{(n_r+n_s)-k} \in I$. Επίσης, $(fr)^{n_r} = f^{n_r} r^{n_r} \in I$ και επομένως $fr \in \sqrt{I}$. Έστω τώρα $g \in I$. Τότε $g \in \sqrt{I}$ με $n_g = 1$.

   $\sqrt{\langle 3 \rangle} = \langle 3 \rangle$: αν $r^n \in \langle 3 \rangle$ τότε $r^n = 3m$ και αφού 3 πρώτος, έπεται ότι 3 διαιρεί το r, δηλαδή $r \in \langle 3 \rangle$.

   $\sqrt{\langle 27 \rangle} = \langle 3 \rangle$: αν $r^n \in \langle 27 \rangle = \langle 3^3 \rangle$ τότε $r^n = 3^3 m$ και αφού 3 πρώτος, έπεται ότι 3 διαιρεί το r, δηλαδή $r \in (3)$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι $(3m)^3 \in \langle 27 \rangle$.

   $\sqrt{\langle 36 \rangle} = \langle 6 \rangle$: αν $r^n \in \langle 36 \rangle = \langle 2^2 3^2 \rangle$ τότε $r^n = 2^2 3^2 m$ και αφού $2, 3$ πρώτοι, έπεται ότι $3, 2$ διαιρούν το r, δηλαδή $r \in \langle 6 \rangle$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι $(6m)^2 \in \langle 36 \rangle$.

3. Να βρεθούν όλα τα ιδεώδη του $\mathbb{Z}_{20}$.

   Απάντηση Γνωρίζουμε ότι $(\mathbb{Z}_{20}, +)$ είναι κυκλική ομάδα. Έστω I ιδεώδες του $\mathbb{Z}_{20}$. Το I είναι υποομάδα της $(\mathbb{Z}_{20}, +)$ άρα είναι κυκλική. Επομένως $I = \langle \overline{m} \rangle = m\mathbb{Z}_{20}$ για κάποιο ακέραιο $0 \leq m \leq 19$. Στο $\mathbb{Z}_{20}$ τα αντιστρέψιμα στοιχεία είναι τα $\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}$. Έπεται ότι αν m ανήκει στο $A = \{1, 3, 7, 9, 11, 13, 17, 19\}$ τότε $I = \langle \overline{m} \rangle$ είναι μη γνήσιο και ίσο με τον $\mathbb{Z}_{20}$.

   Έστω λοιπόν ότι J είναι γνήσιο ιδεώδες διάφορο του μηδενός. Επίσης $m = km'$ όπου $k \in A$ αν και μόνο αν $\langle \overline{m} \rangle = \langle \overline{m'} \rangle$ (ελέγξτε το!).

   Έτσι προκύπτουν τα παρακάτω διαφορετικά γνήσια μη μηδενικά ιδεώδη:

   - $\langle \overline{2} \rangle = \langle \overline{6}) = \langle \overline{14}) = \langle \overline{18} \rangle$
   - $\langle \overline{4} \rangle = \langle \overline{12}) = \langle \overline{8} \rangle = \langle \overline{16} \rangle$
   - $\langle \overline{5} \rangle = \langle \overline{15} \rangle$
   - $\langle \overline{10} \rangle$

4. Στο δακτύλιο $R = \mathbb{Z}[x]$ να δείξετε ότι $\langle x^2 + 3x + 1, x \rangle$ είναι μη γνήσιο και ισούται με R, ενώ $\langle x^2 + 2x + 1, x^2 + 3x + 2 \rangle = \langle x + 1 \rangle$.

   Απάντηση $1 = x^2 + 3x + 1 - x(x + 3) \in \langle x^2 + 3x + 1, x)$ και άρα $\langle x^2 + 3x + 1, x) = R$.

   Έστω $J = \langle x^2 + 2x + 1, x^2 + 3x + 2 \rangle$, $I = \langle x + 1 \rangle$. Τότε $x^2 + 2x + 1 = (x + 1)^2 \in I$, $x^2 + 3x + 2 = (x + 1)(x + 2) \in I$. Επομένως ένα τυχαίο στοιχείο του J, $f(x)(x^2+2x+1)+g(x)x^2+3x+2 \in I$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι $x + 1 = (x^2 + 3x + 2) - (x^2 + 2x + 1) \in J$.

5.

   (α΄) Να υπολογίσετε όλους τους ομομορφισμούς δακτυλίων από τον $\mathbb{Z}$ στον $\mathbb{Z}$. Για κάθε έναν από αυτούς να βρείτε και τον πυρήνα.

   (β΄) Έστω $R = \mathbb{Z} \times \mathbb{Z}$, ο δακτύλιος με πρόσθεση και πολλαπλασιασμό ανά συντεταγμένη. Να βρείτε όλους ομομορφισμούς δακτυλίων από τον R στον $\mathbb{Z}$. Για κάθε έναν από αυτούς να βρείτε και τον πυρήνα.

   Απάντηση

(α') Έστω $\phi : \mathbb{Z} \to \mathbb{Z}$, ομομορφισμός δακτυλίων, και έστω ότι $\phi(1) = m$. Τότε $\phi(1) = \phi(1 \cdot 1) = m^2$. Επομένως $m^2 = m$ και άρα $m = 1, 0$. Στη πρώτη περίπτωση έπεται ότι $\phi(a) = a$ και $\ker \phi = (0)$ ενώ στη δεύτερη περίπτωση $\phi(a) = 0$ και $\ker \phi = \mathbb{Z}$.

(β') Έστω $\phi(1, 0) = m$. Όπως προηγουμένως έπεται ότι $m = 1, 0$. Επίσης το ίδιο και για $\phi(0, 1)$. Έστω ότι $\phi(1, 0) = 1$, $\phi(0, 1) = 1$. Τότε $\phi(1, 1) = \phi(1, 0) + \phi(0, 1) = 2$ ενώ $\phi(1, 1) = \phi((1, 1) \cdot (1, 1)) = 2^2$, άτοπο. Μένουμε λοιπόν με τις παρακάτω περιπτώσεις: $\phi_1(a, b) = 0$ ($\ker \phi_1 = R$, $\phi_2(a, b) = a$, $\ker \phi_2 = \{0\} \times \mathbb{Z}$, $\phi_3(a, b) = b$, $\ker \phi_3 = \mathbb{Z} \times \{0\}$.

6. Να βρεθούν τα αριστερά ιδεώδη του $\mathcal{M}_{2\times 2}(\mathbb{Z}_2)$

Το αριστερό ιδεώδες $\mathcal{M}_{2\times 2}(\mathbb{Z}_2)A = \{BA : B \in \mathcal{M}_{2\times 2}(\mathbb{Z}_2)\}$ είναι μη γνήσιο αν και μόνο αν A είναι αντιστρέψιμος πίνακας, δηλ. $\det A \neq 0$.

Θα ξεκινήσουμε λοιπόν υπολογίζοντας τα αριστερά μη μηδενικά ιδεώδη της μορφής $J = \mathcal{M}_{2\times 2}(\mathbb{Z}_2)A$ όπου $\det A = 0$ (και $A = (a_{ij}) \neq 0$).

Έστω ότι η δεύτερη στήλη του A είναι μηδενική, ενώ $a_{11} = 1$. Τότε αν πολλαπλασιάσουμε από τα αριστερά με τον πίνακα $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ και στη συνέχεια με πράξεις γραμμών, μπορούμε να δείξουμε ότι οι πίνακες

$$J = \{0, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\}$$

Αντίστοιχα αν η πρώτη στήλη του A είναι μηδενική.

Τέλος και στις τρεις περιπτώσεις που ο μη αντιστρέψιμος πίνακας A έχει μη μηδενικό στοιχείο και στις δύο στήλες, προκύπτει ότι

$$J = \{0, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\}$$

7. Έστω $I = \langle x^2 + 1 \rangle$ στο δακτύλιο $R = \mathbb{Z}_2[x]$. Να αποδείξετε ότι στο δακτύλιο R/I ισχύει ότι $x^n + I$ είναι ίσο είτε με $x + I$ είτε με $1 + I$. Να συμπεράνετε ότι $R/I = \{I, 1 + I, x + I, x + 1 + I\}$. Να βρείτε τους πίνακες πρόσθεσης και πολλαπλασιασμού του R/I.

Απάντηση Αν $n = 2k$, θα δείξουμε με επαγωγή στο k ότι $x^n + I = 1 + I$. Πράγματι, η πρόταση ισχύει για $k = 0$. Έστω αληθής για k. Τότε $x^{2(k+1)} + I = x^{2k}x^2 + I = (1 + I) * (1 + I) = 1 + I$. Με τον ίδιο τρόπο προκύπτει ότι αν $n = 2k+1$ τότε $x^{2k+1} = x + I$. Έπεται ότι αν $f(x) = a_n x^n + \cdots + a_1 x + a_0$ όπου $a_i \in \mathbb{Z}_2$, τότε $f(x) + I = b_1 x + b_0 + I$ όπου $b_i \in \mathbb{Z}_2$.

$+$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$1+I$	$1+I$	0	$(x+1)+I$	$x+I$
$x+I$	$x+I$	$(x+1)+I$	0	$1+I$
$(x+1)+I$	$(x+1)+I$	$x+I$	$1+I$	0

$.$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$x+I$	$0+I$	$x+I$	$1+I$	$(x+1)+I$
$(x+1)+I$	$0+I$	$(x+1)+I$	$(x+1)+I$	$0+I$

8. Έστω $J = \langle x^2 + x + 1 \rangle$ στο δακτύλιο $R = \mathbb{Z}_2[x]$. Να αποδείξετε ότι $R/J = \{J, 1 + J, x + J, x + 1 + J\}$. Να βρείτε τους πίνακες πρόσθεσης και πολλαπλασιασμού του R/J. Να συμπεράνετε ότι R/J είναι σώμα.

   Απάντηση Έχουμε ότι $x^2 + I = (x+1) + I$ ενώ $x^3 + I = (x^2 + x) + I = 1 + I$ και $x^4 + I = x + I$. Άρα $x^n + I \in \{1 + I, x + I, (x + 1) + I\}$. Όπως και προηγουμένως αν $f(x) = a_n x^N + \cdots + a_1 x + a_0$ όπου $a_i \in \mathbb{Z}_2$, τότε $f(x) + I = b_1 x + b_0 + I$ όπου $b_i \in \mathbb{Z}_2$.

$+$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$0+I$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$1+I$	$1+I$	0	$(x+1)+I$	$x+I$
$x+I$	$x+I$	$(x+1)+I$	0	$1+I$
$(x+1)+I$	$(x+1)+I$	$x+I$	$1+I$	0

$.$	$0+I$	$1+I$	$x+I$	$(x+1)+I$
$1+I$		$1+I$	$x+I$	$(x+1)+I$
$x+I$		$x+I$	$(x+1)+I$	$1+I$
$(x+1)+I$		$(x+1)+I$	$1+I$	$x+I$

9. Έστω $\phi: \ R[x] \longrightarrow R[a]$ ο ομομορφισμός εκτίμησης δακτυλίων, όπου $f(x) \mapsto f(a)$. Να βρείτε το πυρήνα του ϕ σε κάθε μία από τις παρακάτω περιπτώσεις: α) $\phi: \ \mathbb{Q}[x] \longrightarrow \mathbb{Q}[i]$, β) $\phi: \ \mathbb{C}[x] \longrightarrow \mathbb{C}[i]$, ς) $\phi: \ \mathbb{Z}[x] \longrightarrow \mathbb{Z}[0]$.

   Απάντηση

   α) Είναι φανερό ότι κανένα (μη μηδενικό) πολυώνυμο βαθμού 0 ή 1 δεν ανήκει στον $\ker\phi$. Επίσης $x^2+1 \in \ker\phi$. Έστω τώρα $f(x) \in \ker\phi$ βαθμού ≥ 2. Από τον Ευκλείδιο αλγόριθμο διαίρεσης δύο πολυωνύμων, έπεται ότι αν $f(x) \in \mathbb{Q}[x]$ τότε $f(x) = (x^2+1)p(x) + r(x)$ όπου $\deg r(x)$ είναι 0 ή 1. Άρα $\phi(f(x)) = \phi(x^2+1)\phi(p(x)) + \phi(r(x)) = 0$. Επομένως $r(x) \in \ker\phi$. Για να αποφύγουμε το άτοπο, $r(x) = 0$ και $f(x) = (x^2+1)p(x)$, άρα $\ker\phi = (x^2+1)$.

   β) Είναι φανερό ότι κανένα (μη μηδενικό) πολυώνυμο βαθμού 0 δεν ανήκει στον $\ker\phi$. Επίσης $x-i \in \ker\phi$. Έστω τώρα $f(x) \in \ker\phi$ βαθμού ≥ 1. Από τον Ευκλείδιο αλγόριθμο διαίρεσης δύο πολυωνύμων, έπεται ότι αν $f(x) \in \mathbb{Q}[x]$ τότε $f(x) = (x-i)p(x) + r(x)$ όπου $\deg r(x)$ είναι 0. Άρα $\phi(f(x)) = \phi(x-i)\phi(p(x)) + \phi(r(x)) = 0$. Επομένως $r(x) \in \ker\phi$. Για να αποφύγουμε το άτοπο, $r(x) = 0$ και $f(x) = (x-i)p(x)$, άρα $\ker\phi = \langle x-i \rangle$.

   γ) $\ker\phi = (x)$.

10. Έστω p πρώτος. Να δείξετε ότι στο σώμα $\mathbb{Z}_p$ τα στοιχεία $\overline{1}$ και $\overline{p-1}$ είναι τα μόνα στοιχεία που είναι αντίστροφα του εαυτού τους. Να αποφασίσετε αν ισχύει ότι $x^p + a = (x+a)^p$ στο $\mathbb{Z}_p[x]$.

    Απάντηση Τα στοιχεία που είναι αντίστροφα του εαυτού τους είναι ρίζες του πολυωνύμου x^2-1. Ένα πολυώνυμο δευτέρου βαθμού έχει το πολύ δύο ρίζες σε ένα σώμα. Το $\overline{1}$ και $\overline{p-1} = \overline{-1}$ είναι ρίζες.

    Είναι εύκολο να δει κανείς ότι p πρώτος διαιρεί $\binom{p}{k}$ για κάθε $k \neq 0, p$. Από το δυωνυμικό ανάπτυγμα προκύπτει ότι $(x+a)^p = x^p + a^p$. Αφού $a^p = a$ για κάθε a στο $\mathbb{Z}_p$ έπεται ότι $x^p + a = (x+a)^p$.

11. Να βρείτε το υπόλοιπο της διαίρεσης του πολυωνύμου $x^6 + 3x^5 + 4x^2 - 3x + 2$ με το $3x^2 + 2x - 3$ στο $\mathbb{Z}_7[x]$.

    Απάντηση $x^6+3x^5+4x^2-3x+2 = (x^2+2x-3)(5x^4+5x^2-x)-6x+2$.

12. Έστω τα πολυώνυμα $x^5 - 1$, $x^6 - 1$, $x^7 - x$ στο $\mathbb{Z}_{14}[x]$. Να βρείτε τις ρίζες τους.

Απάντηση $\phi(14) = 6$. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_{14}$ έχουν τάξη που διαιρεί το 6 και είναι ρίζες του $x^6 - 1$. Τα αντιστρέψιμα στοιχεία είναι τα $1, 3, 5, 9, 11, 13$. Η τάξη των στοιχείων που είναι ρίζες του $x^5 - 1$ πρέπει να διαιρεί το 5. Το μόνο στοιχείο που μπορεί να είναι ρίζα του $x^5 - 1$ είναι αυτό που έχει τάξη 1, δηλ. το 1. Είναι προφανές ότι όλα τα αντιστρέψιμα είναι ρίζες του $x(x^7 - 1)$. Επίσης 0 είναι ρίζα. Το ίδιο ισχύει για το 2: $2^4 = 2 \Rightarrow 2^7 = 2^4 2^3 = 2^4 = 2$. Αντίστοιχα για το 7. Έπεται ότι όλα τα στοιχεία του $\mathbb{Z}_{14}$ είναι ρίζες του $x^7 - x$: ($(ab)^7 = a^7 b^7 = ab$).

13. Έστω $I = \langle 3, \sqrt{2} \rangle$, $J = \langle 2, \sqrt{2} \rangle$ ιδεώδη στον $\mathbb{Z}[\sqrt{2}]$. Να βρείτε γεννήτορες για τα ιδεώδη $I + J$, IJ, $I \cap J$. Να αποδείξετε ότι αν $a + b\sqrt{2} \notin J$ τότε $J + \langle a + b\sqrt{2} \rangle = \mathbb{Z}[\sqrt{2}]$.

Απάντηση $I = \langle 1 \rangle$ αφού $2 = \sqrt{2}\sqrt{2} \in I$ και $3 - 2 \in I$. Επίσης $J = \langle \sqrt{2} \rangle$. Έπεται ότι $I + J = \mathbb{Z}[\sqrt{2}]$, $IJ = I \cap J = J$. Αν $a + b\sqrt{2} \notin J$ τότε αφού $b\sqrt{2} \in J$ έπεται ότι $a \notin J$. Επομένως $a \notin 2\mathbb{Z}$. Επομένως $a = 2k+1$. Έπεται ότι $J + \langle a + b\sqrt{2} \rangle = \langle \sqrt{2}, a \rangle = \langle 1 \rangle$ αφού $1 = (2k+1) - 2$.

14. Έστω $f(x, y) = x^4 + 2$. Να γράψετε το $f(x)$ ως γινόμενο αναγώγων παραγόντων στο $\mathbb{Z}[x, y]$, $\mathbb{Q}[x, y]$,$\mathbb{R}[x, y]$,$\mathbb{C}[x, y]$. Είναι το ιδεώδες $\langle f(x, y) \rangle$ μέγιστο στους αντίστοιχους δακτυλίους;

Έστω ότι $f(x, y) = f_1(x, y) f_2(x, y)$ τότε (κοιτάζοντας τον μεγαλύτερο βαθμό του y και στα δύο πολυώνυμα και στη συνέχεια στο γινόμενο f) προκύπτει ότι το y δεν εμφανίζεαι στα πολυώνυμα f_1, f_2. Άρα για να απαντήσουμε Θα θεωρήσουμε το πολυώνυμο $g(x) = x^4 + 2 \in \mathbb{Z}$. Για αυτό μπορούμε να δούμε ότι $\pm 1, \pm 2$ δεν είναι ρίζες του $g(x)$ και σύμφωνα με το θεώρημα που κάναμε προκύπτει ότι $g(x)$ δεν έχει ρίζα στο $\mathbb{Q}$. Θα δούμε τώρα αν μπορούμε να το γράψουμε ως γινόμενο δύο πολυωνύμων με ακέραιους συντελεστές βαθμού 2 το καθένα . Έστω $g_1(x) = a_2 x^2 + a_1 x + a_0$, $g_2(x) = b_2 x^2 + b_1 x + b_0$. Έπεται ότι $a_2 b_2 = 1 \Rightarrow a_2 = b_2 = \pm 1$. Επίσης $a_0 b_0 = 2$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a_0 = \pm 2$ ενώ $b_0 = \pm 1$. Αφού $a_2 b_0 + a_1 b_1 + a_0 b_2 = 0 \Rightarrow 1 + a_1 b_1 + 2 = 0 \Rightarrow a_1 b_1 = -3$. Τέλος $a_1 b_0 + b_1 a_0 = 0 \Rightarrow a_1 + 2b_1 = 0 \Rightarrow a_1 = -2b_1$. Αυτό όμως οδηγεί σε άτοπο αφού αντικαθιστώντας έχουμε: $(-2b_1) b_1 = -3$ που δεν έχει λύση στους ακεραίους. Άρα $g(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$ και κατά συνέπεια και στο $\mathbb{Q}[x]$ και αντίστοιχα και το πολυώνυμο $f(x, y)$ στους δακτυλίους $\mathbb{Z}[x, y]$

και $\mathbb{Q}[x, y]$. (Πολύ πιο γρήγορα θα μπορούσε να καταλήξει κανείς στο ίδιο αποτέλεσμα χρησιμοποιώντας το Κριτήριο του Eisenstein).

Παρατηρούμε ότι $x^4 + 2 = (x^2 - 2i)(x^2 + 2i)$ στο $\mathbb{C}[x]$ και αφού οι τετραγωνικές ρίζες του i είναι $\pm e^{i\pi/4}$ (δείτε τον μοναδιαίο κύκλο) έπεται ότι οι ρίζες του $x^4 + 2$ στο $\mathbb{C}$ είναι: $\pm\sqrt{2}e^{i\pi/4}$ και $\pm\sqrt{2}e^{3\pi/4}$. Επίσης $\overline{\sqrt{2}e^{i\pi/4}} = -\sqrt{2}e^{3\pi/4}$. Τελικά οι δύο παράγοντες του $x^4 + 2$ στο $\mathbb{R}[x, y]$ προκύπτουν από τα γινόμενα $(x - z)(x - \overline{z})$ όπου z είναι ρίζα του $x^4 + 2$ και είναι ίσοι με $x^2 - 2x + 2$ και $x^2 + 2x + 2$.

Στο $\mathbb{C}[x, y]$ το $f(x, y) = (x - e^{i\pi/4})(x + e^{i\pi/4})(x - e^{3i\pi/4})(x + e^{3i\pi/4})$. Το ιδεώδες $\langle f(x, y)\rangle$ ΔΕΝ είναι μέγιστο σε κανέναν από τους δακτυλίους αφού ισχύει $(f(x, y)) \subset (f(x, y), y)$.

15. Να γράψετε το $x^3 - y^3$ ως γινόμενο αναγώγων στο $\mathbb{Q}[x, y]$, $\mathbb{C}[x, y]$.

Ισχύει ότι $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$. Το πολυώνυμο $x - y$ είναι ανάγωγο αφού έχει βαθμό 1 στο x αλλά και y. Θα ελέγξουμε αν $x^2 + xy + y^2$ είναι ανάγωγο στο $\mathbb{Q}[x, y]$. Έστω ότι $x^2 + xy + y^2 = (a_1x + b_1y + c_1)(a_2x + b_2y + c_2)$. Έπεται ότι $a_1a_2 = 1$, $a_1b_2 + a_2b_1 = 1$, $a_1c_2 = 0 \Rightarrow c_2 = 0$, $b_1c_2 = 0 \Rightarrow c_2 = 0$, $b_1b_2 = 1$. Προκύπτει ότι $(a_1b_2)^2 - (a_1b_2) + 1 = 0$ που δεν έχει λύση στους πραγματικούς. Άρα $x^3 - y^3 = (x - y)(x^2 + xy + y^2)$ είναι η ανάλυση σε ανάγωγα στο $\mathbb{Q}[x, y]$.

Αφού $a_1b_2 = 1 + i\sqrt{3}/2$ είναι λύση της εξίσωσης $(a_1b_2)^2 - (a_1b_2) + 1 = 0$ μπορούμε να θέσουμε $a_1 = 1$ και $b_2 = 1 + i\sqrt{3}/2$. Άρα $x^2 + xy + y^2 = (x + \frac{2}{1+i\sqrt{3}}y)(x + \frac{1+i\sqrt{3}}{2}y)$.

3. Να αποφασίσετε αν $k[x]/\langle x^2 - 6x + 5\rangle$ είναι σώμα όταν $k = \mathbb{Q}, \mathbb{R}$. Ομοίως για τον δακτύλιο $k[x, y]/\langle x^2 - 6x + 6\rangle$.

Ο δακτύλιος πηλίκο $k[x]/\langle x^2 - 6x + 5\rangle$ θα είναι σώμα αν και μόνο αν το πολυώνυμο $x^2 - 6x + 5$ είναι ανάγωγο στον δακτύλιο $k[x]$. Αφού έχει ρίζες στο k, δεν είναι ανάγωγα στο $\mathbb{R}[x]$. Ο δεύτερος δακτύλιος πηλίκο είναι ακεραία περιοχή και όχι σώμα.

16. Να αποφασίσετε αν $x^3 + 3x^2 - 8$, $x^4 - 22x^2 + 1$ είναι ανάγωγα στο $\mathbb{Q}[x]$.

Για το πρώτο πολυώνυμο, αρκεί να ελέγξουμε αν έχει ρίζα από το σύνολο των διαιρετών του 8: $\{\pm1, \pm2, \pm4, \pm8\}$.

Για το δεύτερο πολυώνυμο παρατηρούμε ότι ±1 δεν είναι ρίζα. Αρκεί λοιπόν να βεβαιωθούμε ότι $f(x) = x^4 - 22x^2 + 1$ δε γράφεται ως γινόμενο πολυωνύμων βαθμού 2.

17. Να βρείτε όλα τα ανάγωγα πολυώνυμα βαθμού 3 στο $\mathbb{Z}_3[x]$.

    Θα θεωρήσουμε όλα τα πολυώνυμα βαθμού 3 στο $\mathbb{Z}_3[x]$ ($2 \times 3 \times 3 \times 3$ τέτοια πολυώνυμα) και θα κρατήσουμε μόνο εκείνα που δεν έχουν ρίζα στο $\mathbb{Z}_3$. Μπορούμε λοιπόν να αγνοήσουμε όλα εκείνα με σταθερό όρο 0 και μας μένει να εξετάσουμε ($2 \times 3 \times 3 \times 2$ περιπτώσεις.)

18. Έστω $f(x) = x^3 + 5x + 122$. Να βρείτε p έτσι ώστε $x^3 + \overline{5}x + \overline{122}$ να είναι ανάγωγο στο $\mathbb{Z}_p[x]$. Να συμπεράνετε ότι $f(x)$ είναι αναγκαστικά ανάγωγο στο $\mathbb{Q}[x]$. Είναι $f(x)$ ανάγωγο στο $\mathbb{R}[x]$;

    Όταν $p = 3$, $x^3+\overline{5}x+\overline{122} = x^3+2x+2$ και δεν έχει ρίζα στο $\mathbb{Z}_3$ άρα είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Αν $f(x)$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$ τότε στο $\mathbb{Z}[x]$ θα ισχύει ότι $f(x) = f_1(x)f_2(x)$ όπου $f_1(x), f_2(x)$ έχουν βαθμό μεγαλύτερο ή ίσο του 1. Ο αρχικός τους όρος είνι ± 1 και άρα περνώντας στο $\mathbb{Z}_3[x]$ θα πάρουμε μία ανάλυση και για το $x^5 + x + 2$, άτοπο. Το $f(x)$ ΔΕΝ ανάγωγο στο $\mathbb{R}[x]$ αφού έχει βαθμό μεγαλύτερο του 2.

19. Έστω $I = \langle x^4 + x^3 + x^2 + x + 1 \rangle$. Να αποδείξετε ότι το σύνολο

$$1 + I, x + 1, \dots, x^3 + I$$

    είναι βάση του $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}[x]/I$. Στη συνέχεια να βρείτε μία βάση του $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}[e^{2\pi i/5}]$.

    Απάντηση Ένα τυχαίο στοιχείο του $\mathbb{Q}[x]/I$ είναι της μορφής $f(x) + I$ όπου $f(x) \in \mathbb{Q}[x]$. Διαιρούμε $f(x)$ με το $x^4+x^3+x^2+x+1$. Προκύπτει ότι το υπόλοιπο είναι της μορφής $r(x)$ όπου $r(x) = 0$ οπότε $f(x)+I = I$ ή $\deg r(x) \leq 3$. Έπεται ότι κάθε μη μηδενικό στοιχείο του $\mathbb{Q}[x]/I$ είναι της μορφής

$$a_0 + a_1x + a_2x^2 + a_3x^3 + I = a_0(1 + I) + \cdots + a_3(x^3 + I)$$

    και επομένως $1 + I, x + I, \dots, x^3 + I$ παράγουν τον $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}[x]/I$. Θα δείξουμε ότι είναι γραμμικά ανεξάρτητα. Αν

$$a_0(1+I)+a_1(x+I)+a_2(x^2+I)+a_3(x^3+I) = I \Rightarrow a_0+\cdots+a_3x^3+I = I$$

$$\Rightarrow a_0 + \cdots + a_3x^3 \in I \Rightarrow a_0 = \cdots = a_3 = 0$$

    αφού κάθε μη μηδενικό στοιχείο του I έχει βαθμό τουλάχιστον 4. Μία βάση του $\mathbb{Q}$-διανυσματικού χώρου $\mathbb{Q}[e^{2\pi i/5}]$ είναι

$$1, e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5} \; .$$

(Βάσεις απεικονίζονται σε βάσεις μέσα από ισομορφισμούς διανυσματικών χώρων και τα παραπάνω είναι οι ομομορφικές εικόνες του προηγούμενου συνόλου).

20. Να βρείτε όλα τα πρώτα και όλα τα μέγιστα ιδεώδη του $\mathbb{Z}_5 \times \mathbb{Z}_4$.

    Απάντηση $\mathbb{Z}_5 \times (2)$ είναι πρώτο και μέγιστο. $\langle 0 \rangle \times \mathbb{Z}_4$ είναι πρώτο και μέγιστο.

21. Να αποφασίσετε αν $x^{169} - 10$, $4x^{20} - 18x^5 + 12x + 6$ είναι ανάγωγα στο $\mathbb{Q}[x]$ και στο $\mathbb{Z}[x]$.

    Απάντηση $x^{169} - 10$ είναι ανάγωγο σύμφωνα με το κριτήριο του Eisenstein για $p = 2$, άρα ανάγωγο στο $\mathbb{Q}[x]$ και στο $\mathbb{Z}[x]$. $4x^{20} - 18x^5 + 12x + 6 = 2(2x^{20} - 9x^5 + 6x + 3)$ ανάγωγο στο $\mathbb{Q}[x]$ (κριτήριο Eisenstein για το $2x^{20} - 9x^5 + 6x + 3$) αλλά όχι στο $\mathbb{Z}[x]$.

22. Να βρείτε δύο πρώτα ιδεώδη του $\mathbb{Z}[x]/\langle 2x^2 \rangle$ που να μην είναι μέγιστα. Στη συνέχεια να βρείτε τρία διαφορετικά μέγιστα ιδεώδη του $\mathbb{Z}[x]/\langle 2x^2 \rangle$.

    Απάντηση Έστω $I = \langle 2x^2 \rangle$. Τότε $\langle x \rangle / I$, $\langle 2 \rangle / I$ είναι πρώτα ιδεώδη, μη μέγιστα. $\langle x, 2 \rangle / I$, $\langle x, 3 \rangle / I$, $\langle 2, x + 1 \rangle / I$ είναι μέγιστα.

23. Να δείξετε ότι το σώμα κλασμάτων του $\mathbb{Z}[i]$ είναι το $\mathbb{Q}[i]$.

    Απάντηση Θα δείξουμε ότι $\mathbb{Q}[i]$ είναι το μικρότερο σώμα που περιέχει το $\mathbb{Z}[i]$. Πράγματι $\mathbb{Q}[i] (\cong \mathbb{Q}[x]/\langle x^2 + 1 \rangle$ είναι σώμα και περιέχει $\mathbb{Z}[i]$. Έστω K οποιοδήποτε άλλο σώμα που περιέχει το $\mathbb{Z}[i]$. Αφού $\mathbb{Z} \subset \mathbb{Z}[i]$ έπεται ότι $\mathbb{Q} \subset K$. Άρα K περιέχει και $a + bi \forall a, b \in \mathbb{Z}$.