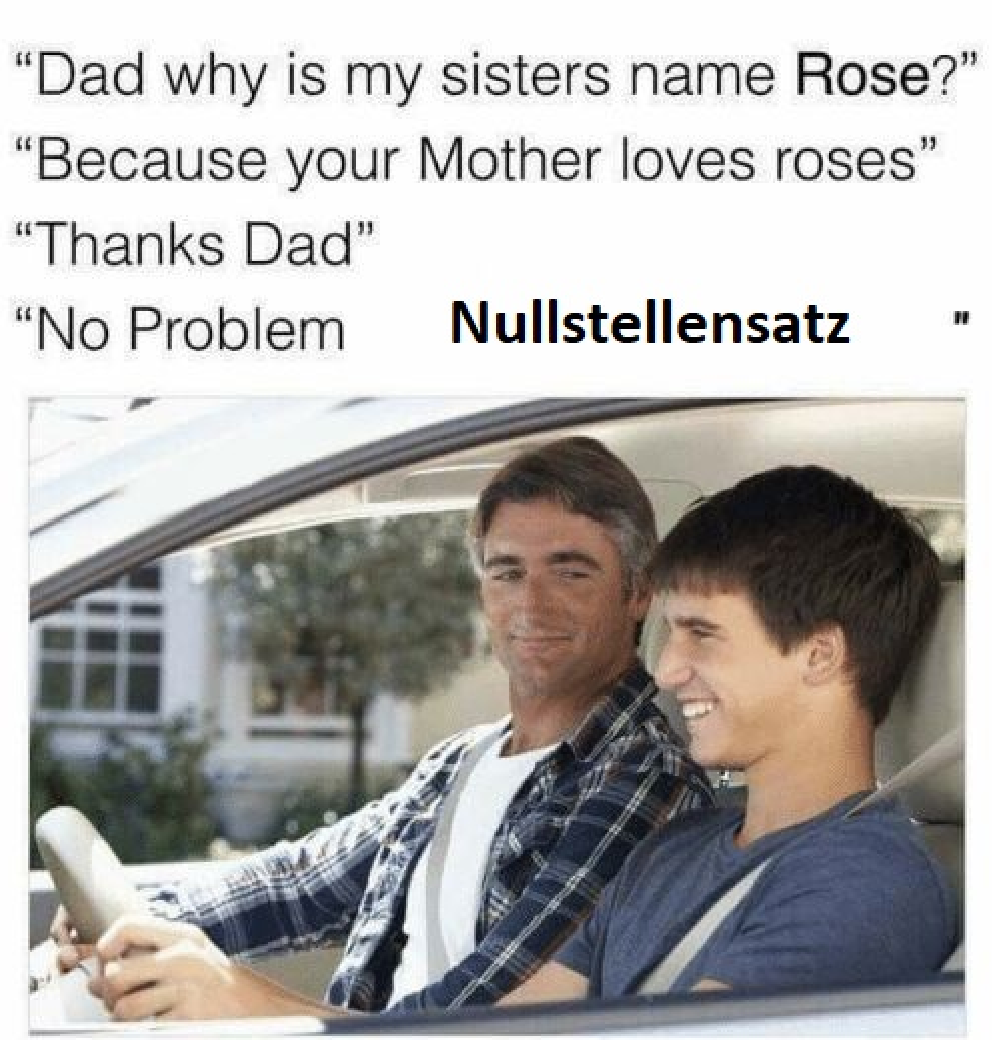
Μεταθετική Άλγεβρα

Εργασία 2

Ονομ/νο: Νούλας Δημήτριος
AM: 1112201800377
email: dimitriosnoulas@gmail.com

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837


"Dad why is my sisters name Rose?"
"Because your Mother loves roses"
"Thanks Dad"
"No Problem Nullstellensatz "

Άσκηση 2.1) Βρείτε τα πρώτα και μέγιστα ιδεώδη του R καθώς για το $nil(R)$ και $Jac(R)$ στις ακόλουθες περιπτώσεις.

(1) $R = \mathbb{Z}$.

(2) $R = \mathbb{Z}_n, n = p^2q^3, p, q$ διακεκριμένοι πρώτοι.

(3) $R = \mathbb{R}[x]$.

(4) $R = \mathbb{C}[x]$.

(5) $R = \mathbb{Q}[x]/(x^2(x-1))$.

Απόδειξη.

(1) Για το $R = \mathbb{Z}$ έχουμε ότι το $\mathbb{Z}/p\mathbb{Z}$ είναι σώμα και ακέραια περιοχή για p πρώτο. Αν έχουμε σύνθετο n το $\mathbb{Z}/n\mathbb{Z}$ έχει μηδενοδιαιρέτες και άρα δεν είναι καν περιοχή. Επιπλέον το (0) είναι πρώτο ιδεώδες καθώς $\mathbb{Z}/(0) \simeq \mathbb{Z}$ είναι περιοχή. Άρα τα πρώτα ιδεώδη είναι:

$$(p) \quad p \text{ πρώτος}, \, (0)$$

Τα μέγιστα είναι (p) με p πρώτο και

$$nil(\mathbb{Z}) = \bigcap_{p \text{ πρώτος}} (p) = (0)$$

καθώς για $p \neq q, p \notin (q)$. Διαφορετικά αν $x \in \mathbb{Z}$ με $x^n = 0 \implies x = 0$.

Επιπλέον

$$Jac(\mathbb{Z}) = (0) \cap \left(\bigcap_{p \text{ πρώτος}} (p) \right) = (0)$$

(2) Για το $R = \mathbb{Z}_n$ με $n = p^2q^3, p, q$ διακεκριμένοι πρώτοι έχουμε ότι τα ιδεώδη του $\mathbb{Z}_m$ είναι σε 1-1 και επί αντιστοιχία με τα ιδεώδη του $\mathbb{Z}$ που περιέχουν το (m). Άρα το διάγραμμα ιδεωδών του $\mathbb{Z}_n$ είναι

$$\begin{tikzcd}
 & & \mathbb{Z}_{p^2q^3} \arrow[dl, dash] \arrow[dr, dash] & & \\
 & ([p]) \arrow[dl, dash] \arrow[dr, dash] & & ([q]) \arrow[dl, dash] \arrow[dr, dash] & \\
([p^2]) \arrow[dr, dash] & & ([pq]) \arrow[dl, dash] \arrow[dr, dash] & & ([q^2]) \arrow[dl, dash] \\
 & ([p^2q]) \arrow[dr] & & ([pq^2]) \arrow[dl, dash] & \\
 & & ([p^2q^2]) \arrow[d, dash] & & \\
 & & (0) & &
\end{tikzcd}$$

και τα μέγιστα ιδεώδη όπως φαίνεται στο διάγραμμα είναι τα $([p]), ([q])$. Μπορούμε να το δούμε διαφορετικά ως:

$$\frac{\mathbb{Z}_{p^2q^3}}{([p])} = \frac{\mathbb{Z}/p^2q^3\mathbb{Z}}{p\mathbb{Z}/p^2q^3\mathbb{Z}} \simeq \mathbb{Z}/p\mathbb{Z}$$

όπου ο ισομορφισμός είναι από το 3ο θεώρημα ισομορφισμών δακτυλίων και αυτό είναι σώμα, άρα το $([p])$ είναι μέγιστο. Όμοια και το $([q])$.

καθώς σε έναν πεπερασμένο δακτύλιο θα έχουμε πεπερασμένα πηλίκα και κάθε πεπερασμένη περιοχή είναι σώμα, τα πρώτα με τα μέγιστα ιδεώδη ταυτίζονται. Άρα

$$nil(\mathbb{Z}_n) = Jac(\mathbb{Z}_n) = ([p]) \cap ([q]) = ([pq])$$

(3) Έχουμε το αποτέλεσμα ότι στα σώματα k τα ιδεώδη του $k[x]$ είναι κύρια. Για $k = \mathbb{R}$ από το θεμελιώδες θεώρημα της άλγεβρας, αν $deg(f(x)) \geq 3$ τότε υπάρχει $z \in \mathbb{C}$ έτσι ώστε

$$x^2 - (z + \overline{z})x + z\overline{z} \in \mathbb{R}[x]$$

$$(x^2 - (z + \overline{z})x + z\overline{z}) | f(x)$$

άρα τα ανάγωγα $f(x) \in \mathbb{R}[x]$ είναι τα πολυώνυμα βαθμού 1 και βαθμού 2 με αρνητική διακρίνουσα. Αν τώρα ένα $g(x)$ έχει παραγοντοποίηση τότε ο δακτύλιος $\mathbb{R}[x]/(g(x))$ θα έχει μηδενοδιαιρέτες και δεν θα είναι περιοχή.

Άρα τα μέγιστα ιδεώδη του $\mathbb{R}[x]$ είναι τα $(x - a), (x^2 + ax + b)$ με $a^2 - 4b < 0$ και τα πρώτα είναι τα ίδια μαζί με το (0) εφόσον $\mathbb{R}[x]$ περιοχή. Επιπλέον, ένα μη μηδενικό πολυώνυμο υπεράνω των πραγματικών θα έχει μη μηδενικό μεγιστοβάθμιο συντελεστή a_n και στο πολυώνυμο υψωμένο σε κάποια δύναμη m θα εμφανίζεται ο συντελεστής $(a_n)^m \neq 0$. Άρα δεν υπάρχουν μηδενοδύναμα στοιχεία, δηλαδή $nil(\mathbb{R}[x]) = (0)$.

Αν $f(x) \in Jac(\mathbb{R}[x])$ με $f(x)$ όχι το μηδενικό πολυώνυμο, τότε από την πρόταση 2.4.3 έχουμε ότι για κάθε $g(x) \in \mathbb{R}[x]$ ότι

$$1 - f(x)g(x) \in U(\mathbb{R}[x]) = \mathbb{R} \setminus \{0\}$$

άρα για $g(x) = x$ παίρνουμε το συμπέρασμα ότι το $f(x)$ πρέπει να είναι βαθμού 0 για να ισχύει ότι $deg(1 - f(x)g(x)) = 0$ ώστε να είναι αντιστρέψιμο. Αν $f(x) = c \in \mathbb{R}$, τότε για $g(x) = \frac{1}{c}$ παίρνουμε $0 \in \mathbb{R} \setminus \{0\}$ το οποίο είναι άτοπο. Άρα $Jac(\mathbb{R}[x]) = (0)$.

(4) Για $R = \mathbb{C}[x]$ όμοια με πριν, με το θεμελιώδες θεώρημα της άλγεβρας έχουμε ότι τα μόνα ανάγωγα πολυώνυμα είναι τα $x - a \in \mathbb{C}[x]$ και άρα τα μέγιστα ιδεώδη είναι τα $(x - a)$ και τα πρώτα τα ίδια μαζί με το (0). Με τα ίδια επιχειρήματα με το (3) έχουμε $nil(\mathbb{C}[x]) = Jac(\mathbb{C}[x]) = (0)$.

(5) Όμοια με το $\mathbb{Z}_n$ και την ανάλυση σε διαιρέτες, έχουμε το διάγραμμα ιδεωδών

$$\begin{tikzcd}
 & & \mathbb{Q}[x]/(x^2(x-1)) \arrow[dl, dash] \arrow[d, dash] \\
 & x\mathbb{Q}[x]/(x^2(x-1)) \arrow[dl, dash] \arrow[dr, dash] & (x-1)\mathbb{Q}[x]/(x^2(x-1)) \arrow[d, dash] \\
x^2\mathbb{Q}[x]/(x^2(x-1)) \arrow[dr, dash] & & x(x-1)\mathbb{Q}[x]/(x^2(x-1)) \arrow[dl, dash] \\
 & (0) &
\end{tikzcd}$$

$\square$

Όπως φαίνεται στο διάγραμμα, τα μέγιστα και πρώτα ιδεώδη είναι τα $([x]), ([x-1])$ (με αγκύλες εννούμε την κλάση modulo $x^2(x-1)$). Πράγματι έχουμε

$$R/([x]) = \frac{\mathbb{Q}[x]/(x^2(x-1))}{(x)/(x^2(x-1))} \simeq \mathbb{Q}[x]/(x) \simeq \mathbb{Q}$$

το οποίο είναι σώμα και όμοια το $([x-1])$.

Τα υπόλοιπα ιδεώδη δεν είναι πρώτα, το (0) δεν είναι καθώς ο R δεν είναι περιοχή. Έχουμε:

$$R/([x^2]) = \frac{\mathbb{Q}[x]/(x^2(x-1))}{(x^2)/(x^2(x-1))} \simeq \mathbb{Q}[x]/(x^2)$$

$$R/([x(x-1)]) = \frac{\mathbb{Q}[x]/(x^2(x-1))}{(x(x-1))/(x^2(x-1))} \simeq \mathbb{Q}[x]/(x(x-1))$$

τα οποία δεν είναι περιοχές αφού $x \cdot x = 0$ και $x(x-1) = 0$ αντίστοιχα.

Άρα

$$nil(R) = Jac(R) = ([x]) \cap ([x-1]) = ([x^2 - x]) = \frac{(x^2 - x)\mathbb{Q}[x]}{x^2(x-1)}$$

Άσκηση 2.2) Υπολογίστε το $\sqrt{I}$ στις ακόλουθες περιπτώσεις.

(1) $R = k[x,y], I = ((x-1)^3, y^4)$, όπου k σώμα.

(2) $R = k[x,y], I = (x-1, y^2 - 4y - xy + y + 4)$, όπου k σώμα.

(3) $R = \mathbb{Z}[x], I = (5, x^2+2)$.

Απόδειξη.

(1)

$$\sqrt{I} = \sqrt{((x-1)^3, y^4)} = \sqrt{((x-1)^3) + (y^4)} = \sqrt{\sqrt{((x-1)^3)} + \sqrt{(y^4)}} =$$
$$= \sqrt{\sqrt{(x-1)}^3 + \sqrt{(y)^4}} = \sqrt{(x-1) + (y)} = \sqrt{(x-1, y)} = (x-1, y)$$

όπου η τρίτη ισότητα είναι η ιδιότητα του ριζικού $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$. Στην τέταρτη ισότητα χρησιμοποιούμε ότι το κύριο ιδεώδες $((x-1)^3)$ είναι ίσο με το I^3 όπου $I = (x-1)$ και όμοια για το (y). Έπειτα χρησιμοποιούμε την ιδιότητα που φεύγουν οι ρίζες και οι δυνάμεις καθώς τα $(x-1), (y)$ είναι πρώτα ιδεώδη εφόσον:

$$k[x,y]/(x-1) \simeq k[y] \qquad k[x,y]/(y) \simeq k[x]$$

τα οποία είναι περιοχές. Στο τέλος εφαρμόζουμε την ίδια ιδιότητα καθώς το $(x-1, y)$ είναι μέγιστο και άρα πρώτο εφόσον

$$k[x,y]/(x-1,y) \simeq k$$

(2) Έχουμε $y^2 - 4y - xy + y + 4 = (y-2)^2 + y(1-x)$. Άρα

$$I = (x-1, y^2 - 4y - xy + y + 4) = (x-1, (y-2)^2 + y(1-x)) = (x-1, (y-2)^2)$$

Άρα με τις ίδιες ιδιότητες με πριν

$$\sqrt{I} = \sqrt{\sqrt{x-1} + \sqrt{((y-2)^2)}} = \sqrt{(x-1) + \sqrt{(y-2)}^2} =$$
$$= \sqrt{(x-1, y-2)} = (x-1, y-2)$$

(3)

$$\frac{\mathbb{Z}[x]}{(5, x^2+2)} \simeq \frac{\mathbb{Z}[x]/(5)}{(5, x^2+2)/(5)} \simeq \frac{\mathbb{Z}_5[x]}{(x^2+2)} \simeq \mathbb{F}_{5^2}$$

άρα το ιδεώδες είναι μέγιστο και συνεπώς $\sqrt{I} = I = (5, x^2+2)$.

Ο πρώτος ισομορφισμός προκύπτει από το 3ο θεώρημα ισομορφισμών. Για τον δεύτερο, από το 1ο θεώρημα ισομορφισμών για τον ομομορφισμό:

$$\pi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_5[x]$$
$$\sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} [a_i]_5 x^i$$

με πυρήνα το ιδεώδες (5) παίρνουμε ότι

$$\mathbb{Z}[x]/(5) \simeq \mathbb{Z}_5[x]$$

και ο περιορισμός του π στο ιδεώδες $(5, x^2+2)$ δίνει $(x^2+2) \simeq (5, x^2+2)/(5)$ και επειδή είναι ο περιορισμός του ισομορφισμού του "αριθμητή" έχουμε τον δεύτερο ισομορφισμό. Ο τελευταίος προκύπτει επειδή το x^2+2 είναι βαθμού 2 χωρίς ρίζες στο Z_5 και άρα το πηλίκο είναι σώμα.

□

Άσκηση 2.3) Έστω I, J ιδεώδη του δακτυλίου R. Δείξτε τις εξής σχέσεις.

(1) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(2) $\sqrt{I} = R \iff I = R$.

(3) $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$.

Απόδειξη.

(1) Έχουμε από ορισμό ριζικού $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$. Για την άλλη κατεύθυνση, έστω $x \in \sqrt{\sqrt{I}}$. Τότε υπάρχει $n \in \mathbb{Z}_{>0}$ τέτοιο ώστε $x^n \in \sqrt{I}$. Δηλαδή, υπάρχει $k \in \mathbb{Z}_{>0}$ τέτοιο ώστε $(x^n)^k \in I$. Άρα $x^{nk} \in I$, δηλαδή $x \in \sqrt{I}$.

(2) Αν $I = R$ επειδή $I \subseteq \sqrt{I}$ παίρνουμε $\sqrt{I} = R$. Αν $\sqrt{I} = R$, αυτό σημαίνει ότι $1 \in \sqrt{I}$ δηλαδή $1^n \in I$ για κάποιο θετικό n. Δηλαδή, $1 \in I \implies I = R$.

(3) Έστω $x \in \sqrt{I + J}$. Τότε υπάρχει $n \in \mathbb{Z}_{>0}$ τέτοιο ώστε $x^n \in I + J \subseteq \sqrt{I} + \sqrt{J}$. Δηλαδή, $x^n \in \sqrt{I} + \sqrt{J} \implies x \in \sqrt{\sqrt{I} + \sqrt{J}}$.

Αντίστροφα, έστω $x \in \sqrt{\sqrt{I} + \sqrt{J}}$. Υπάρχει $n \in \mathbb{Z}_{>0}$ τέτοιο ώστε $x^n = a + b \in \sqrt{I} + \sqrt{J}$ και επιπλέον υπάρχουν $k, \lambda \in \mathbb{Z}_{>0}$ τέτοια ώστε $a^k \in I, b^\lambda \in J$. Έχουμε:

$$(x^n)^{k+\lambda} = (a+b)^{k+\lambda} = \sum_{i=0}^{k+\lambda} \binom{k+\lambda}{i} a^i b^{k+\lambda-i} =$$

$$= a^k \left(\sum_{i=k}^{k+\lambda} \binom{k+\lambda}{i} a^{i-k} b^{k+\lambda-i} \right) + b^\lambda \left(\sum_{i=0}^{k-1} \binom{k+\lambda}{i} a^i b^{k-i} \right) \in I + J$$

δηλαδή $x^{n(k+\lambda)} \in I + J \implies x \in \sqrt{I + J}$.

□

Άσκηση 2.7) Έστω R, S δακτύλιοι. Δείξτε ότι κάθε πρώτο ιδεώδες του $R \times S$ είναι της μορφής $\mathfrak{p} \times S$ ή $R \times \mathfrak{q}$, όπου $\mathfrak{p}$ (αντίστοιχα $\mathfrak{q}$) είναι πρώτο ιδεώδες του R (αντίστοιχα S).
Αληθεύει ότι $nil(R \times S) = nil(R) \times nil(S)$;
Αληθεύει ότι $Jac(R \times S) = Jac(R) \times Jac(S)$;

Απόδειξη.

Θα δείξουμε κάποια αποτελέσματα πριν απαντήσουμε. Αρχικά, κάθε ιδεώδες I ενός δακτυλίου $R = R_1 \times R_2$ είναι της μορφής $I = I_1 \times I_2$ με I_1 ιδεώδες του R_1 και I_2 ιδεώδες του R_2.

Πράγματι, έστω I ιδεώδες του $R = R_1 \times R_2$. Θέτουμε:

$$I_1 = \{x_1 : \quad (x_1, 0) \in I\} \subseteq R_1$$

$$I_2 = \{x_2 : \quad (0, x_2) \in I\} \subseteq R_2$$

τα οποία είναι ιδεώδη των R_1, R_2 αντίστοιχα.

Πράγματι, αν $x, y \in I_1$ τότε $(x, 0), (y, 0) \in I$ και το I είναι ιδεώδες. Άρα $(x, 0) - (y, 0) = (x - y, 0) \in I$, δηλαδή $x - y \in I_1$. Επιπλέον αν $r \in R_1$, τότε $(r, r')(x, 0) = (rx, 0) \in I$. Δηλαδή $rx \in I_1$ και έτσι το I_1 είναι ιδεώδες του R_1 και όμοια το I_2 είναι ιδεώδες του R_2.

Τώρα ισχυριζόμαστε ότι $I = I_1 \times I_2$. Έχουμε ότι $I_1 \times 0, 0 \times I_2 \subseteq I$ και άρα

$$I \supseteq (I_1 \times 0) + (0 \times I_2) = I_1 \times I_2$$

Αντίστροφα, έστω $(x, y) \in I$. Τότε $(x, 0) = (1, 0)(x, y) \in I$ αφού το I είναι ιδεώδες, δηλαδή $x \in I_1$. Όμοια $y \in I_2$ και άρα $(x, y) \in I_1 \times I_2$.

Έχουμε επιπλέον τον ισομορφισμό:

$$R/I \simeq R_1/I_1 \times R_2/I_2$$

$$(r_1, r_2) + I \longmapsto (r_1 + I_1, r_2 + I_2)$$

Είναι πράγματι ισομορφισμός, το ομομορφισμός και το επί είναι προφανή. Για τον πυρήνα της απεικόνισης έχουμε:

$$(r_1 + I_1, r_2 + I_2) = (0, 0) \iff r_1 + I_1 = 0, r_2 + I_2 = 0 \iff r_1 \in I_1, r_2 \in I_2$$

$$\iff (r_1, 0), (0, r_2) \in I \implies (r_1, r_2) \in I = 0_{R/I}$$

άρα ο πυρήνας είναι τετριμμένος.

Ένα άλλο αποτέλεσμα είναι ότι ο δακτύλιος $R = R_1 \times R_2$ είναι περιοχή αν και μόνο αν ένα από τα R_1 ή R_2 είναι περιοχή και το άλλο είναι 0. Πράγματι, αν R περιοχή τότε:

$$(1, 0)(0, 1) = (0, 0) \implies (1, 0) = (0, 0) \text{ ή } (0, 1) = (0, 0)$$

άρα για κάποιον δακτύλιο θα ισχύει $1 = 0$, δηλαδή θα είναι ο τετριμμένος. Έτσι δίχως βλάβη γενικότητας, αν $R_2 = 0$ τότε:

$$xy = 0 \implies (xy, 0) = (0, 0) \iff (x, 0)(y, 0) = (0, 0)$$

$$\implies (x, 0) = (0, 0) \text{ ή } (y, 0) = (0, 0) \iff x = 0 \text{ ή } y = 0$$

Αντίστροφα, αν R_1 περιοχή και $R_2 = 0$ τότε:

$$(x, 0)(y, 0) = (0, 0) \iff (xy, 0) = (0, 0) \iff xy = 0$$

$$\implies x = 0 \text{ ή } y = 0 \implies (x, 0) = (0, 0) \text{ ή } (y, 0) = (0, 0)$$

Έστω τώρα ο δακτύλιος $R \times S$ και $P = (P_1, P_2)$ ένα πρώτο ιδεώδες του. Τότε ο δακτύλιος πηλίκο $(R \times S)/P$ είναι περιοχή. Δηλαδή μέσω του ισομορφισμού έχουμε την περιοχή $R/P_1 \times S/P_2$.

Με βάση τα προηγούμενα αποτελέσματα, στην πρώτη περίπτωση αν $S/P_2 = 0$ έχουμε $S = P_2$ και R/P_1 περιοχή, δηλαδή P_1 πρώτο ιδεώδες του R. Άρα $P = (\mathfrak{p}, S)$ στην πρώτη περίπτωση και $P = (R, \mathfrak{q})$ όμοια στην άλλη περίπτωση όπου $R/P_1 = 0$.

$$\begin{aligned} nil(R \times S) &= \bigcap_{P \trianglelefteq R \times S \text{ πρώτο}} P = \left(\bigcap_{\mathfrak{p} \trianglelefteq R \text{ πρώτο}} \mathfrak{p} \times S \right) \bigcap \left(\bigcap_{\mathfrak{q} \trianglelefteq S \text{ πρώτο}} R \times \mathfrak{q} \right) = \\ &= \left(\left(\bigcap_{\mathfrak{p} \trianglelefteq R \text{ πρώτο}} \mathfrak{p} \right) \times S \right) \bigcap \left(R \times \left(\bigcap_{\mathfrak{q} \trianglelefteq S \text{ πρώτο}} \mathfrak{q} \right) \right) = \\ &= (nil(R) \times S) \bigcap (R \times nil(S)) = nil(R) \times nil(S) \end{aligned}$$

Για το $Jac(R \times S)$, αν $\mathfrak{m}$ μεγιστικό ιδεώδες τότε θα είναι και πρώτο. Άρα $\mathfrak{m} = \mathfrak{p} \times S$ ή $R \times \mathfrak{q}$ με $\mathfrak{p}$ ή αντίστοιχα $\mathfrak{q}$ πρώτο. Ωστόσο, θα έχουμε ότι $(R \times S)/m$ σώμα ισόμορφο με $R/\mathfrak{p} \times 0$ αν βρισκόμαστε στην πρώτη περίπτωση. Δηλαδή, το $R/\mathfrak{p}$ είναι σώμα και άρα $\mathfrak{p}$ μεγιστικό. Συνεπώς έχουμε τις ίδιες πράξεις με παραπάνω:

$$\begin{aligned} Jac(R \times S) &= \bigcap_{P \trianglelefteq R \times S \text{ μέγιστο}} P = \left(\bigcap_{\mathfrak{p} \trianglelefteq R \text{ μέγιστο}} \mathfrak{p} \times S \right) \bigcap \left(\bigcap_{\mathfrak{q} \trianglelefteq S \text{ μέγιστο}} R \times \mathfrak{q} \right) = \\ &= \left(\left(\bigcap_{\mathfrak{p} \trianglelefteq R \text{ μέγιστο}} \mathfrak{p} \right) \times S \right) \bigcap \left(R \times \left(\bigcap_{\mathfrak{q} \trianglelefteq S \text{ μέγιστο}} \mathfrak{q} \right) \right) = \\ &= (Jac(R) \times S) \bigcap (R \times Jac(S)) = Jac(R) \times Jac(S) \end{aligned}$$

Αν επιχειρηματολογήσουμε χωρίς να βασιστούμε στα προηγούμενα, έστω $(x, y) \in nil(R \times S)$. Τότε για κάποιο n ισχύει $(0, 0) = (x, y)^n = (x^n, y^n)$ και άρα $x \in nil(R), y \in nil(S) \implies (x, y) \in nil(R \times S)$. Αντίστροφα, αν $x \in nil(R), y \in nil(S)$ τότε υπάρχουν $n, m \in \mathbb{Z}_{>0}$ έτσι ώστε $x^n = 0_R, y^m = 0_S$. Αν $k = \max\{n, m\}$ τότε

$$(x, y)^k = (x^k, y^k) = (0, 0)$$

άρα $(x, y) \in nil(R \times S)$.

Όμοια, αν $(x, y) \in Jac(R \times S)$ τότε για κάθε $(r, s) \in R \times S$ έχουμε

$$(1, 1) - (x, y)(r, s) \in U(R \times S) = U(R) \times U(S)$$

$$\iff (1 - xr, 1 - ys) \in U(R) \times U(S)$$

$$\iff x \in Jac(R), \quad y \in Jac(S)$$

□

Άσκηση 2.10) Τα μόνα ταυτοδύναμα στοιχεία τοπικού δακτυλίου είναι τα $0, 1$.

Απόδειξη.

Έστω $e \neq 0, 1$. Τότε $e^2 = e \implies 0 = e(1-e)$. Δηλαδή, τα $e, (1-e) \neq 0$ είναι μηδενοδιαιρέτες και άρα όχι αντριστρέψιμα. Έτσι το ιδεώδες (e) περιέχεται σε κάποιο μέγιστο ιδεώδες $\mathfrak{m}$. Αυτό είναι μοναδικό καθώς βρισκόμαστε σε τοπικό δακτύλιο και άρα το e ανήκει στην τομή όλων των μεγίστων ιδεωδών, δηλαδή $e \in Jac(R)$. Με την πρόταση 2.4.3 αυτό είναι ισοδύναμο με:

$$e \in Jac(R) \iff (1 - er) \in U(R) \quad \forall r \in R$$

και για $r = 1$ παίρνουμε ότι το $1 - e$ είναι αντριστρέψιμο, το οποίο είναι άτοπο.

$\square$

Άσκηση 2.12) Έστω $V \subseteq k^n$ μη κενό αλγεβρικό σύνολο.

(1) Δείξτε ότι το $I(V)$ είναι ιδεώδες του $k[x_1, \ldots, x_n]$ και

$$k[x_1, \ldots, x_n]/I(V) \simeq k[V]$$

(2) Δείξτε ότι $nil(k[V]) = 0$.

(3) Για κάθε $P \in V$, έστω $\mathfrak{m}_P \in k[V]$ τό σύνολο των πολυωνυμικών συναρτήσεων του $k[V]$ που μηδενίζονται στο P. Δείξτε ότι το $\mathfrak{m}_P$ είναι μέγιστο ιδεώδες του $k[V]$.

(4) Σύμφωνα με το (3) έχουμε μια απεικόνιση

$$P \mapsto \mathfrak{m}_P$$

από το V στα ιδεώδη του $k[V]$. Δείξτε ότι αυτή η απεικόνιση είναι $1-1$.

Απόδειξη.

Όπου x θα συμβολίζουμε το $(x_1, x_2, \ldots, x_n)$ στα παρακάτω

(1) Έστω $f(x), g(x) \in I(V)$ και $h(x) \in k[x_1, \ldots, x_n]$. Τότε για τυχόν $P \in V$ έχουμε:

$$0 = f(P) - g(P) = (f-g)(P)$$

άρα το πολυώνυμο $f(x) - g(x) = (f-g)(x)$ ανήκει στο $I(V)$. Επιπλέον

$$(hf)(P) = h(P)f(P) = h(P) \cdot 0 = 0$$

άρα και το πολυώνυμο $h(x)f(x) = (hf)(x)$ ανήκει στο $I(V)$, δηλαδή το $I(V)$ είναι ιδεώδες του $k[V]$.

Ορίζουμε την απεικόνιση

$$\begin{aligned} \phi : k[x_1, \ldots, x_n] &\longrightarrow k[V] \\ f &\longmapsto f_V : V \to k \\ & \qquad P \mapsto f(P) \end{aligned}$$

Η απεικόνιση ϕ είναι επί εφόσον περιορίζουμε κάθε πολυώνυμο στο υποσύνολο V του k^n. Είναι επιπλέον ομομορφισμός καθώς:

$$\phi(f+g)(P) = (f+g)_V(P) = (f+g)(P) = f(P) + g(P) = f_V(P) + g_V(P) =$$

$$= (f_V + g_V)(P) = [\phi(f) + \phi(g)](P)$$

$$\phi(fg)(P) = (fg)_V(P) = (fg)(P) = f(P)g(P) = f_v(P)g_v(P) = [\phi(f)\phi(g)](P)$$

Αν τώρα $f(x) \in I(V)$ τότε $f_V(P) = f(P) = 0$ για κάθε $P \in V$ δηλαδή η f_V είναι η μηδενική απεικόνιση από το V στο k και άρα $f(x) \in ker\phi$.

Αντίστροφα, αν

$$\begin{aligned} \phi(f) = 0_{k[V]} : V &\to k \\ P &\mapsto 0 = f(P) \quad \forall P \in V \end{aligned}$$

τότε $f(x) \in I(V)$. Άρα $ker\phi = I(V)$ και από το 1ο θεώρημα ισομορφισμών δακτυλίων παίρνουμε:

$$k[x_1, \ldots, x_n]/I(V) \simeq k[V]$$

(2) Έστω $f_V \in nil(k[V])$. Τότε υπάρχει $n \in \mathbb{Z}_{>0}$ τέτοιο ώστε $(f_V)^n = 0_{k[V]} : V \to k$. Το $0_{k[V]}$ είναι ως συνάρτηση το μηδενικό πολυώνυμο περιορισμένο στο V.

Αν υποθέσουμε ότι το f_V δεν είναι περιορισμός του μηδενικού πολυωνύμου τότε θα έχει μεγιστοβάθμιο συντελεστή (ως προς όλες τις μεταβλητές $x_1, \dots x_n$) $a_m \neq 0 \in k$.

Τότε στο $(f_V)^n$ θα εμφανίζεται ο συντελεστής $(a_m)^n$ ο οποίος από την υπόθεση θα είναι 0. Δηλαδή, το στοιχείο a_m του σώματος k θα είναι 0 το οποίο είναι άτοπο.

(3) Έστω $P \in V$, το $\mathfrak{m}_P = \{f_V \in k[V] : \quad f_V(P) = 0\}$ είναι ιδεώδες εφόσον:

$$(f_V - g_V)(P) = f_V(P) - g_V(P) = 0 - 0 = 0$$

$$(g_V f_V)(P) = g_V(P) f_V(P) = g_V(P) \cdot 0 = 0$$

Ορίζουμε τον ομομορφισμό εκτίμησης ϕ_P στο P

$$k[V] \longrightarrow k$$

$$f_V \longmapsto f_V(P) = f(P)$$

ο οποίος είναι επί εφόσον μπορούμε να θεωρήσουμε τα σταθερά πολυώνυμα $f(x) = a$ για κάθε όρο $a \in k$ και να τα περιορίσουμε στο V.

Αν $f_V \in \mathfrak{m}_P$ τότε $\phi_P(f_V) = f_V(P) = 0$, άρα $\mathfrak{m} \subseteq ker\phi_P$.

Αντίστροφα, αν $f_v \in ker\phi_P$ τότε $\phi_P(f_V) = 0$, όμως $\phi_P(f_V) = f_V(P)$. Άρα $f_V(P) = 0$, δηλαδή $f_V \in \mathfrak{m}_P$.

Επομένως, από το 1ο θεώρημα ισομορφισμών δακτυλίων παίρνουμε

$$\frac{k[V]}{\mathfrak{m}_P} \simeq k$$

και άρα εφόσον το k είναι σώμα, το $\mathfrak{m}_P$ είναι μέγιστο ιδεώδες.

(4) Έστω $P, Q \in V$ και ότι

$$\mathfrak{m}_P = \mathfrak{m}_Q$$

$$\{f_V \in k[V] : \quad f_V(P) = 0\} = \{f_V \in k[V] : \quad f_V(Q) = 0\}$$

Αν $P = (P_1, \dots, P_n), Q = (Q_1, \dots, Q_n)$ τότε για $i = 1, \dots, n$ θεωρούμε τα πολυώνυμα:

$$f_i(x) = x_i - P_i$$

και ισχύει ότι $(f_i)_V \in \mathfrak{m}_P$ αφού $(f_i)_V(P) = f_i(P) = P_i - P_i = 0$. Από την ισότητα των συνόλων έχουμε ότι τα $(f_i)_V$ ανήκουν στο $\mathfrak{m}_Q$ δηλαδή μηδενίζονται στο Q. Αυτό σημαίνει ότι $Q_i - P_i = 0$ για κάθε $i = 1, \dots, n$. Άρα $P = Q$.

$\square$

Άσκηση 2.14) Έστω $\phi : R \to S$ ένας ομομορφισμός δακτυλίων.

(1) Δείξτε ότι αν $\mathfrak{q}$ είναι πρώτο ιδεώδες του S, τότε το σύνολο $\phi^{-1}(\mathfrak{q})$ είναι πρώτο ιδεώδες του R.

(2) Αληθεύει ότι αν $\mathfrak{m}$ είναι μέγιστο ιδεώδες του S, τότε το σύνολο $\phi^{-1}(\mathfrak{m})$ είναι μέγιστο ιδεώδες του R;

Απόδειξη.

(1) Έστω $a, b \in R$ με $ab \in \phi^{-1}(\mathfrak{q})$. Δηλαδή, υπάρχει $y \in \mathfrak{q}$ τέτοιο ώστε $y = \phi(ab) = \phi(a)\phi(b)$. Άρα $\phi(a)\phi(b) \in \mathfrak{q}$ το οποίο είναι πρώτο. Έπεται ότι

$$\phi(a) \in \mathfrak{q} \quad \text{ή} \quad \phi(b) \in \mathfrak{q} \implies a \in \phi^{-1}(\mathfrak{q}) \quad \text{ή} \quad b \in \phi^{-1}(\mathfrak{q})$$

άρα το $\phi^{-1}(\mathfrak{q})$ είναι πρώτο ιδεώδες του R.

(2) Δεν αληθεύει. Αν θεωρήσουμε την εμφύτευση $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ και το μοναδικό μέγιστο ιδεώδες $\{0\}$ του $\mathbb{Q}$, είναι μέγιστο αφού $\mathbb{Q}/\{0\} \simeq \mathbb{Q}$ σώμα, έχουμε:

$$i^{-1}(\{0\}) = \{0\}$$

το οποίο φυσικά είναι πρώτο ιδεώδες του $\mathbb{Z}$ αλλά όχι μέγιστο, διαφορετικά θα είχαμε $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$ σώμα που δεν ισχύει.

$\square$

Άσκηση 2.16) Δείξτε ότι ο δακτύλιος

$$\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \in \mathbb{C} : a, b \in \mathbb{Z}\}$$

δεν είναι περιοχή μοναδικής παραγοντοποίησης.

Απόδειξη.

Έχουμε $2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3}) = 4$. Θα δείξουμε ότι κανένα από τα $2, 1 \pm \sqrt{-3}$ δεν είναι αντιστρέψιμο και ότι όλα είναι ανάγωγα.

Ορίζουμε το μέτρο του μιγαδικού

$$N : \mathbb{Z}[\sqrt{-3}] \longrightarrow \mathbb{N}$$

$$a + b\sqrt{-3} \longmapsto |a + b\sqrt{-3}|^2 = a^2 + 3b^2$$

και έχουμε $N(xy) = N(x)N(y)$.

Αν $u \in U(\mathbb{Z}[\sqrt{-3}])$ τότε $uv = 1$ και άρα $1 = N(u)N(v) \implies N(u) = 1$. Δηλαδή $a^2 + 3b^2 = 1$ με $a, b \in \mathbb{Z}$ το οποίο συμβαίνει μόνο όταν $a = \pm 1, b = 0$. Άρα $U(\mathbb{Z}[\sqrt{-3}]) = \{\pm 1\}$.

Δείχνουμε ότι το 2 είναι ανάγωγο. Αν $2 = xy$ με $x, y \in \mathbb{Z}[\sqrt{-3}]$ τότε

$$4 = N(2) = N(xy) = N(x)N(y)$$

αν $N(x) = a^2 + 3b^2$ έχουμε:

$$N(x) = \begin{cases} 1, & x \in U(\mathbb{Z}[\sqrt{-3}]) \\ 2, & a^2 + 3b^2 = 2, \text{ δεν μπορεί να ισχύει} \\ 4, & N(y) = 1 \implies y \in U(\mathbb{Z}[\sqrt{-3}]) \end{cases}$$

άρα το 2 είναι ανάγωγο σε κάθε δυνατή περίπτωση του $N(x)$. Όμοια είναι και τα υπόλοιπα ανάγωγα αφού $4 = N(1 \pm \sqrt{-3})$.

Άρα το $\mathbb{Z}[\sqrt{-3}]$ δεν είναι περιοχή μοναδικής παραγοντοποίησης καθώς τα $2, 1 \pm \sqrt{-3}$ είναι όλα ανάγωγα και έτσι η σχέση $2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$ θα έπρεπε να μας δίνει ότι $2 = u(1 \pm \sqrt{-3})$ το οποίο δεν ισχύει για κανένα αντιστρέψιμο $u = \pm 1$. $\square$