Άσκηση! Έστω $I_1, I_2, \dots, I_n$ μέγιστα ιδεώδη (1)
του R με $I_1 I_2 \cdots I_n = \{0\}$.
Αν P πρώτο ιδεώδες του R, τότε υπάρχει
$i \in \{1, \dots, n\}$ με $P = I_i$.
Απόδειξη Έστω $P \neq I_i$ $\forall i = 1, \dots, n$.
Επειδή I_i μέγιστο $I_i \not\subseteq P$ και άρα υπάρχει
$x_i \in I_i \setminus P$.
Έχουμε $x_1 x_2 \cdots x_n \in I_1 I_2 \cdots I_n = \{0\} \Rightarrow$
$\Rightarrow x_1 x_2 \cdots x_n = 0 \in P$ και επειδή P πρώτο,
$x_i \in P$ για κάποιο $i \in \{1, \dots, n\}$, άτοπο.

Επεκτάσεις και **συστολές** ιδεωδών.
extensions contractions

Έστω R, S δακτύλιοι και $f : R \to S$ ομομορφισμός. Αν J ιδεώδες του S τότε το $f^{-1}(J)$ ιδεώδες του R.
Πράγματι, έστω $x, y \in f^{-1}(J)$ και $r \in R$.
Τότε $f(x), f(y) \in J \Rightarrow f(x+y) = f(x) + f(x) \in J \Rightarrow$
$\Rightarrow x + y \in f^{-1}(J)$.
Αν $x \in f^{-1}(J)$ και $r \in R$, τότε $f(x) \in J$ και
$f(r) f(x) = f(rx) \in J \Rightarrow rx \in f^{-1}(J)$
Το $f^{-1}(J)$ λέγεται __συστολή__ του J ως προς την f. Αν f γνωστή, γράφουμε $J^c = f^{-1}(J)$
Ανάποδα: Έστω I ιδεώδες του R. Το $f(I)$ δεν είναι πάντοτε ιδεώδες του S
Παράδειγμα: $R = \mathbb{Z}$, $S = \mathbb{Q}$ και $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ η εμφύτευση. Αν $I = 2\mathbb{Z}$, τότε
$f(I) = 2\mathbb{Z} \subseteq \mathbb{Q}$ σώμα. Τα μόνα ιδεώδη του $\mathbb{Q}$ είναι το $\{0\}$ και το $\mathbb{Q}$. Άρα $f(I) = 2\mathbb{Z}$

όχι ιδεώδες του R.

Αν I ιδεώδες του R, τότε $f(I) \subseteq S$. Το ιδεώδες που παράγεται από το $f(I)$ λέγεται επέκταση (extension) του I και συμβολίζεται με I^e. Άρα $I^e = \{ \underbrace{\sum s_i f(x_i)}_{\text{πεπερασμένο}} \mid s_i \in S, x_i \in I \}$.

(μπορεί κάποιο $s_i \notin f(R) \subseteq S$)

Έστω $\mathcal{A} = \{ J^c \subseteq R \mid J$ ιδεώδες του $S \}$ και
$\mathcal{B} = \{ I^e \subseteq S \mid I$ ιδεώδες του $R \}$.

Τότε υπάρχει 1-1 και επί (bijection) αντιστοιχία $\mathcal{A} \xleftrightarrow{T} \mathcal{B}$ με $T(J^c) = J^{ce}$ για κάθε ιδεώδες J του S και $T^{-1}(I^e) = I^{ec}$ για κάθε ιδεώδες I του R.

Απόδειξη: $J^c = f^{-1}(J) = \{ x \in R \mid f(x) \in J \}$.
Εφόσον $f(x) \in J$ $\forall x \in J^c \Rightarrow J^{ce} = \{ \sum s_i f(x_i) \mid s_i \in S, x_i \in J \} \subseteq J$. Συνεπώς $J^{cec} = f^{-1}(J^{ce}) \subseteq f^{-1}(J) = J^c$. Αν $x \in J^c$

Τότε $\underbrace{f(x)}_{\in J} = 1_S f(x) \in \{ \sum s_i f(x_i) \mid x_i \in J^c, s_i \in S \} = J^{ce}$. Άρα $x \in f^{-1}(J^{ce}) = J^{cec}$. Τελικώς $J^c \subseteq J^{cec}$ και άρα $J^c = J^{cec}$. Άρα $J^c = T^{-1}T(J^c)$

Έστω $y \in I^e$, όπου I ιδεώδες του R.

Τότε $y = \sum s_i f(x_i)$, $s_i \in S$, $x_i \in I$.

Τότε $f^{-1}(y) \in f^{-1}(I^e) = I^{ec}$. $\Rightarrow$

$\Rightarrow y \in f(I^{ec}) \subseteq I^{ece}$

Άρα $I^e \subseteq I^{ece}$.

Αντιστρόφως, έστω $y \in I^{ece}$. Τότε
$y = \sum s_i f(x_i)$, $s_i \in S$, $x_i \in I^{ec}$.
$x_i \in I^{ec} = f^{-1}(I^e) \Rightarrow f(x_i) = I^e \ \forall i$
Άρα και $y = \sum s_i f(x_i) \in I^e$. Συνεπώς
$I^{ece} \subseteq I^e$. Τελικώς $I^e = I^{ece} =$
$= T\,T^{-1}(I^e)$

Εφόσον $T^{-1}T(J^c)\ \forall J^c \in \mathcal{A}$ και
$T\,T^{-1}(I^e)\ \forall I^e \in \mathcal{B}$ η T είναι 1-1
<u>και επί.</u>

<u>Άσκηση:</u> Έστω $f: R \to S$ ομομορφισμός και
I_1, I_2 ιδεώδη του R και J_1, J_2 ιδεώδη του S.
<u>Τότε:</u> 1) $(I_1 + I_2)^e = I_1^e + I_2^e$.
2) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$.
3) $(I_1 I_2)^e = I_1^e I_2^e$.
4) $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$ (Υπενθυμίζουμε ότι αν I_1, I_2 ιδεώδη του R τότε το $(I_1 : I_2) = \{r \in R \mid rI_1 \subseteq I_2\}$ και είναι ιδεώδες του R (ελέγξτε, το έχουμε δείξει)
5) ~~$\sqrt{I}$~~ $(\sqrt{I})^e \subseteq \sqrt{I^e}$
6) $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$.
7) $(J_1 \cap J_2)^c = J_1^c J_2^c$

8) $(J_1 J_2)^c \supseteq J_1^c J_2^c$.

9) $(J_1 : J_2)^c \subseteq (J_1^c : J_2^c)$

10) $(\sqrt{J})^c = \sqrt{J^c}$.

<u>Απόδειξη:</u> 1) Προφανής (Δείξτε τη)

2) $I_1 \cap I_2 \subseteq I_1 \Rightarrow (I_1 \cap I_2)^e \subseteq I_1^e$.
Ομοίως $(I_1 \cap I_2)^e \subseteq I_2^e$. Άρα $(I_1 \cap I_2)^e \subseteq$
$\subseteq I_1^e \cap I_2^e$.

3) Έστω $y \in (I_1 I_2)^e$. Τότε

$$y = \sum_i s_i f(x_i), \quad s_i \in S, \quad x_i \in I_1 I_2.$$

Εφόσον $x_i \in I_1 I_2$, $x_i = \sum_j t_{ij} x_{ij} x_{ij}'$,
$t_{ij} \in R$, $x_{ij} \in I_1$, $x_{ij}' \in I_2$

Άρα $y = \sum_i s_i f\left(\sum_j t_{ij} x_{ij} x_{ij}'\right) =$

$$= \sum_j \sum_i s_i f(t_{ij} x_{ij}) f(x_{ij}')$$

Αλλά $f(t_{ij} x_{ij}) \in f(I_1) \subseteq I_1^e$ και $f(x_{ij}') \subseteq f(I_2) \subseteq$
$\subseteq I_2^e$. Συνεπώς $\sum_i s_i f(t_{ij} x_{ij}) f(x_{ij}') \in$
$\in I_1^e I_2^e \ \forall j \Rightarrow y = \sum_j \sum_i s_i f(t_{ij} x_{ij}) f(x_{ij}') \in$
$\in I_1^e I_2^e$. $\left| (I_1 I_2)^e \subseteq I_1^e I_2^e \right|$

Έστω $y \in I_1^e I_2^e$. Τότε $y = \sum s_i y_i y_i'$,
$s_i \in S$, $y_i \in I_1^e$, $y_i' \in I_2^e$.

$y_i = \sum_j s_{ij} f(x_{ij})$, $s_{ij} \in S$, $x_{ij} \in I_1$

$y_i' = \sum_\lambda s_{i\lambda}' f(x_{i\lambda}')$, $s_{i\lambda}' \in S$, $x_{i\lambda}' \in I_2$

Τότε $y = \sum_i s_i \sum_j \sum_\lambda s_{ij} f(x_{ij}) s'_{i\lambda} f(x'_{i\lambda}) =$

$$= \sum_{i,j,\lambda} \underbrace{s_i s_{ij} s'_{i\lambda}}_{\in S} f(\underbrace{x_{ij} x'_{i\lambda}}_{\in I_1 I_2}) \in (I_1 I_2)^e.$$

Άρα $I_1^e I_2^e \subseteq (I_1 I_2)^e$ και επειδή $(I_1 I_2)^e \subseteq I_1^e I_2^e$, έπεται $(I_1 I_2)^e = I_1^e I_2^e$.

5) $y \in (\sqrt{I})^e$. Τότε $y = \sum_{i=1}^n s_i f(x_i)$, όπου $x_i \in \sqrt{I} \subseteq R$ $\forall i = 1, \dots, n$. Άρα $x_i^{k_i} \in I$, $k_i > 0$ $\forall i = 1, \dots, n$.

Έστω $m = k_1 + k_2 + \dots + k_n$.

Τότε $y^m = \left(\sum_{i=1}^n s_i f(x_i)\right)^m = \sum s_1^{r_1} s_2^{r_2} \cdots s_n^{r_n} \cdot f(x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n})$, όπου $r_1 + r_2 + \dots + r_n = m = k_1 + k_2 + \dots + k_n$.

Αν $r_i < k_i$ $\forall i = 1, \dots, n$, τότε $m = \sum_{i=1}^n r_i < \sum_{i=1}^n k_i = m$, άτοπο.

Άρα υπάρχει i με $r_i \geq k_i \Rightarrow x_i^{r_i} \in I \Rightarrow x_1^{r_1} \cdots x_n^{r_n} \in I$. Επομένως

$$y^m = \sum \underbrace{s_1^{r_1} \cdots s_n^{r_n}}_{\in S} f(\underbrace{x_1^{r_1} \cdots x_n^{r_n}}_{\in I}) \in I^e \Rightarrow$$

$\Rightarrow y \in \sqrt{I^e}$. Συμπέρασμα: $(\sqrt{I})^e \subseteq \sqrt{I^e}$

4) $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$

Έστω $J = (I_1 : I_2) \Rightarrow J I_2 \subseteq I_1 \Rightarrow$

$\Rightarrow (J I_2)^e \subseteq I_1^e \xRightarrow{3)} J^e I_2^e \subseteq I_1^e \Rightarrow$

$\Rightarrow J^e \subseteq (I_1^e : I_2^e)$.

Τα υπόλοιπα δείξτε τα μόνοι σας.

Μηδενοδιαιρέτες:

Ένα $x \in R$ λέγεται μηδενοδιαιρέτης (zero-divisor) $\iff$ υπάρχει $y \in R \setminus \{0\}$ με $xy = 0$.

Παρατήρηση: Ένας δακτύλιος χωρίς μηδενοδιαιρέτες είναι ακέραια περιοχή και αντιστρόφως.

Παρατήρηση: $x \in R$ μηδενοδιαιρέτης $\iff$
$\iff (0 : (x)) \neq \{0\}$, όπου $(0 : x) = (0 : (x))$, $(x) = Rx$, το ιδεώδες που παράγεται από το x.

Γενικότερα, έστω I ιδεώδες του R.
Ο μηδενιστής (annihilator) του I είναι το σύνολο των $x \in R$ με $xI = \{0\}$, δηλαδή το ιδεώδες $(0 : I)$. Συμβολίζουμε με $Ann(I) = (0 : I)$ τον μηδενιστή του I.

Τότε το σύνολο των μηδενοδιαιρετών του R είναι το $D = \bigcup_{x \neq 0} Ann(x)$ (y μηδενοδιαιρέτης $\Rightarrow xy = 0$ με $x \neq 0 \Rightarrow y \in Ann(x)$. Το αντίστροφο είναι προφανές.

<u>Ερώτηση:</u> Αν x, y θετικοί ακέραιοι και $x = \prod_{p \text{ πρώτος}} p^{\lambda_p}$, $\lambda_p \geq 0$ και με $y = \prod_{p \text{ πρώτος}} p^{\mu_p}$ με $\mu_p \geq 0$, ποιο είναι το ιδεώδες $((x):(y))$;

Έστω $z = \prod_{p \text{ πρώτος}} p^{\nu_p} \in ((x):(y))$.

Τότε $zy \in (x) \Leftrightarrow \prod_{p \text{ πρώτος}} p^{\nu_p + \mu_p}$ πολλαπλάσιο του $x = \prod_{p \text{ πρώτος}} p^{\lambda_p}$, δηλαδή $\nu_p + \mu_p \geq \lambda_p \Leftrightarrow$

$\Leftrightarrow \nu_p \geq \lambda_p - \mu_p$.

Άρα $\nu_p \geq \max\{\lambda_p - \mu_p, 0\} = \lambda_p - \min\{\lambda_p, \mu_p\}$

Απόδειξη της ισότητας: $\max\{\lambda_p - \mu_p, 0\} = \lambda_p - \min\{\lambda_p, \mu_p\}$

1) Αν $\lambda_p \geq \mu_p \Leftrightarrow \lambda_p - \mu_p \geq 0$, τότε $\max\{\lambda_p - \mu_p, 0\} = \underline{\lambda_p - \mu_p}$. Επίσης $\min\{\lambda_p, \mu_p\} = \mu_p \Rightarrow$
$\Rightarrow \lambda_p - \min\{\lambda_p, \mu_p\} = \underline{\lambda_p - \mu_p}$.

2) Αν $\lambda_p < \mu_p$, τότε $\lambda_p - \mu_p < 0 \Rightarrow \max\{\lambda_p - \mu_p, 0\} = 0$. και $\min\{\lambda_p, \mu_p\} = \lambda_p \Rightarrow \lambda_p - \min\{\lambda_p, \mu_p\} = \lambda_p - \lambda_p = 0$.

Ξέρουμε ότι $\mu\kappa\delta(x, y) = \prod_{p \text{ πρώτος}} p^{\min\{\lambda_p, \mu_p\}}$

Άρα $z = \prod_{p \text{ πρώτος}} p^{\nu_p}$ πολ/σιο του $\prod_{p \text{ πρώτος}} p^{\lambda_p - \min\{\lambda_p, \mu_p\}}$

$$= \frac{\prod_p p^{\lambda_p}}{\prod_p p^{\min\{\lambda_p, \mu_p\}}} = \frac{x}{\mu\kappa\delta(x, y)}$$

(8)

Επομένως $((x):(y)) = \left(\frac{x}{\text{μκδ}(x,y)}\right)$.

Π.χ. ~~(x)⊕(5)=3ℤ, y=5, x,y=15ℤ~~

~~((3):(5)) = $\left(\frac{3}{(3,5)}\right)$~~ =

$x=6,\ y=15$.

Τότε $((x):(y)) = (6\mathbb{Z} : 15\mathbb{Z}) = \left(\frac{6}{(6,15)}\right)\mathbb{Z} =$
$= \left(\frac{6}{3}\right)\mathbb{Z} = 2\mathbb{Z} = (2)$

Πρότυπα: (Modules) Έστω R δακτύλιος και M μια προσθετική αβελιανή ομάδα και ένας εξωτερικός πολλαπλασιασμός $\cdot : R\times M \to M / (r,x) \mapsto rx$ $\forall r\in R,\ x\in M$ με τις ακόλουθες ιδιότητες

α) $(rs)x = r(sx) = s(rx)$

β) $(r+s)x = rx+sx \quad \forall r,s\in R,\ x\in M$

γ) $r(x+y) = rx+ry \quad \forall r\in R,\ x,y\in M$.

δ) $1_R \cdot x = x \quad \forall x\in M$.

Παραδείγματα: Κάθε αβελιανή ομάδα είναι ένα $R=\mathbb{Z}$-πρότυπο και αντιστρόφως.

Εύκολα αποδεικνύεται: $0_R x = 0_M$. $(0_R x = (0_R+0_R)x =$
$= 0_R x + 0_R x \Rightarrow 0_R x = 0_R x - 0_R x = 0_M$.

$r 0_M = 0_M$ ανάλογα.

~~κ.ο.κ.~~ $-x = (-1_R)x$. $(x + (-1_R)x = 1_R x + (-1_R)x =$
$= (1_R + (-1_R))x = 0_R x = 0_M$.

$x - y = x + (-1_R)y$ κ.τ.λ., όπως στους διανυσματικούς χώρους

<u>Υποπρότυπα:</u> (Submodules).

Αν N είναι προσθετική υποομάδα ενός R-προτύπου M και $rx \in N$ $\forall r \in R$ και $x \in N$, τότε το N λέγεται R-υποπρότυπο του M.

π.χ. $\{0_M\}$ είναι πάντα υποπρότυπο του M.

Έστω R δακτύλιος. Τότε ο R με πράξη τον πολλαπλασιασμό του είναι ένα R-πρότυπο.
<u>Τα υποπρότυπα του R είναι ακριβώς τα ιδεώδη του.</u>

<u>Ομομορφισμοί R-προτύπων:</u> Έστω M και N δύο R-πρότυπα και $f: M \to N$ με τις ακόλουθες ιδιότητες:

1) $f(x+y) = f(x) + f(y)$ $\forall x, y \in M$

2) $f(rx) = r f(x)$ $\forall r \in R$ και $x \in M$.

Μια τέτοια απεικόνιση λέγεται ομομορφισμός των R-προτύπων M και N ή απλά R-ομομορφισμός.

1) Επιμορφισμός: f επί (onto)

2) Μονομορφισμός: f 1-1.

3) Ισομορφισμός: f 1-1 και επί.

<u>Πρόταση:</u> Ισχύουν τα εξής: Έστω $f: M \to N$ R-ομομορφισμός

α) Αν K υποπρότυπο του M ($K \leq M$) τότε και $f(K)$ υποπρότυπο του N. Ιδιαιτέρως $Imf = f(M) \leq N$.

β) Αν L υποπρότυπο του N, τότε και $f^{-1}(L)$ υποπρότυπο του M. Ιδιαιτέρως $Kerf = f^{-1}(\{0_M\}) \leq M$

<u>Απόδειξη:</u> Κάντε τη μόνοι σας. #

Αν $f: M \to N$ R-ισομορφισμός, τότε λέμε ότι τα M και N είναι R-ισόμορφα ή απλά ισόμορφα. Γράφουμε $M \underset{R}{\cong} N$ ή απλά $M \cong N$.