

Αλγεβρική Θεωρία Αριθμών 1^ο μάθημα 18/2/2024

Κίνητρο:

Στην Διοφαντική εξίσωση

$$f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$$

Πρόβλημα: να βρεθούν λύσεις $x_1, \dots, x_n \in \mathbb{Z}^n$

$$x^n + y^n = z^n$$

Να βρεθούν οι ακ. λύσεις

Παράδειγμα

$$y^3 = x^2 - 16$$

(Ελληνική
Καρτούν)

$$\underline{y^3 = (x-4)(x+4)}$$

$$d = (x-4, x+4)$$

Εστω

$$(x, y) \in \mathbb{Z} \times \mathbb{Z}$$

η λύση αυτή της
εξίσωσης

$$d \mid x-4$$

$$d \mid x+4$$

$$d \mid 8$$

$$\underline{d=1}$$

Αν x είναι περιττός τότε

Θεώρημα μονογονικότητας ανάλογος σε πρώτους.

$$a, b, c \in \mathbb{N} \setminus \{0\}$$

$$a^n = bc$$

$$(b, c) = 1$$

$$\alpha_1^n = b$$

$$c = \alpha_2^n$$

όλοι οι
πρώτοι

παράγοντες του

εμφανίζονται

ως πρώτοι παράγοντες

του a^n άρα εμφανίζονται
σε n -στές δυνάμεις.

$$x-4 = a^3$$

$$x+4 = b^3$$

$$(a, b) = 1$$

$$b^3 - a^3 = 8$$

$$(b-a)\pi = 8$$

a, b είναι

ακ. οπότε

αυτή η εξίσωση είναι αδύνατη.

Av $0 \neq x$ είναι άρτιος

$$8 \mid x^2$$

$$y^3 = \frac{x^2 - 16}{8}$$

x άρτιος $\Rightarrow$
 y άρτιος
 $2 \mid y$.

$$4 \mid x$$

$$x = 4x_1$$

$$16x_1^2 - 16 = (4y_1)^3$$

$\Downarrow$

$$x_1^2 = 4y_1^3 + 1 \leadsto x_1 \text{ περιττός}$$

$$x_1 = 2m+1 \quad m \in \mathbb{Z}$$

$$m^2 + m = y_1^3$$

$$m(m+1) = y_1^3$$

$$m(m+1) = 1$$

είναι δύο διαδοχικοί
 αββοι

αλλά οι μοναδιαίοι διαδοχικοί
 αββοι

$$\{-1, 0, 1\}$$

$$\Rightarrow m=0 \vee m+1=0$$

$$y_1=0 \Rightarrow y_1=0$$

$$\text{Μοναδιαίοι λύσεις} \\ (x, y) = (\pm 4, 0)$$

Παράδειγμα

$$y^3 = x^2 + 1$$

$$y^3 = (x+i)(x-i)$$

$$\text{Υποθέτουμε} \\ (x, y) \in \mathbb{Z} \times \mathbb{Z} \\ (\text{λύση})$$

$$\sqrt{\mathbb{Z}[i]}$$

$$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$$

$$N(a+bi) = a^2 + b^2 = (a+bi)(a-bi) = \|a+bi\|^2$$

$$\Sigma(\mathbb{Z}[i]) = \text{ομάδα των μονικών} = \{\pm 1, \pm i\}$$

R αντιμεταθετικός δακτύλιος με μονάδα.
ακ. περιοχή

$R - \{0\}$ δεν είναι ομάδα (κατ' ανάγκη)

$E(R) = \{u \text{ ομάδα των πο/ων αντιστρέφ.}\}$

$$E(\mathbb{Z}) = \pm 1$$

$$E(\mathbb{Z}[i]) = ?$$

Ψάχνουμε να βρούμε

$$xy = 1$$

$\mathbb{Z}[i] \Rightarrow x$ ώστε να υπάρχει

$$y \in \mathbb{Z}[i]$$

$$N: \mathbb{Z}[i] \rightarrow \mathbb{Z}$$

$$N(x)N(y) = N(xy) = N(1) = 1$$

$$x \in E(\mathbb{Z}[i]) \Leftrightarrow N(x) = \pm 1$$

$$x = a + ib$$

$$N(x) = a^2 + b^2 = \pm 1$$

$$a^2 + b^2 = 1$$

$$a = \pm 1 \quad b = 0$$

$$a = 0 \quad b = \pm 1$$

$$\text{Αν } a \geq 2 \quad \text{ή } b \geq 2 \quad a^2 + b^2 \geq 4$$

$$E(\mathbb{Z}[i]) = \{ \pm 1, \pm i \}$$

$$y^3 = (x+i)(x-i)$$

$$2 = (-i)(1+i)^2$$

$$\pi = 1+i \quad \text{ανάγωγο στοιχείο.}$$

Στο $\mathbb{Z}$ έχουμε ορισμό των έννοια του πρώτου

Ορίσμος R ακεραία περιοχή

$$(a \cdot b = 0 \Rightarrow a = 0 \text{ ή } b = 0)$$

Ενα $a \in R, a \neq 0$ θα λέγεται

ανάγωγο :

$$\text{Αν } a = b \cdot c \quad b, c \in R \Rightarrow b \in E(R) \text{ ή } c \in E(R)$$

-7 στο $\mathbb{Z}$ είναι ανάγωγο

$$-7 = \underbrace{(-1)}_{\text{μονάδα}} \cdot 7$$

$7 \in \mathbb{Z}$ είναι ανάγωγο

$$7 = (-1)(-7) \\ \text{μονάδα.}$$

$p \in \mathbb{R}, p \neq 0, p \in E(R)$ θα λέγεται "πρώτο"

$$p \mid \alpha \beta, \alpha, \beta \in R \Rightarrow p \mid \alpha \text{ ή } p \mid \beta$$

Παράδειγμα

$\mathbb{Z}$ (οι έννοιες πρώτου και ανάγωγου ταυτίζονται)

• $\checkmark 2 \in \mathbb{Z}[\sqrt{-5}]$ είναι ανάγωγο

• $\checkmark 7 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ δεν είναι ανάγωγο

$$7 + \sqrt{-5} = \underbrace{(1 + \sqrt{-5})} \underbrace{(2 - \sqrt{-5})}$$

$$\mathbb{Z}[\sqrt{-5}] = \{ \alpha + \beta\sqrt{-5} : \alpha, \beta \in \mathbb{Z} \}$$

$$N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}$$

$$(\alpha + \beta\sqrt{-5}) \longrightarrow (\alpha + \beta\sqrt{-5})(\alpha - \beta\sqrt{-5}) \\ = \alpha^2 + 5\beta^2$$

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

$$E(\mathbb{Z}[\sqrt{-5}]) = \{ x \in \mathbb{Z}[\sqrt{-5}] : N(x) = \pm 1 \}$$

$$\alpha^2 + 5\beta^2 = \pm 1$$

$$\alpha^2 + 5\beta^2 = 1$$

$$\Rightarrow \alpha^2 = 1 \quad \underline{\alpha = \pm 1}$$

2 είναι ανάγωγο, το 2 δεν είναι πρώτο στο $\mathbb{Z}[\sqrt{-5}]$

$$2 \mid 6 = (1+5) = (1-\sqrt{-5})(1+\sqrt{-5}) = (1+\sqrt{-5})^2$$

$$2 \nmid 1 \pm \sqrt{-5}$$

Ευκλείδεια περιοχή

R κκ. περιοχή

$$\phi : R \rightarrow \mathbb{Z}$$

θα λέγεται ευκλείδεια

για κάθε $a, b \in R, b \neq 0$ $\phi(ab) \geq \phi(a)$

$a, b \in R, b \neq 0$ υπάρχουν $\pi, \upsilon \in R$

$$a = b\pi + \upsilon \quad \phi(\upsilon) < \phi(b)$$

(R, ϕ) όπου ϕ ευκλείδεια συνάρτηση λέγεται ευκλείδεια περιοχή.

$$(\mathbb{Z}[i], \phi)$$

$$\phi(a+ib) = a^2 + b^2$$

$$(\mathbb{Z}[\sqrt{2}], \phi)$$

$$\phi(a+b\sqrt{2}) = a^2 + 2b^2$$

$$(\mathbb{K}[x], \phi)$$

$\mathbb{K}$ σώμα

$$\phi(f(x)) = \begin{cases} \deg f & \text{αν } f(x) \neq 0 \\ -1 & \text{αν } f(x) = 0 \end{cases}$$

είναι ευκλείδεια περιοχή.

Αριθμός όπως υπάρχει στο $\mathbb{Z}$,

ευκλείδεια δαυτότος ανάγωγο $\Leftrightarrow$ πρώτο.

$$p \mid a \vee b \Rightarrow p \mid a \wedge p \mid b$$

$$y^3 = (x+i)(x-i) \quad - \quad d = (x+i, x-i)$$

$$d \mid 2$$

$$d \mid x+i$$

$$d \mid x-i$$

$$\text{λοχαφίζουμε } d \approx 1$$

$$d \mid 2i$$

$d \cong 1 \iff a = b \cdot u$ μονάδα
 Αποδ του ιδιοτιμου μονάδα
 Αν $d \neq 1$ $d \cong 2 = (1+i)^2 \cdot i$
 $1+i \mid d$

$$\begin{aligned}
 1+i \mid (x+i) \\
 N(1+i) \mid N(x+i) \\
 2 \mid x^2+1 = y^3 \\
 2 \mid y \Rightarrow 2^3 \mid y^3
 \end{aligned}$$

$$\begin{aligned}
 \Rightarrow 8 \mid x^2+1 &\Rightarrow \\
 x^2 &\equiv -1 \pmod{8} \\
 &\text{απο το } 0
 \end{aligned}$$

$$0, 1, 2, 3, 4, 5, 6, 7, 8 \\
 \pm \pm 2 \pm 3$$

$$d \cong 1 \quad d = (x+i, x-i) \quad (x+i)(x-i) = y^3$$

Μονοίριστη ανάλυση

$$\begin{aligned}
 \mathbb{E}(\mathbb{Z}[i]) &= \langle i \rangle \\
 &\text{μονάδα} \\
 &\text{ταξινό 4} \\
 i, i^2 &= -1, \\
 i^3 &= -i, i^4 = 1
 \end{aligned}$$

$$\mathbb{E}(\mathbb{Z}[i]) \ni \varepsilon \rightarrow \varepsilon^3 \in \mathbb{E}(\mathbb{Z}[i])$$

$$\begin{aligned}
 &\text{είναι αυτομορφισμός} \\
 &\text{της ομάδας} \\
 (3, 4) &= 1
 \end{aligned}$$

$$\begin{aligned}
 \varepsilon &= \varepsilon^3 \\
 x+i &= \eta^3
 \end{aligned}$$

ενσωματώνουμε την μονάδα στο η .

$$\eta = \alpha + i\beta \in \mathbb{Z}[i]$$

$$x + i = (\alpha + i\beta)^3 = (\alpha^3 - 3\alpha\beta^2) + i(3\alpha^2\beta - \beta^3)$$

$$1 = \beta(3\alpha^2 - \beta^2) \Rightarrow \beta | 1 \quad \beta = \pm 1$$

$$3\alpha^2 - 1 = \pm 1 \leadsto \alpha = 0$$

$$x = \alpha^3 - 3\alpha\beta^2 = 0 \Rightarrow y = 1$$

$$(x, y) = (0, 1)$$

$\mathbb{Z}[i]$ ευκλείδειος δαυτός $\leadsto$ κανέρι με το $\mathbb{Z}$
 $E(\mathbb{Z}[i]) = \langle i \rangle$

Παράδειγμα

$$\begin{aligned} 2y^3 &= x^2 + 5 & \mathbb{Z}[\sqrt{-5}] \\ &= (x + \sqrt{-5})(x - \sqrt{-5}) \end{aligned}$$

$$E(\mathbb{Z}[\sqrt{-5}]) = \pm 1$$

2 είναι ανάγωγο στοιχείο το $\mathbb{Z}[\sqrt{-5}]$

$$2 = xy$$

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

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

$$N(x) = \pm 2$$

$$N(y) = \pm 2$$

Λάθος το 2 είναι ανάγωγο αλλά όχι πρώτο (βλ. αβ $\Rightarrow$ p | αβ $\Rightarrow$ p | α ή p | β)
 Δεν διασπάζεται σε γινόμενο που στοιχεία που δεν είναι μονάδες

$$x = k + j\sqrt{-5} \quad k, j \in \mathbb{Z}$$

$$\downarrow$$

$$k^2 + 5j^2 \neq \pm 2$$

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$$

" $\Rightarrow$ "

$$2 | (x + \sqrt{-5}) \quad \vee \quad 2 | (x - \sqrt{-5})$$

$$\frac{x + \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2}\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

$$\frac{x - \sqrt{-5}}{2} = \frac{x}{2} + \frac{1}{2} \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

αποκο $\frac{1}{2} \notin \mathbb{Z}$.

απο η Δ.Ε $2y^3 = x^2 + 5$ δεν έχει
ακεραία λύση

$(x, y) = (\pm 7, 3)$ είναι λύση της Δ.Ε.

Fermat

$$x^p + y^p = z^p$$

p πρώτος

$$z^p - 1 \quad \text{ρίζες της } \zeta_p^i$$

$$(z^p - 1) = (z - 1)(z - \zeta_p)(z - \zeta_p^2) \dots (z - \zeta_p^{p-1})$$

$p=2$
διαφορές
τετραγώνων

"διαφορές τετραγώνων"

$$z = -x/y$$

ζ_p

είναι p -ελάχιστη
πρωταρχική
ρ-ρίζα του 1

$$\zeta_p = e^{2\pi i/p}$$

$$z^p = x^p + y^p = \prod_{v=0}^{p-1} (x + \zeta_p^v y)$$

Kummer (1837)

$\mathbb{Z}[\zeta_p]$

είναι
περιοχή
μονομερούς
ανάλυσης

$\Downarrow$ απεικόνιση
του Fermat

αναγωγο = πρώτο

Dirichlet:

η απεικόνιση του Kummer
είναι λεία

το $\mathbb{Z}[\zeta_p]$ δεν είναι κατ.
αναγωγο
περιοχή

$$p < 100$$

$$p = 37, 59, 67$$

1880 ← ο οποίος ^{προσέδει} ^{επιβεβαίωσε} του Fermat
 Βασιζόμενος στην
 ερμηνεία των ιδεών του
 Kummer

1886 G. Frobenius συνέδεσε την θεωρία του Fermat
 με την θεωρία των ελλειπτικών
 καμπυλών.
 ~~~~~> Wiles 1995.

Τότε υπάρχει μονοσήμαντη ανάλυση και τι κάνουμε  
 αν δεν υπάρχει;

Dedekind: ~~~~~> στο συνδυασμό υπάρχει "μονοσήμαντη  
 ανάλυση στα ιδεώδη"

Στοιχειώδη θεωρία αριθμών  $\mathbb{Z}$   $\mathbb{Q} = \text{Quot}(\mathbb{Z})$

αλγεβρική επέκταση  $\mathbb{Q}(\theta)$   $\theta$  είναι αλγεβρικός  
 αριθμός, ικανοποιεί  $\theta = i$   
 $x^2 + 1 = 0$   
 $x^2 + 5 = 0$

$\mathbb{Q} \xrightarrow{R_\theta} \mathbb{Q}(\theta)$   
 θα ορίσουμε ένα  
 δακτύλιο που θα  
 παίρνει τον ρόλο του  $\mathbb{Z}$  στην ανάλυση  
 στο μεγαλύτερο  
 σώμα  $\mathbb{Q}(\theta)$ .  
 μια πολυωνυμική  
 εξίσωση με  
 από το  $\mathbb{Q}$

Ορισμός. ο  $\alpha$  θα λέγεται ακέραιος αλγεβρικός  
 αν και μόνο αν ικανοποιεί ένα μονομύο  
 πολυώνυμο με συντελεστές από το  $\mathbb{Z}$

$$f(x) = x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_1x + \alpha_0$$

1 μονομύο πολυώνυμο  $\mathbb{Z}$

Κάθε αλγεβρικός (οχι ακεραίος!) ικανοποιεί ένα μονικό πολυώνυμο με συντελεστές από το  $\mathbb{Q}$ .

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \quad \underline{a_n \neq 0}$$

$$f(x) = \textcircled{3} x^2 + 5x + 6$$

$$x^2 + \frac{5}{3}x + \frac{6}{3}$$

Παραγ.  $\alpha \in \mathbb{Q}$  αυτός είναι ακ. αλγεβρικός αν και μόνο αν  $\alpha \in \mathbb{Z}$

$$\alpha \in \mathbb{Q} : \alpha = \frac{n}{m} \quad n, m \in \mathbb{Z}$$

$$\alpha - \frac{n}{m} = 0 \Rightarrow m\alpha - n = 0 \quad m \neq 0$$

$$\alpha \text{ ικανοποιεί το } m\alpha - n = 0 \in \mathbb{Z}[x]$$

$$f(x) = \underline{x}^n + a_{n-1} x^{n-1} + \dots + \underline{a_0} \in \mathbb{Z}[x]$$

$$\alpha = \frac{\kappa}{\lambda} \in \mathbb{Q}. \Rightarrow \kappa \mid a_0$$

$$\lambda \mid 1$$

$\frac{\kappa}{\lambda}$  αναγωγή  $(\kappa, \lambda) = 1$

$$\left(\frac{\kappa}{\lambda}\right)^n + a_{n-1} \left(\frac{\kappa}{\lambda}\right)^{n-1} + \dots + a_0 = 0$$

$$\kappa^n + a_{n-1} \kappa^{n-1} \lambda + \dots + a_0 \lambda^n = 0$$

$$\Rightarrow \lambda \mid \kappa^n \Rightarrow \lambda \mid 1$$

$$\lambda = \pm 1.$$

---

Οι ακ. αλγεβρικοί αποτελούν δακτύλιο

$x$  ακ. αλγεβρικός  $y$  ακ. αλγεβρικός

$x+y$  είναι ακ. αλγ.  $x \cdot y$  είναι ακ. αλγεβρικός

Γνωρίζουμε ότι το ελάχιστο πολυώνυμο του  $x$  είναι  
μονικό  $\mathbb{Z}[x]$   
 $y$



πως θα υπολογίσουμε το ελάχιστο  
του  $x+y$  από τα ελάχιστα των  $x, y$

μονο στο  $\mathbb{Z}[x]$

Πρόταση  $\alpha \in \mathbb{C}$  είναι αλγεβρικός αν και  
μόνο αν η προσεταιριστική οργάνωση ( $\mathbb{Z}$ -module)  
που παράγεται από τις δυνάμεις του  $\alpha$   
 $1, \alpha, \alpha^2, \dots$  είναι πεπερασμένη  
παραγωγή.

Απόδ. Εστω  $\alpha$  αλγεβρικός, δηλαδή ικανοποιεί  
μία εξίσωση της μορφής

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

$$F[\alpha] \quad f \in \mathbb{Q}[x]$$

$$F(x) = \pi(x) f(x) + u(x) \quad \begin{matrix} \nearrow u=0 \\ \searrow \deg u < n \end{matrix}$$

$\mathbb{Z}[x]$

$$F(\alpha) = u(\alpha)$$

και ερμουν

οι δυνάμεις  $1, \alpha, \dots, \alpha^{n-1}$   
για να παρουν  
την οριζοντι.

$$\alpha^n = -(\alpha_{n-1} \alpha^{n-1} + \dots + \alpha + a_0)$$

$$\textcircled{3} \alpha^n = \underline{\hspace{2cm}}$$

$\mathbb{Z}$ -module.

Αντίστροφο αν υποθέσουμε  $z_1, \dots, z_n$  παράγουν  
την  $\mathbb{Z}[\alpha]$  για καθε  $1 \leq i \leq n-1$  υπάρχει

$$\lambda_{ij} \in \mathbb{Z}$$

$$\alpha z_i = \sum_{j=0}^{n-1} \lambda_{j,i} \alpha^j z_j$$

$$(\alpha I_n - (\lambda_{i,j})) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0 \quad \begin{matrix} \text{έχει των} \\ (x_1, \dots, x_n)^t \neq 0 \end{matrix}$$

$$\Rightarrow \det(\alpha I_n - (\lambda_{i,j})) = 0$$



$$x^n + b_1 x^{n-1} + \dots + b_1 x + b_0 = 0$$

μονιμ εφ' όλης ρε  
συνέπειες στο  $\mathbb{Z}$ .

Το σύνολο  $R$  των ακ. αλγεβρικών είναι  
δακτυλίδιο

$\alpha$  ανήκει σε μια πεπ. παράχ. προδότημοφκδα  
 $\theta$

$$\alpha + \theta$$

$$\alpha \cdot \theta$$

είναι

ακ. φράσσειν σκεδισκ φων

- α' β' γα σποια σποια

ανήκων σε μια πεπ.

παράχρσιν προδότημσ φκδα