

2ο Μάθημα 23/2/2024

$K \leftarrow$ πεπερασμένη επέκταση του $\mathbb{Q}$ είναι απλή
 (γιατί το $\mathbb{Q}$ έχει
 χαρακτηριστικό 0
 άρα όλες οι
 επεκτάσεις του
 είναι διαχωρίσιμες)

Απλή $K = \mathbb{Q}(\vartheta)$ ϑ είναι
 ένας αλγεβρικός
 αριθμός

$K \leftarrow \mathbb{Q}_K \leftarrow$ δακτύλιος των ακ. αλγεβρικών αριθμών
 αποτελ. από τα $x \in K$
 το x ικανοποιεί ένα μονίμο πολώνυμο
 με συντελεστές από το $\mathbb{Z}$.

Το ϑ μπορεί να επιλεγεί να είναι ακ. αλγεβρικός
 $\vartheta \in K$, $\vartheta \in \mathbb{Q}_K$

το ϑ ικανοποιεί ένα πολ. $f(x) \in \mathbb{Q}[x]$
 $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Q}[x]$ $a_i \in \mathbb{Q}$

$f(\vartheta) = 0$. Υπάρχει ένα $m \in \mathbb{Z}$ ώστε

$$\underline{m a_i \in \mathbb{Z}}. \quad f(\vartheta) = 0 \xrightarrow{m^n} \underline{(m\vartheta)^n + m a_{n-1} (m\vartheta)^{n-1} + \dots + m^{n-1} a_1 (m\vartheta) + m^n a_0 = 0}$$

οπότε ο $\underline{m\vartheta}$ ικανοποιεί ένα μονίμο πολώνυμο
 με συντελεστές στο $\mathbb{Z}$

$$\sum_{i=0}^n x^i a_i m^{n-i} = f(x)$$

Γενική θεωρία των αλγεβρικών αριθμών

Τετραγωνικά σώματα αριθμών επέκτασης βαθμού 2.

$$K = \mathbb{Q}(\vartheta)$$

~ 1

$$\mathbb{Q} \mid \mathbb{Q}$$

$$\text{Irr}(\vartheta, \mathbb{Q}) = X^2 - \alpha X - \beta \quad \text{αναγωγή πολυωνόμο}$$

$$\alpha = 0 \quad \vartheta^* = \vartheta - \frac{\alpha}{2} \quad \text{το οποίο ικανοποιεί}$$

$$\mathbb{Q}(\vartheta) = \mathbb{Q}(\vartheta^*) \quad \downarrow \text{είναι ρίζα του}$$

$$X^2 - b' \quad b' = \frac{\alpha^2}{4} + \beta.$$

$$\circ \quad b' \text{ δεν είναι τετράγωνο, γιατί } \mathbb{Q}(\vartheta) = \mathbb{Q}.$$

$$b' = 8 = 2^2 \cdot 2 \quad \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$$

$$b' = m r^2, \quad r \in \mathbb{Q}$$

$$\mathbb{Q}(\sqrt{b'}) = \mathbb{Q}(\sqrt{m})$$

$$\text{Κάθε τετραγωνικό σωμά αριθμού } \mathbb{Q}(\sqrt{m})$$

$$m \neq 1, \quad \square \nmid m$$

m ελεύθερο τετραγώνου square free.

$$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}[\sqrt{m}] \quad \frac{3+\sqrt{m}}{5+\sqrt{m}}$$

↑ πολυωνύμιας ειφφράσις

Οποιαδήποτε πολυωνύμια, μη μηδενικά ειφφράσις του $\sqrt{m}$ είναι αντιστρέψιμα.

$$g(x) \quad \text{ώστε} \quad g(\sqrt{m}) \neq 0$$

$$f(x) = \text{Irr}(\sqrt{m}, x) = x^2 - m$$

$$f(x) \nmid g(x) \Rightarrow$$

$$(f(x), g(x)) = 1$$

$$\alpha(x)f(x) + \beta(x)g(x) = 1$$

$$\frac{a(\sqrt{m})}{g(\sqrt{m})} \frac{b(\sqrt{m})}{\theta(\sqrt{m})} = a(\sqrt{m}) \theta(\sqrt{m}) \quad \underline{a, b \in \mathbb{Q}[x]}$$

$$\mathbb{Q}(\partial) = \mathbb{Q}[\partial]$$

$$K = \mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m}, a, b \in \mathbb{Q}\}$$

$$g(\sqrt{m})$$

$$g(x) \in \mathbb{Q}[x]$$

$$g(x) = \pi(x) \underbrace{(x^2 - m)} + v(x)$$

$$\deg v(x) \leq 2$$

$$g(\sqrt{m}) = \pi(\sqrt{m}) \odot + \frac{v(\sqrt{m})}{\alpha_0 + \alpha_1 \sqrt{m}} \quad \alpha_0, \alpha_1 \in \mathbb{Q}.$$

$$\text{Gal}(K/\mathbb{Q}) = \{1, \sigma\} \quad \text{Gal}(K/\mathbb{Q}) = \left\{ \sigma: K \rightarrow K \right. \\ \left. \sigma|_{\mathbb{Q}} = \text{Id}_{\mathbb{Q}} \right\}$$

$$z \in \text{Gal}(K/\mathbb{Q}) : z(\sqrt{m}) \text{ σε μια ρίζα του ελαχιστου πολυνομου}$$

$$z(\sqrt{m}) = \begin{cases} \sqrt{m} & z = 1 \\ -\sqrt{m} & z = \sigma \end{cases}$$

$$z(\alpha_0 + \alpha_1 \sqrt{m}) = z(\alpha_0) + z(\alpha_1) z(\sqrt{m}) \\ = \alpha_0 + \alpha_1 (\pm \sqrt{m})$$

$$\alpha = a + b\sqrt{m}$$

$$S_K(\alpha) = \alpha + \sigma(\alpha) \in \mathbb{Q}$$

γιατι εινα Gal(K/Q) ανατομο

$$= \sum_{z \in \text{Gal}(K/\mathbb{Q})} z(\alpha)$$

$$N_K(\alpha) = \prod_{z \in \text{Gal}(K/\mathbb{Q})} z(\alpha) = \alpha \cdot \sigma(\alpha)$$

$$\alpha = a + b\sqrt{m} \\ \sigma(\alpha) = a - b\sqrt{m}$$

$$S_K(\alpha) = \underline{2a} \\ N_K(\alpha) = a^2 - mb^2$$

$$\text{Irr}(\alpha, x) = (x - \alpha)(x - \sigma(\alpha)) = x^2 - S(\alpha)x + N(\alpha)$$

0 α είναι ακ. αλγεβρικός αν και μόνο $S_K(\alpha) \in \mathbb{Z}$
 $N_K(\alpha) \in \mathbb{Z}$.

Πάρε να λογαριάζουμε όλους τους ακ. αλγεβρικούς

$\mathbb{Z}[\sqrt{m}]$ είναι ακ. αλγεβρικοί. $x-a$
 $a \in \mathbb{Z}$

Υπάρχουν και άλλα στοιχεία

$$\alpha = a + b\sqrt{m} \quad 2a = \gamma \quad 2b = \delta$$

$$S(\alpha) \in \mathbb{Z} \Leftrightarrow \gamma = \frac{\alpha}{2} \in \mathbb{Z}.$$

$$\mathbb{Z} \ni N(\alpha) = a^2 - mb^2 = \frac{\gamma^2}{4} - m \frac{\delta^2}{4} = \frac{\gamma^2 - m\delta^2}{4} \in \mathbb{Z}$$

$$\gamma^2 \equiv m\delta^2 \pmod{4} \quad \text{ισοσύνη και αναγκαία συνθήκη}$$

$$\alpha \in \mathcal{O}_K$$

Τα τετράγωνα $\pmod{4}$
 είναι 0, 1

$$\begin{array}{c} 0, 1, 2, 3 \\ \hline 0, 1, 0, 1 \end{array}$$

$$m \equiv 2, 3 \pmod{4}$$

για να έχει λύση

$$\gamma^2 \equiv m\delta^2 \pmod{4} \Rightarrow \gamma = \delta \equiv 0 \pmod{2}$$

$$m \equiv 1 \pmod{4}$$

η ισοδυναμία έχει λύση

$$\Rightarrow a, b \in \mathbb{Z}$$

$$\gamma \equiv \delta \pmod{2}$$

$$\frac{\gamma - \delta}{2} \in \mathbb{Z}$$

$$\alpha = a + b\sqrt{m} = \frac{\gamma - \delta}{2} + \delta \frac{1 + \sqrt{m}}{2}$$

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] & m \equiv 1 \pmod{4}. \end{cases}$$

$$K = \mathbb{Q}[\theta]$$

$$\mathbb{Q}(\sqrt{m})$$

$$\mathcal{O}_K \supseteq \mathbb{Z}[\theta]$$

αλλά ο επιλεγμένος μπορεί να είναι γενήσιος

Οφάδα των μονάδων:

$$\varepsilon \in \mathcal{O}_K \quad \text{είναι μονάδα} \iff \varepsilon \varepsilon' = 1 \quad \text{σπκρχει}$$

$$\varepsilon \in E(\mathcal{O}_K) \iff N(\varepsilon) = \pm 1$$

$$\text{Αν } \varepsilon \cdot \varepsilon' = 1 \Rightarrow N(\varepsilon) N(\varepsilon') = 1 \in \mathbb{Z}$$

$$N(\varepsilon) = \pm 1$$

$$\begin{aligned} N(\varepsilon) &= \varepsilon \sigma(\varepsilon) = 1 & \varepsilon' &= \sigma(\varepsilon) \\ \varepsilon \cdot \sigma(\varepsilon) &= -1 & \varepsilon' &= -\sigma(\varepsilon). \end{aligned}$$

$$\omega_m = \begin{cases} \sqrt{m} & m \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{m}}{2} & m \equiv 1 \pmod{4} \end{cases}$$

$$\varepsilon = a + b\omega_m \quad \text{είναι μονάδα αν και μόνο αν.}$$

$$a^2 - b^2 m = \pm 1 \quad m \equiv 2, 3 \pmod{4}$$

$$a^2 + ab + \frac{1-m}{4} b^2 = \pm 1 \quad m \equiv 1 \pmod{4}$$

1 περίπτωση $m < 0$

$$m \equiv 2, 3 \pmod{4}$$

Μιγαδικά τετραγωνικά άρρητα αριθμοί

$$a^2 + b^2 m > 0$$

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

$$|m| > 1 \quad \text{τότε } b = 0 \quad a = \pm 1 \Rightarrow \varepsilon = \pm 1$$

$$m = -1$$

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

$$\varepsilon = \pm 1, \pm i$$

$$m \equiv 1 \pmod{4}$$

$$a^2 + ab + \frac{1-m}{4} b^2 = \left(a + \frac{b}{2}\right)^2 + \frac{|m|}{4} b^2 \geq 0$$

$$|m| > 4 \Rightarrow b = 0 \quad \varepsilon = \pm 1$$

$$|m| \leq 4$$

$$m \equiv 1 \pmod{4}$$

$$m = -3$$

$$\left(a + \frac{b}{2}\right)^2 + \frac{3}{4} b^2 = 1$$

$|b| \geq 2$ δεν έχει λύση

$b=1 \quad \alpha^2 + \alpha + 1 = 1 \quad \alpha=0, \alpha=1$

$$\left\{ \pm 1, \frac{1 \pm \sqrt{3}}{2}, \frac{-1 \pm \sqrt{3}}{2} \right\}$$

$m < 0$

$m > 0$

Πραγματικά σύρματα αριθμών $\mathbb{Q}(\sqrt{3})$

$\cap \mathbb{R}$

Η ομάδα των μονάδων είναι άπειρη

$$X^2 - mY^2 = 1$$

Διοφαντίνη επίλυση
ή επίλυση του
Pell

Θεωρία μονάδων του Dirichlet

$$E(\mathcal{O}_K) = \{ \pm \varepsilon_0^n : n \in \mathbb{Z} \}$$

θεμελιώδης μονάδα

$$\pm = N(\alpha) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\alpha) = \prod_{\sigma \in \text{Hom}(\dots)} \sigma(\alpha)$$

L/K

L, K είναι αλγεβρικά σωρικά αριθμών
($K = \mathbb{Q}$)

$n = [L:K] < \infty$

$L = K(\vartheta), \vartheta \in \mathcal{O}_L$

$\text{Irr}(\vartheta, K)(x) = \text{έχει απλές ρίζες}$

$\mathbb{Q}, K, L$ είναι

χαρτηρισμένη
0 και 1
οι επεκτάσεις
είναι διαχωριστές

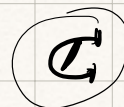
Εμφάνιση του $L \rightarrow \text{στο } \overline{K}$

$\sigma(\alpha) = \alpha \text{ για κάθε } \alpha \in K$

$L \rightarrow \mathbb{Q}$

αλγεβρική
υπόσυνταξη
του κάτω
σωμάτος

αλγεβρική
υπόσυνταξη
του $\mathbb{Q}$.



↓
είναι ένας μονομορφισμός σωμάτων.
 $\sigma: L \rightarrow \bar{K}$

Παρατήρηση

$$f: L \rightarrow M$$

L, M σώματα
είναι ή μη δένιου
ή μονομορφισμός

$$\ker f \triangleleft L$$

$$\ker f = \{0\} \quad \ker f = L$$

$$\alpha \in L \quad \alpha = \alpha_0 + \alpha_1 \partial + \dots + \alpha_{n-1} \partial^{n-1} \quad \alpha_i \in K$$

$$\sigma(\alpha) = \alpha_0 + \alpha_1 \sigma(\partial) + \dots + \alpha_{n-1} \sigma(\partial^{n-1}) \quad L = K[\partial]$$

$$\sigma|_K = \text{id}$$

$$\sigma(1+1) = \sigma(1) + \sigma(1) = 2\sigma(1)$$

$$\sigma|_K = \text{id}$$

$$\sigma(1) = 1$$

$$\sigma(1\alpha) = \sigma(\alpha)$$

$$\sigma(1)\sigma(\alpha) = \sigma(\alpha)$$

$$(\sigma(1)-1)\sigma(\alpha) = 0$$

Γνωρίζουμε τον σ αν
γνωρίζουμε το $\sigma(\partial)$
και το $\sigma(\partial)$ ριζά του
αντικειμένου
πολυωνύμου

$$f(x) = \text{Irr}(\partial, K)(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$$

$\alpha_i \in K$

$$0 = f(\partial)$$

$$0 = \sigma(0) = \sigma f(\partial) = \sum_{v=0}^n \sigma(\alpha_v \partial^v) = \sum_{v=0}^n \sigma(\alpha_v) \sigma(\partial)^v$$

$$= \sum_{v=0}^n \alpha_v (\sigma(\partial))^v$$

$$\Rightarrow f(\sigma(\partial)) = 0.$$

$$f(x) = \text{Irr}(\partial, K) = \prod_{i=1}^n (x - \partial^{(i)})$$

$$\partial^{(n)} = \partial$$

Έχουμε αριθμούς η το πλῆθος εμφυτεύσεων στο $\bar{K}$

$\mathbb{Q}(\sqrt{m})$ έχει δύο εμφυτεύσεις στο $\bar{\mathbb{Q}}$ του L/K

$\mathbb{Q}$

$$\text{Id: } \sqrt{m} \mapsto \sqrt{m}$$

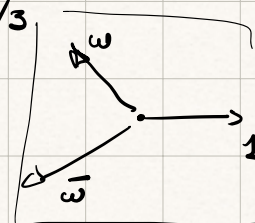
$$\sigma: \sqrt{m} \mapsto -\sqrt{m}$$

$$\mathbb{Q}(\sqrt[3]{2})$$

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega \sqrt[3]{2})(x - \bar{\omega} \sqrt[3]{2})$$

$\omega = \text{κύβητος ρίζα της μονάδας}$

$$\mathbb{Q}(\sqrt[3]{2}) \begin{cases} \xrightarrow{\text{πραγματική εμφύτευση}} \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R} \\ \xrightarrow{\text{2 μιγαδικές εμφυτεύσεις}} \mathbb{Q}(\omega \sqrt[3]{2}) \not\subset \mathbb{R} \\ \xrightarrow{\text{2 μιγαδικές εμφυτεύσεις}} \mathbb{Q}(\bar{\omega} \sqrt[3]{2}) \not\subset \mathbb{R} \end{cases}$$



$$\eta = 2 \text{ μιγαδ.} + \text{πραγματικές}$$

Θεώρημα μονάδων του Dirichlet

$$\eta = r_1 + 2r_2$$

αν r_1 το πλῆθος των πραγματικών εμφ.
 r_2 το πλῆθος των μιγαδικών εμφ.

υπάρχουν $\varepsilon_1, \dots, \varepsilon_r$
θεμελιώδεις μονάδες

$$r = r_1 + r_2 - 1$$

$$E(\mathcal{O}_K) = \left\{ \varepsilon = \varepsilon_1^{s_1} \varepsilon_2^{s_2} \dots \varepsilon_r^{s_r} \mid s_i \in \mathbb{Z} \right\}$$

$$\mathbb{Q}(\sqrt{m}) \quad m < 0$$

$$\begin{aligned} r_1 &= 0 \\ r_2 &= 1 \end{aligned}$$

δεν υπάρχει $\mathbb{Z}$ -μορφή

$\mathbb{Z}$ είναι ρίζα της μονάδας.

$$\mathbb{Q}(\sqrt{m}) \quad m > 0$$

$$\begin{aligned} r_1 &= 2 \\ r_2 &= 0 \end{aligned}$$

$$r_1 + r_2 - 1 = 1$$

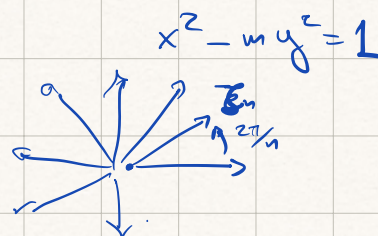
είναι $\mathbb{Z}$ -μορφή

$$\mathbb{Q}(\zeta_n)/\mathbb{Q}$$

$$\zeta_n = e^{2\pi i/n}$$

το αναγωγικό πολυώνυμο

$$\Phi_n(x) = \text{Irr}(\zeta_n, \mathbb{Q})(x) = \prod_{v=1}^n (x - \zeta_n^v)$$



$\deg \Phi_n(x) = \varphi(n) \stackrel{(v,n)=1}{=} \text{α συνάρτηση του Euler}$

$$J_n \longrightarrow J_n^v \quad (v,n)=1 \quad \varphi(n)$$

Έχουμε η το πλύνος εμφυτεύσεις

Οι μονομορφισμοί θα λέγονται γραμμικά ανεξάρτητοι στο L

$$\lambda_1 \sigma_1(x) + \lambda_2 \sigma_2(x) + \dots + \lambda_n \sigma_n(x) = 0 \quad \lambda_i \in L$$

ισχύει για κάθε $x \in K$ αν και μόνο αν $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$

Πρόταση Το σύνολο των εμφυτεύσεων του L/K
 $L \longrightarrow \bar{K}$
 είναι γραμμικά ανεξάρτητο

Αποδ. με επαγωγή: $k=1$ $\forall x \in K$ $\lambda_1 \sigma_1(x) = 0 \Rightarrow \lambda_1 = 0$
 $\neq 0$ σ_1 μονομορφισμός

Εστω ότι $k-1$ το πλύνος εμφυτεύσεις
 είναι γραμμικά ανεξάρτητες $\lambda_1 = 0$.

Θα δείξουμε ότι η πρόταση είναι αληθής και
 για k το πλύνος εμφυτεύσεις.

$$\lambda_1 \sigma_1(x) + \dots + \lambda_k \sigma_k(x) = 0 \quad \lambda_i \in \bar{K} \text{ για κάθε } x \in L$$

Θεωρούμε $\alpha \in L$

$$\lambda_1 \sigma_1(\alpha x) + \dots + \lambda_k \sigma_k(\alpha x) = 0$$

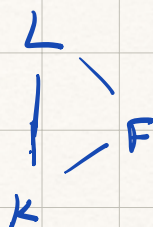
$$\lambda_1 \sigma_1(\alpha) \sigma_1(x) + \dots + \lambda_k \sigma_k(\alpha) \sigma_k(x) = 0$$

$$\lambda_1 \sigma_k(\alpha) \sigma_1(x) + \dots + \lambda_k \sigma_k(\alpha) \sigma_k(x) = 0$$

$$0 = \lambda_1 (\sigma_1(\alpha) - \sigma_k(\alpha)) \sigma_1(x) + \dots + \lambda_{k-1} (\sigma_{k-1}(\alpha) - \sigma_k(\alpha)) \sigma_{k-1}(x)$$

$$\lambda_i (\sigma_i(\alpha) - \sigma_k(\alpha)) = 0$$

$\downarrow$ $\sigma_i \neq \sigma_k \neq 0 \Rightarrow$ μπορού να διαλέξω το α ώστε $\sigma_i(\alpha) \neq \sigma_k(\alpha)$
 $\lambda_i = 0$



$$\sigma_i|_K = \text{Id}$$

$$F = \left\{ \alpha \in L : \text{ώστε } \sigma_1(\alpha) = \dots = \sigma_n(\alpha) \right\}$$

$$F = K.$$

$$[L : F] \geq n$$

Πράγματι

~~K=F~~

$$\text{έστω } [L : F] = m < n$$

$$\omega_1, \dots, \omega_m \quad \text{βάση της } L/F.$$

Γραμμικό
σύστημα

$$x_1 \sigma_1(\omega_i) + x_2 \sigma_2(\omega_i) + \dots + x_n \sigma_n(\omega_i) = 0$$

πληθος εξισώσεων μεγαλύτερο από των άγνωστων.

Το σύστημα έχει μη τετριμμένη λύση

$$\sum_1 \sigma_1(\alpha) + \dots + \sum_n \sigma_n(\alpha) = 0 \quad \text{για κάθε } \alpha \in L$$

$$\alpha = \langle \omega_1, \dots, \omega_m \rangle$$

άτοπο γιατί

οι $\sigma_1, \dots, \sigma_n$ είναι
γραμμικά
ανεξαρτήτως.

$$[L : F] \geq n$$

$$K \subset F \subset L$$

$\geq n$

$$n = [K : L] = [K : F] \cdot [F : L]$$

(1)

n

$$\text{Αν } \alpha \in L \quad \text{τότε } \alpha \in K \Rightarrow \sigma_r(\alpha) = \alpha \quad \text{για}$$

κάθε

$r = 1, 2, \dots, n$

Galois L/K

$\alpha \in L$ ανήκει στο K

αλλιώς μόνο αν $\sigma(\alpha) = \alpha \quad \forall \sigma \in G$

$$G = \text{Gal}(L/K)$$