Ανάλυση των πρώτων στο p-τάξεως κυκλοτομικό σώμα $\mathbb{Q}(\zeta_p)$, p$\geq$ 2 πρώτος

Νικόλαος Δ. Κατσίπης *

4 Δεκεμβρίου 2006

Το άρθρο αυτό αποτελεί το περιεχόμενο εργασίας, που παρουσιάστηκε στα πλαίσια του μεταπτυχιακού μαθήματος : *Αλγεβρική Θεωρία Αριθμών* .

1 Εύρεση ακέραιας βάσης και υπολογισμός της διακρίνουσας του σώματος $\mathbb{Q}(\zeta_p)$

Θεωρούμε το κυκλοτομικό σώμα $\mathbb{Q}(\zeta)$, όπου ζ είναι αρχική ρίζα της μονάδας τάξεως p, (p περιττός πρώτος). Συμβολίζουμε με $\mathbb{A}$ τους αλγεβρικούς ακέραιους του $\mathbb{Q}(\zeta)$. Παρατηρούμε ότι ο ζ είναι ρίζα του : $g(t) = t^{p-1} + \ldots + t + 1$,το οποίο είναι ανάγωγο πολυώνυμο του $\mathbb{Q}[t]$. Αυτό διότι :
$g(t) = t^p - 1/t - 1$, οπότε $g(t+1) = (t+1)^p - 1/t = (t^p + \sum_{i=1}^{p-1}\binom{p}{i}\cdot t^{p-i} + 1 - 1)/t = t^{p-1} + \sum_{i=1}^{p-1}\binom{p}{i}\cdot t^{p-i-1}$ είναι πολυώνυμο *Eisenstein* ως προς p, άρα είναι ανάγωγο πάνω από το $\mathbb{Q}$ [1]. Συνεπώς και το $g(t)$ είναι ανάγωγο πολυώνυμο πάνω από το $\mathbb{Q}$.
Ειδικότερα συμπεραίνουμε ότι τα $1, \zeta, \ldots, \zeta^{p-2}$ αποτελούν μια βάση της επέκτασης $\mathbb{Q}(\zeta)/\mathbb{Q}$.
Οι ρίζες του $g(t)$ είναι οι ζ^i, $1 \leq i \leq p-1$, άρα [2] :

$$\mathrm{T}r(\zeta^i) = (-\text{συντελεστής του } x^{p-1}) = -1 \ \ , \ i = 1 \ldots p-1. \qquad (1)$$

Επίσης, το ελάχιστο πολυώνυμο του 1-ζ είναι το $g(-t+1) = ((-t+1)^p - 1)/(-t)$, το οποίο έχει σταθερό όρο p. Άρα [3]:

$$\mathrm{N}(1-\zeta) = p.$$

---

*Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

[1]πρβλ. σχόλια 3.1 , 3.2

[2]Το χαρακτηριστικό εδώ πολυώνυμο συμπίπτει με το ελάχιστο αφού $degg(t) = [\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$.

[3]$N(1-\zeta) = (-1)^{p-1}\cdot p$

Για κάθε $\alpha \in \mathbb{A}$, συμβολίζουμε με α_i την εικόνα του α μέσω του αυτομορφισμού :

$$\zeta \to \zeta^i, \;\; i = 1 \ldots p-1, \;\; \alpha_1 = \alpha.$$

Άρα οι συζυγείς του α·(1-ζ) είναι οι α_i·(1-ζ^i), $i = 1 \ldots p-1$ και συνεπώς :

$$\mathrm{T}r(\alpha(1-\zeta)) = \sum_{i=1}^{p-1} \alpha_i(1-\zeta^i) = \beta(1-\zeta), \;\; \beta \in A.$$

Τότε :

$$\mathrm{N}(\mathrm{T}r(\alpha(1-\zeta)) = \mathrm{N}(\beta) \cdot \mathrm{N}(1-\zeta) = \mathrm{N}(\beta) \cdot p.$$

Όμως $\mathrm{N}(\mathrm{T}r(\alpha(1-\zeta)) = [\mathrm{T}r(\alpha(1-\zeta)]^{p-1}$, διότι το $\mathrm{T}r(\alpha(1-\zeta) \in \mathbb{Q}$ [4]. Επίσης $\mathrm{N}(\beta) \in \mathbb{Z}$ διότι $\beta \in \mathbb{A}$. Άρα έχουμε ότι :

$$p \;\mid\; \mathrm{T}r(\alpha(1-\zeta), \;\; \text{για κάθε } \alpha \in \mathbb{A}. \tag{2}$$

Τώρα είμαστε σε θέση να υπολογίσουμε την ακέραια βάση του $\mathbb{Q}(z)$.
Έστω κ ο δείκτης του ζ [5]. Τότε για κάθε $\alpha \in \mathbb{A}$:
$\varkappa \cdot \alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}$, όπου $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}$. Τότε :

$$\mathrm{T}r(\alpha(1-\zeta)) =$$

$$= 1/k \cdot \mathrm{T}r[a_0(1-\zeta) + a_1(\zeta - \zeta^2) + \ldots + a_{p-2}(\zeta^{p-2} - \zeta^{p-1})] =$$

$$= 1/k \cdot [a_0(\mathrm{T}r(1) - \mathrm{T}r(\zeta)) + a_1(\mathrm{T}r(\zeta) - \mathrm{T}r(\zeta^2)) + \ldots + a_{p-2}(\mathrm{T}r(\zeta^{p-2}) - \mathrm{T}r(\zeta^{p-1}))] =$$

$$= 1/k[a_0((p-1) - (-1)) + a_1(-1 - (-1)) + \ldots + a_{p-2}(-1 - (-1))] =$$

$$= \frac{p \cdot a_0}{k}.$$

Λόγω της (2) έχουμε ότι :

$$\frac{p \cdot a_0}{k} \in p\mathbb{Z}.$$

[4] Ισχύει ότι αν $\alpha \in \mathbb{Q}$ τότε $\mathrm{T}r_{L/K}(\alpha) = \alpha^{[L:K]}$

[5] $[\mathbb{A} : \mathbb{Z}[\zeta]] = \kappa = i_\zeta$

Άρα
$$k|a_0.$$
Στη συνέχεια ο $\alpha - \frac{a_0}{k}$ είναι αλγεβρικός ακέραιος, άρα και ο :
$$\zeta^{p-1} \cdot (\alpha - \frac{a_0}{k}) = \zeta^{-1} \cdot (\alpha - \frac{a_0}{k}) =$$
$$= \frac{a_1 + a_2\zeta + \ldots + a_{p-2}\zeta^{p-3}}{k} := \alpha'.$$
Αν εργαστούμε όπως πριν με τον α, δηλαδή πολλαπλασιάζοντας τον α' επί $(1 - \zeta)$ κ.τ.λ βρίσκουμε ότι $k|a_1$ και επαναλαμβάνουμε την ίδια διαδικασία εως ότου αποδείξουμε ότι $k|a_i$ για κάθε $i = 0, 1, \ldots p-2$.
Συνεπώς, κάθε $\alpha \in \mathbb{A}$ είναι της μορφής :
$$b_0 + b_1\zeta + \ldots + b_{p-2}\zeta^{p-2} \ \ , \ \ b_i \in \mathbb{Z},$$
το οποίο αποδεικνύει ότι μια ακέραια βάση είναι η $1, \zeta, \ldots \zeta^{p-2}$.
Επίσης μια άλλη ακέραια βάση είναι η $\zeta, \ldots \zeta^{p-2}, \zeta^{p-1}$, [6] της οποίας είναι πιο εύκολο να υπολογίσουμε την διακρίνουσα :
$$D(\zeta, \ldots \zeta^{p-2}, \zeta^{p-1}) = det(\mathrm{Tr}(\zeta^{i+j}))_{1 \leq i,j \leq p-1} =$$
$$= \begin{pmatrix} -1 & -1 & \ldots & -1 & p-1 \\ -1 & -1 & \ldots & p-1 & -1 \\ \vdots & & \ldots & & \vdots \\ p-1 & -1 & \ldots & -1 & -1 \end{pmatrix} =^{7}$$
$$= \begin{pmatrix} -1 & -1 & \ldots & -1 & p-1 \\ 0 & 0 & \ldots & p & -p \\ \vdots & & \ldots & & \vdots \\ p & 0 & \ldots & 0 & -p \end{pmatrix} =^{8}$$
$$= \begin{pmatrix} -1 & -1 & \ldots & -1 & 1 \\ 0 & 0 & \ldots & p & 0 \\ \vdots & & \ldots & & \vdots \\ p & 0 & \ldots & 0 & 0 \end{pmatrix} =$$
$$(-1)^{\frac{p-1}{2}} \cdot p^{p-2}.$$

[6] πρβλ. σχόλια 3.3
[7] αφαιρώντας την πρώτη γραμμή από όλες τις υπόλοιπες
[8] προσθέτωντας στην τελευταία στήλη το άθροισμα όλων των προηγουμένων

Αποδείξαμε λοιπόν το εξής:

Θεώρημα 1.1: Αν ζ είναι αρχική ρίζα του 1 τάξεως p , όπου p περιττός πρώτος, τότε στο $\mathbb{Q}(\zeta)$ (που λέγεται $p-$τάξεως κυκλοτομικό σώμα) μία ακέραια βάση είναι η $1, \zeta, \ldots \zeta^{p-2}$ και η διακρίνουσα είναι $(-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

2 Ανάλυση των Πρώτων στο p-Τάξεως Κυκλοτομικό Σώμα $(p > 2)$

Έστω ζ η αρχική $p-$τάξεως ρίζα της μονάδας,$\mathbb{K} = \mathbb{Q}(\zeta)$ και $\mathbb{A}$ ο δακτύλιος των ακεραίων του σώματος $\mathbb{K}$.
Μια ακέραια βάση του $\mathbb{K}$ είναι η $1, \zeta, \ldots \zeta^{p-2}$. Θέτοντας $\lambda = \zeta - 1$ είναι εύκολο να δούμε ότι και η $1, \lambda, \ldots \lambda^{p-2}$ είναι ακέραια βάση του $\mathbb{K}$ [9]. Προφανώς $\mathbb{K} = \mathbb{Q}(\lambda)$ και αφού το ελάχιστο πολυώνυμο του ζ είναι το $\frac{t^p-1}{t-1}$, το ελάχιστο πολυώνυμο του λ είναι $\frac{(t+1)^p-1}{t}$, δηλαδή είναι ένα πολυώνυμο του *Eisenstein* ως προς τον πρώτο p. Σχετικά έχουμε το εξής γενικό λήμμα.

Λήμμα 2.1: Έστω το αριθμητικό σώμα $\mathbb{Q}(\vartheta)$ βαθμού n και το ϑ είναι ρίζα ενός πολυωνύμου του *Eisenstein* ως προς τον πρώτο p. Τότε η κανονική ανάλυση του p σε πρώτα ιδεώδη του $\mathbb{Q}(\vartheta)$ είναι της μορφής :

$$(p) = \wp^n \ \ , \ \mathrm{N}(\wp) = p.$$

Απόδειξη: Πρβλ. σχόλια 3.6.

Συνεπώς λόγω του λήμματος 2.1, θα είναι :

$$(p) = \wp^{p-1}, \ \mathrm{N}(\wp) = p. \tag{3}$$

Επίσης : $\mathrm{N}((\lambda)) = \mid \mathrm{N}(\lambda) \mid = p$.
Άρα το κύριο ιδεώδες (λ) είναι πρώτο και διαιρεί το p [10].
Λόγω της (3) ο p έχει μόνο ένα πρώτο διαιρέτη τον $\wp$, οπότε $\wp = (\lambda)$. Άρα :

$$(p) = (\lambda)^{p-1} \ \ , \ \mathrm{N}((\lambda)) = p, \ \text{όπου } \lambda = \zeta - 1.$$

[9] πρβλ. σχόλια 3.4
[10] πρβλ. σχόλια 3.5

Ας δούμε τώρα την ανάλυση των πρώτων $p' \neq p$.

Λήμμα 2.2: Αν $\wp'$ είναι ένα πρώτο ιδεώδες που διαιρεί τον ρητό πρώτο $p' \neq p$, τότε $\mathrm{N}(\wp') \equiv 1 \pmod{p}$.

Απόδειξη: Για το τυχόν $\alpha \in \mathbb{A}$ έστω $\hat{\alpha} = \alpha + \wp' \in \mathbb{A}/\wp'$.
Εξ ορισμού είναι : $N(\wp') = Card(\mathbb{A}/\wp')$.
Παρατηρούμε ότι οι κλάσεις : $\hat{1}, \hat{\zeta}, \ldots \widehat{\zeta^{p-1}}$ είναι διαφορετικές.
Αυτό διότι, αν $\widehat{\zeta^i} = \widehat{\zeta^j}$, $0 \leq i < j \leq p-1$, τότε $\zeta^i - \zeta^j \in \wp'$, δηλαδή $(\zeta^i - \zeta^j) \subseteq \wp'$. Δηλαδή, $\wp' | (\zeta^i - \zeta^j) = (\zeta^i)(1 - \zeta^{j-i})$.Τότε :

$$\mathrm{N}(\wp') | \mathrm{N}(\zeta^i) \cdot \mathrm{N}(1 - \zeta^{j-i}) = \mathrm{N}(1 - \zeta^{j-i})$$

Όμως, το ελάχιστο πολυώνυμο του ζ^{j-i} είναι το $g(t) = t^{p-1} + \ldots + t + 1$, οπότε το ελάχιστο του $1 - \zeta^{j-i}$ είναι το $g(t+1)$, με σταθερό όρο p. Έτσι, $\mathrm{N}(1 - \zeta^{j-i}) = p$ και τότε αποκλείεται η σχέση $\mathrm{N}(\wp') | \mathrm{N}(1 - \zeta^{j-i})$, αφού $\mathrm{N}(\wp')$ =δύναμη του p'.
Έτσι οι κλάσεις $\hat{1}, \hat{\zeta}, \ldots \widehat{\zeta^{p-1}}$ αποτελούν υποομάδα τάξης p της πολλαπλασιαστική-ς ομάδας των μη μηδενικών κλάσεων του $\mathbb{A}/\wp'$ η οποία έχει τάξη $\mathrm{N}(\wp') - 1$.
Έπεται λοιπόν ότι $p | \mathrm{N}(\wp') - 1$.

Θεώρημα 2.3: Στο κυκλοτομικό σώμα τάξεως $p > 2$, οι ρητοί πρώτοι αναλύονται ως εξής (ζ αρχική ρίζα τάξεως p) :

(i) $(p) = (\zeta - 1)^{p-1}$, $(\zeta - 1)$ πρώτο ιδεώδες βαθμού 1.

(ii) Αν $p' \neq p$ και f είναι η τάξη του $p' \pmod{p}$ (= ο ελάχιστος εκθέτης m τέτοιος ώστε $p'^m \equiv 1 \pmod{p}$ ' ως γνωστόν, $f | p-1$), τότε :

$$(p') = \wp'_1 \cdot \ldots \cdot \wp'_g \ \ , \ \ g = \frac{p-1}{f},$$

όπου καθένα από τα διαφορετικά πρώτα ιδεώδη $\wp'_1, \ldots, \wp'_g$ είναι βαθμού f.

Απόδειξη:

(i) Έχει ήδη αποδειχτεί.

(ii) Έστω $\wp'$ πρώτο ιδεώδες που διαιρεί το p'. Θα δείξουμε οτι ο βαθμός του $\wp'$ είναι f.
Έστω ότι ο βαθμός του $\wp'$ είναι s. Επειδή $p'^s = \mathrm{N}(\wp') \equiv 1 \pmod{p}$ [11],

[11] Λόγω του λήμματος 2.2

πρέπει, εξ ορισμού του f, να είναι $s \geq f$.
Θα δείξουμε τώρα ότι $s \leq f$.
Έστω $\alpha \in \mathbb{A}$. Ας γράψουμε τον α ως εξής :

$$\alpha = \sum_{i=1}^{p-2} a_i \zeta^i \quad , \quad a_i \in \mathbb{Z} \quad , \quad i = 0, \ldots, p-2. \tag{4}$$

Επίσης ισχύουν οι σχέσεις :

- $\zeta^{p'^f} = \zeta$, διότι $p'^f \equiv 1 \pmod{p}$.
- $(\beta+\gamma)^{p'^f} \equiv \beta^{p'^f} + \gamma^{p'^f} \pmod{p'}$ για όλα τα $\beta, \gamma \in \mathbb{A}$[12].
- $a^{p'^f} \equiv a \pmod{p'}$ $\forall a \in \mathbb{Z}$ [13].

Οπότε, υψώνοντας την (4) στην δύναμη p'^f και χρησιμοποιώντας τις παραπάνω σχέσεις έχουμε οτι :

$$\alpha^{p'^f} \equiv \alpha \pmod{p'},$$

δηλαδή :

$$(\alpha^{p'^f} - \alpha) \subseteq (p') \subseteq \wp'.$$

Συμπεραίνουμε λοιπόν ότι κάθε $\hat{\alpha} \in \mathbb{A}/\wp'$ είναι ρίζα του πολυωνύμου $t^{p'^f} - t \in \mathbb{A}/\wp'[t]$.
Όμως σε οποιοδήποτε σώμα, το πλήθος των ριζών ενός πολυωνύμου είναι το πολύ ίσο με τον βαθμό του. Άρα :

$$Card(\mathbb{A}/\wp') \leq p'^f,$$

δηλαδή,

$$p'^s \leq p'^f,$$

δηλαδή,

$$s \leq f.$$

Δείξαμε δηλαδή ότι ο τυχών πρώτος διαιρέτης $\wp'$ του p' έχει βαθμό f.
Επιπλέον αφού $p' \neq p$ έχουμε ότι :
$p' \not| $ (διακρίνουσα του $\mathbb{Q}(\zeta_p)$)$= (-1)^{\frac{p-1}{2}} \cdot p^{p-2}$.

[12] Απο την ανάπτυξη του διωνύμου του Νεύτωνα : $(\beta+\gamma)^{p'^f} = \sum_{i=0}^{p'^f} \binom{p'^f}{i} \beta^i \cdot \gamma^{p'^f - i}$
[13] Μικρό Θεώρημα $Fermat$

Άρα ο p' δεν διακλαδώνεται [14].
Οπότε το πλήθος των πρώτων διαιρετών $\wp'$ του p' είναι $\frac{p-1}{f}$ [15].

3 Σχόλια

(3.1) **Ορισμός :** Ένα πολυώνυμο $t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ λέγεται πολυώνυμο *Eisenstein* ως προς τον πρώτο $p \in \mathbb{Z}$ αν $p|a_i$, $i = 0, 1, \ldots, n-1$ και $p^2 \not| \ a_0$.

(3.2) Το $p|\binom{p}{i}$, $\forall i \in \{1, \ldots p-1\}$, διότι :

$$\text{αν } x = \binom{p}{i} = \frac{p!}{(p-i)! \cdot i!},$$

δηλαδή

$$p \cdot (p-1)! = x \cdot (p-i)! \cdot i!.$$

Όμως

$$p | x \cdot (p-i)! \cdot i!$$

$$\text{μκδ}(p, (p-1)! \cdot i!) = 1.$$

Άρα

$$p|x.$$

(3.3) Αν η $\{1, \zeta, \ldots \zeta^{p-2}\}$ είναι ακέραια βάση του $\mathbb{Q}(\zeta_p)$ τότε και η $\{\zeta, \ldots \zeta^{p-1}\}$ είναι ακέραια βάση. Αυτό διότι :
Ο πινακας μετάβασης από την βάση $\{1, \zeta, \ldots \zeta^{p-2}\}$ στην $\{\zeta, \ldots \zeta^{p-1}\}$ είναι ο

$$A = \begin{pmatrix} -1 & -1 & \ldots & -1 & -1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & & \ldots & & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \in \mathbb{Z}^{(p-1),(p-1)},$$

[14] Ισχύει το εξής θεώρημα : *Ο πρώτος p διακλαδώνεται στο $\mathbb{K} \Leftrightarrow$ διαιρεί την διακρίνουσα του $\mathbb{K}$*

[15] Λόγω του Θεωρήματος : *Αν $(p') = \wp_1^{e_1} \cdot \ldots \cdot \wp_m^{e_m}$, τότε $e_1 f_1 + \ldots + e_m f_m = n$, όπου $n = [\mathbb{K} : \mathbb{Q}]$ και f_i ο βαθμός του $\wp_i$*

αφού,

- $1 = -\zeta - \zeta^2 - \ldots - \zeta^{p-1}$.
- $\zeta = 1 \cdot \zeta + 0 \cdot \zeta^2 + \ldots + 0 \cdot \zeta^{p-1}$.
- $\zeta^2 = 0 \cdot \zeta + 1 \cdot \zeta^2 + \ldots + 0 \cdot \zeta^{p-1}$

  $\vdots$
- $\zeta^{p-2} = 0 \cdot \zeta + 0 \cdot \zeta^2 + \ldots + 1 \cdot \zeta^{p-2} + 0 \cdot \zeta^{p-1}$

Έχουμε ότι $|det(A)| = 1$.
Άρα η $\{\zeta, \ldots \zeta^{p-1}\}$ είναι ακέραια βάση.

(3.4) Αν η $\{1, \zeta, \ldots \zeta^{p-2}\}$ είναι ακέραια βάση του $\mathbb{Q}(\zeta_p)$, θέτοντας $\lambda = \zeta - 1$ έχουμε ότι και η $\{1, \lambda, \ldots \lambda^{p-2}\}$ είναι ακέραια βάση. Αυτό διότι :
Ο πινακας μετάβασης από την βάση $\{1, \lambda, \ldots \lambda^{p-2}\}$ στην $\{1, \zeta, \ldots \zeta^{p-2}\}$ είναι ο

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & -1 & 0 & \ldots & 0 & 0 \\ 1 & -2 & 1 & \ldots & 0 & 0 \\ \vdots & & & \ldots & & \vdots \\ 1 & -\binom{p-2}{1} & \binom{p-2}{2} & & \ldots & -1 \end{pmatrix}$$

αφού,

- $1 = 1 \cdot 1 + 0 \cdot \zeta + \ldots + 0 \cdot \zeta^{p-2}$.
- $\lambda = 1 \cdot 1 - 1 \cdot \zeta + 0 \cdot \zeta^2 \ldots + 0 \cdot \zeta^{p-2}$.

  $\vdots$
- $\lambda^{p-2} = 1 \cdot 1 - \binom{p-2}{1} \cdot \zeta + -\binom{p-2}{2}\zeta^2 + \ldots - 1 \cdot \zeta^{p-2}$

Έχουμε ότι $|det(A)| = 1$.
Άρα η $\{1, \lambda, \ldots \zeta^{p-2}\}$ είναι ακέραια βάση.

Επίσης μια άλλη προσέγγιση του (**3.4**) είναι η εξής :

Σε αυτή την περίπτωση μπορούμε να αποφύγουμε τα παραπάνω και να δείξουμε με πιο φυσικό τρόπο ότι η $\{\zeta, \ldots \zeta^{p-1}\}$ είναι ακέραια βάση.

Αφού τα $1, \zeta, \ldots, \zeta^{p-2}$ είναι ακέραια βάση, ο τυχών $\alpha \in \mathbb{A}$ είναι της μορφής $a_0 + a_1 \cdot \zeta + \ldots + a_{p-2} \cdot \zeta^{p-2}$, όπου $a_0, \ldots, a_{p-2} \in \mathbb{Z}$. Αλλά τότε

$$\alpha = a_0 + a_1 \cdot (1+\lambda) + a_2 \cdot (1+\lambda)^2 + \ldots + a_{p-2} \cdot (1+\lambda)^{p-2} =$$

$$= b_0 + b_1 \cdot \lambda + \ldots + b_{p-2} \cdot \lambda^{p-2}, \text{ για κατάλληλους } b_0, \ldots, b_{p-2} \in \mathbb{Z}.$$

(3.5) Έχουμε $\mathrm{N}((\lambda)) = |\mathrm{N}(\lambda)| = p$. Το $p \in (\lambda)$ διότι :

$$p = \mathrm{N}((\lambda)) = |\mathbb{A}/(\lambda)|.$$

Άρα :

$$p \cdot (x + (\lambda)) = 0 + (\lambda) \quad , \quad \forall x \in \mathbb{A}.$$

Οπότε :

$$p \cdot x \in (\lambda) \quad , \quad \forall x \in \mathbb{A}.$$

Για $x = 1$ έχουμε ότι :

$$p = N((\lambda)) \in (\lambda).$$

Άρα $(p) \subseteq (\lambda)$, δηλαδή $(\lambda)|(p)$.

(3.6) Απόδειξη Λήμματος 2.1 :

Έστω $t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t]$ το πολυώνυμο *Eisenstein* ως προς τον πρώτο p, του οποίου ρίζα είναι το ϑ. Τότε

$$\vartheta^n + a_{n-1}\vartheta^{n-1} + \ldots + a_1\vartheta + a_0 = 0 \tag{5}$$

Έστω

$$(p) = \prod_{i=1}^{m} \wp_i^{e_i},$$

η κανονική ανάλυση του p σε πρώτα ιδεώδη του $\mathbb{K}$ και f_i ο βαθμός του $\wp_i$. Τότε γνωρίζουμε ότι :

$$\sum_{i=1}^{m} e_i \cdot f_i = n \tag{6}$$

Η σχέση

$$a_j \equiv 0 \pmod{p} \quad , \quad j = 0, \ldots n-1$$

συνεπάγεται την σχέση

$$a_j \equiv 0 \pmod{\wp_i} \quad , \quad j = 0, \ldots n-1 \quad , \quad i = 1, \ldots, m.$$

Άρα :

$$\vartheta \equiv 0 \pmod{\wp_i} \ , \ i = 1, \dots, m.$$

Επίσης

$$\nu_{\wp_i}(a_0) = e_i \ , \ i = 1, \dots, m,$$

αφού $p | a_0$ αλλά $p^2 \not| a_0$.
Τώρα λόγω της (6) έχουμε ότι $e_1 \leq n$. Αν $e_1 = n$ έχουμε τελειώσει. Έστω λοιπόν ότι $e_1 < n$, δηλαδή $e_1 + 1 \leq n$. Τότε στην (5) κάθε όρος $a_{n-k}\vartheta^{n-k} \ , \ k = 1, \dots n-1$, διαιρείται από το $\wp_1^{e_1+1}$ [16].
Επίσης το ϑ^n διαιρείται από το $\wp_1^n$, άρα διαιρείται από το $\wp_1^{e_1+1}$.
Συνεπώς :

$$a_0 = -a_1\vartheta - \dots - a_{n-1}\vartheta^{n-1} - \vartheta^n \equiv 0 \pmod{\wp_i^{e_i+1}},$$

το οποίο όμως είναι άτοπο αφού $\nu_{\wp_1}(a_0) = e_1$.

Αναφορές

[1] Νικόλαος Τζανάκης, Σημειώσεις Αλγεβρικής Θεωρίας Αριθμών.

[16] αφού $\wp_i^{e_i} | (p)$ και $\wp_i | \vartheta$