Θεωρία Iwasawa

Νούλας Δημήτριος
dnoulas@math.uoa.gr

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Κεφάλαιο 2

Προαπαιτούμενα

2.1 Άλγεβρική Θεωρία Αριθμών

Έστω L/K μια πεπερασμένη επέκταση σωμάτων αριθμών με δακτύλιους ακεραίων $\mathcal{O}_L$ και $\mathcal{O}_K$ αντίστοιχα.

Θεώρημα 2.1. *Κάθε γνήσιο μη-μηδενικό πρώτο ιδεώδες $\mathfrak{a} \subset \mathcal{O}_K$ έχει μοναδική παραγοντοποίηση:*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

με $e_i > 0$ και τα $\mathfrak{p}_i$ είναι πρώτα ιδεώδη.

Δοθέντος ενός πρώτου ιδεωδούς $\mathfrak{p} \subset \mathcal{O}_K$, μπορούμε να θεωρήσουμε το ιδεώδες $\mathfrak{p}\mathcal{O}_L$ στον δακτύλιο $\mathcal{O}_L$. Με βάση το προηγούμενο θεώρημα μπορούμε να το παραγοντοποιήσουμε σε γινόμενο πρώτων ιδεωδών:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \tag{2.1}$$

με τα $\mathfrak{p}_i$ να είναι πρώτα ιδεώδη του $\mathcal{O}_L$.

Ορισμός 2.2. *Σε μια παραγοντοποίηση όπως στην 2.1, λεμε το $e_i = e(\mathfrak{p}_i/\mathfrak{p})$ δείκτη διακλάδωσης του $\mathfrak{p}$ στο $\mathfrak{p}_i$. Θα λέμε ότι το πρώτο ιδεώδες $\mathfrak{p}$ διακλαδίζεται στο L αν ισχύει $e_i > 1$ για κάποιο i. Ο βαθμός αδράνειας $f_i = f(\mathfrak{p}_i/\mathfrak{p})$ είναι η διάσταση του διανυσματικού χώρου $\mathcal{O}_L/\mathfrak{p}_i$ πάνω από το πεπερασμένο σώμα $\mathcal{O}_K/\mathfrak{p}$.*

Πρόταση 2.3. *Ένα πρώτο ιδεώδες $\mathfrak{p}$ στο $\mathcal{O}_K$ διακλαδίζεται στο $\mathcal{O}_L$ αν και μόνο αν $\mathfrak{p} \mid \mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)$.*

!Τι σημαίνει $disc(\mathcal{O}_L/\mathcal{O}_K)$· η διακρίνουσα ορίζεται για σώματα αριθμών. Λογικά:

$$disc_{\mathcal{O}_K}(\mathcal{O}_L) = \det(T_{L/K}(a_i a_j))$$

όπου a_i βάση του $\mathcal{O}_L$ ως $\mathcal{O}_K$-πρότυπο, που σημαίνει τα a_i είναι βάση του L υπεράνω του K (σωστό με βάση Milne)

Θεώρημα 2.4. *Με βάση τα παραπάνω έχουμε:*

$$\sum_{i=1}^{r} e(\mathfrak{p}_i/\mathfrak{p}) f(\mathfrak{p}_i/\mathfrak{p}) = \sum_{i=1}^{r} e_i f_i = [L : K] \tag{2.2}$$

Στο εξής θα θεωρούμε ότι η επέκταση L/K είναι Galois. Έτσι μπορούμε να απλοποιήσουμε το προηγούμενο θεώρημα αρκετά. Ξεκινάμε με την ακόλουθη πρόταση.

Πρόταση 2.5. *Η ομάδα $\mathrm{Gal}(L/K)$ δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών $\mathfrak{p}_\mathfrak{i}$ του $\mathcal{O}_L$ που βρίσκονται υπεράνω του $\mathfrak{p}$.*

Απόδειξη. Προς άτοπο, έστω ότι $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$ για κάθε $\sigma \in \mathrm{Gal}(L/K)$. Υπενθυμίζουμε ότι το $\sigma(\mathfrak{p}_i)$ θα είναι και αυτό πρώτο ιδεώδες που θα στέκεται πάνω από το $\mathfrak{p}$. Καθώς είμαστε σε περιοχές Dedekind τα $\mathfrak{p}_i$ και $\sigma(p_i)$ θα είναι μεγιστικά. Άρα $\mathfrak{p}_i \not\subseteq \sigma(\mathfrak{p}_i)$. Από το αντιθετοαντίστροφο του λήμματος αποφυγής πρώτων παίρνουμε ότι

$$\mathfrak{p}_i \not\subseteq \bigcup_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{p}_i)$$

δηλαδή, υπάρχει $x \in \mathfrak{p}_i$ που αποφεύγει όλα τα $\sigma(\mathfrak{p}_i)$. Για την νόρμα, παρατηρούμε ότι:

$$N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

βρίσκεται μέσα στο $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{p}_i$, διότι η νόρμα θα βρίσκεται μέσα στο $\mathcal{O}_K$ καθώς και στο παραπάνω γινόμενο εμφανίζεται το x που ανήκει στο ιδεώδες $\mathfrak{p}_i$. Έχουμε ότι $x \notin \sigma(p_i)$ και άρα $\sigma^{-1}(x) \notin \mathfrak{p}_i$ για κάθε $\sigma \in \mathrm{Gal}(L/K)$. Άρα $\prod \sigma^{-1}(x) = \prod \sigma(x) \notin \mathfrak{p}_i \cap \mathcal{O}_K = \mathfrak{p}$, το οποίο είναι άτοπο. □

Πόρισμα 2.6. *Έστω L/K Galois επέκταση και $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ πρώτο ιδεώδες. Τότε $e(\mathfrak{p}_i/\mathfrak{p}) = e(\mathfrak{p}_j/\mathfrak{p}) = e$ και $f(\mathfrak{p}_i/\mathfrak{p}) = f(\mathfrak{p}_j/\mathfrak{p}) = f$ για κάθε i, j της εξίσωσης 2.1. Ειδικότερα, έχουμε $[L : K] = ref$.*

Απόδειξη. Ο αυτομορφισμός σ διατηρεί τις αλγεβρικές σχέσεις:

$$\sigma(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{r} \sigma(p_i)^{e_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i} = \mathfrak{p}\mathcal{O}_L$$

και συγκρίνουμε τους εκθέτες για να πάρουμε ότι είναι ίδιοι. Αν $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$ τότε παίρνουμε $f_i = f_j$ από τον ισομορφισμό πεπερασμένων σωμάτων:

$$\mathcal{O}_L/\mathfrak{p}_i \simeq \mathcal{O}_L/\mathfrak{p}_j$$

από τον επιμορφισμό που επάγει ο σ:

$$\mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{p}_j$$

$$x \longmapsto \sigma(x) + \mathfrak{p}_j$$

□

Για $[L : K] = n$ υπενθυμίζουμε την ορολογία:

	e	f	r
αδρανές	1	n	1
πλήρως διακλαδιζόμενο	n	1	1
πλήρως διασπώμενο	1	1	n

Ορισμός 2.7. *Έστω $\mathfrak{q}$ ένα πρώτο ιδεώδες του $\mathcal{O}_L$. Η υποομάδα $D_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$ λέγεται η ομάδα διάσπασης του $\mathfrak{q}$ υπεράνω του K.*

Από την πρόταση 2.5 και το θεώρημα orbit-stabilizer παίρνουμε το ακόλουθο πόρισμα.

Πόρισμα 2.8. *Για L/K επέκταση όπως παραπάνω και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathcal{O}_K$ έχουμε:*

(1) $[\mathrm{Gal}(L/K) : D_\mathfrak{q}] = r$ *για κάθε $\mathfrak{q} \mid \mathfrak{p}$.*

(2) $D_\mathfrak{q} = 1$ *αν και μόνο αν το $\mathfrak{p}\mathcal{O}_L$ διασπάται πλήρως.*

(3) $D_\mathfrak{q} = \mathrm{Gal}(L/K)$ *αν και μόνο αν το $\mathfrak{p}\mathcal{O}_L$ διακλαδίζεται πλήρως, δηλαδή $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^n$ για $n = [L : K]$.*

(4) $|D_\mathfrak{q}| = ef$.

Έχουμε μια φυσική απεικόνιση:

$$D_\mathfrak{q} \longrightarrow \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})\right)$$

που ένα $\sigma \in D_\mathfrak{q}$ εφόσον κρατάει σταθερό το $\mathfrak{q}$ επάγει έναν $\mathcal{O}_L/\mathfrak{q}$-αυτομορφισμό $\overline{\sigma}$ ο οποίος κρατάει σταθερό το υπόσωμα $\mathcal{O}_K/\mathfrak{p}$, αφού ο σ κρατάει σταθερό το K. Αποδεικνύεται ότι αυτή η απεικόνιση είναι επί (S. Lang ANT prop 14).

Ορισμός 2.9. *Ο πυρήνας $I_\mathfrak{q} \subseteq D_\mathfrak{q}$ του παραπάνω ομομορφισμού λέγεται ομάδα αδράνειας του $\mathfrak{q}$ υπεράνω του K. Ισχύει ότι:*

$$I_\mathfrak{q} = \{s \in D_\mathfrak{q} : \ \sigma(x) = x \mod \mathfrak{q} \ \forall x \in L\}$$

Από το πόρισμα 2.8 έχουμε ότι:

Πόρισμα 2.10. *Για L/K επέκταση όπως παραπάνω έχουμε ότι $|I_\mathfrak{q}| = e$.*

Από την θεωρία πεπερασμένων σωμάτων, η ομάδα Galois πεπερασμένου σώματος είναι κυκλική και ένας γεννήτορας είναι ο $\sigma(x) = x^q$, όπου q είναι η τάξη του υποσώματος. Αυτός ο γεννήτορας είναι γνωστός ως ο αυτομορφισμός του Frobenius. Στην περίπτωσή μας με $q = |\mathcal{O}_K/\mathfrak{p}|$ και $\mathfrak{q} \mid \mathfrak{p}$ υπάρχει δηλαδή ένας αυτομορφισμός $\overline{\sigma_\mathfrak{q}}$ του $\mathcal{O}_L/\mathfrak{q}$ που σταθεροποιεί το $\mathcal{O}_K/\mathfrak{p}$ που δίνεται από την σχέση $\overline{\sigma_\mathfrak{q}}(x + \mathfrak{q}) = x^q + \mathfrak{q}$. Άρα από τον ισομορφισμό:

$$D_\mathfrak{q}/I_\mathfrak{q} \simeq \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{q})/(\mathcal{O}_K/\mathfrak{p})\right)$$

Έχουμε ότι κάποιο σύμπλοκο $\sigma_\mathfrak{q} + I_\mathfrak{q}$ θα αντιστοιχεί στον αυτομορφισμό του Frobenius. Κάθε στοιχείο του συμπλόκου θα λέγεται αυτομορφισμός του Frobenius στο $\mathfrak{q}$ και θα συμβολίζεται με $\mathrm{Frob}_\mathfrak{q}$. Αν η ομάδα αδράνειας $I_\mathfrak{q}$ είναι τετριμμένη, δηλαδή $e = 1$ και το $\mathfrak{p}$ δεν διακλαδίζεται, τότε υπάρχει καλά ορισμένο στοιχείο $\mathrm{Frob}_\mathfrak{q} \in D_\mathfrak{q}$. Είναι σημαντικό να μπορούμε να συσχετίσουμε τα $\mathrm{Frob}_{\mathfrak{q}_1}$ και $\mathrm{Frob}_{\mathfrak{q}_2}$ για διαφορετικά πρώτα ιδεώδη $\mathfrak{q}_i \mid \mathfrak{p}$. Ξέρουμε ότι υπάρχει $\tau \in \mathrm{Gal}(L/K)$ με $\tau(\mathfrak{q}_1) = \mathfrak{q}_2$ και εύκολα φαίνεται ότι $D_{\mathfrak{q}_2} = \tau D_{\mathfrak{q}_1} \tau^{-1}$, καθώς και $\mathrm{Frob}_{\mathfrak{q}_2} = \tau \,\mathrm{Frob}_{\mathfrak{q}_1}\, \tau^{-1}$. Αν η $\mathrm{Gal}(L/K)$ είναι αβελιανή και το $\mathfrak{p}$ δεν διακλαδίζεται στο L, τότε μπορούμε να ξεχωρίσουμε μοναδικό στοιχείο της $\mathrm{Gal}(L/K)$ που βρίσκεται στην $D_\mathfrak{q}$ για κάθε $\mathfrak{q} \mid \mathfrak{p}$. Αυτό το στοιχείο θα το λέμε $\mathrm{Frob}_\mathfrak{p}$.

Πρόταση 2.11. *Έστω L/K επέκταση Galois και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathcal{O}_K$ και $\mathfrak{q}$ πρώτο ιδεώδες του $\mathcal{O}_L$ με $\mathfrak{q} \mid \mathfrak{p}$. Completions!*

2.2 Κυκλοτομικά Σώματα

Ορισμός 2.12. *Μια πρωταρχική n-οστή ρίζα της μονάδας είναι ένας αριθμός $\zeta_n \in \mathbb{C}$ τέτοιος ώστε $\zeta_n^n = 1$ και $\zeta_n^m \neq 1$ για κάθε $0 < m < n$. Το σώμα $\mathbb{Q}(\zeta_n)$ λέγεται το n-οστό κυκλοτομικό σώμα.*

Ορίζουμε το n-οστό κυκλοτομικό πολυώνυμο $\Phi_n(x)$ ως εξής:

$$\Phi_n(x) = \prod_{\substack{0<m<n \\ \gcd(m,n)=1}} (x - \zeta_n^m)$$

Οι ρίζες του πολυωνύμου είναι ακριβώς οι πρωταρχικές n-οστές ρίζες της μονάδας. Έχουμε $\deg(\Phi_n) = \phi(n)$. Επιπλέον ισχύει ότι $\Phi_n(x) \in \mathbb{Q}[x]$. Αυτό φαίνεται από την σχέση

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2.3}$$

και με επαγωγή στο n. Αφού $\Phi_n(\zeta_n) = 0$ έχουμε ότι $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$. Έχουμε ότι η επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ είναι Galois αφού το Φ_n διασπάται πλήρως στο $\mathbb{Q}(\zeta_n)$. Εφαρμόζοντας τον μετασχηματισμό Möbius στην εξίσωση 2.3 παίρνουμε:

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$$

Λήμμα 2.13. *Έστω $n = p^r$ όπου p πρώτος. Τότε:*

(1) $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \phi(p^r) = p^r - p^{r-1}$.

(2) $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1 - \zeta_{p^r})^{\phi(p^r)}$ *και το* $(1 - \zeta_{p^r})$ *είναι πρώτο ιδεώδες του* $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.

(3) $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$.

(4) $\Delta_{\mathbb{Q}(\zeta_{p^r})} = \pm p^{p^{r-1}(pr-r-1)}$.

Απόδειξη. Άρχικά έχουμε $\mathbb{Z}[\zeta_{p^r}] \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ αφού τα στοιχεία του πρώτου είναι άθροισμα ακεραίων της μορφής $\sum_{i=0}^{p^r-1} a_i\zeta_{p^r}^i$ και τα ακέραια στοιχεία αποτελούν δακτύλιο. Αν ζ'_{p^r} είναι μια άλλη p^r ρίζα της μονάδας, τότε υπάρχουν $s, t \in \mathbb{Z}$ με $p \not| st$ και $\zeta_{p^r} = (\zeta'_{p^r})^t, \zeta'_{p^r} = \zeta_{p^r}^s$. Έτσι, $\mathbb{Q}(\zeta_{p^r}) = \mathbb{Q}(\zeta'_{p^r})$ και $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[\zeta'_{p^r}]$. Επιπλέον,

$$\frac{1 - \zeta'_{p^r}}{1 - \zeta_{p^r}} = \frac{1 - \zeta_{p^r}^s}{1 - \zeta_{p^r}} = 1 + \zeta_{p^r} + \cdots + \zeta_{p^r}^{s-1} \in \mathbb{Z}[\zeta_{p^r}]$$

και όμοια, $(1 - \zeta_{p^r})/(1 - \zeta'_{p^r}) \in \mathbb{Z}[\zeta_{p^r}]$. Αρα το $(1 - \zeta'_{p^r})$ είναι αντιστρέψιμο στο $\mathbb{Z}[\zeta_{p^r}]$ και άρα και στο $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.

$$\Phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = \frac{t^p - 1}{t - 1} = 1 + t + \cdots + t^{p-1},\ t = x^{p^{r-1}}$$

και $\Phi_{p^r}(1) = p$. Από τους ορισμούς φαίνεται ότι:

$$\begin{aligned}\Phi_{p^r}(1) &= \prod(1 - \zeta'_{p^r}) \\ &= \prod \frac{1 - \zeta'_{p^r}}{1 - \zeta_{p^r}}(1 - \zeta_{p^r}) \\ &= u(1 - \zeta_{p^r})^{\phi(p^r)}\end{aligned}$$

με u αντιστρέψιμο στοιχείο του $\mathbb{Z}[\zeta_{p^r}]$. Άρα παίρνουμε ισότητα στα ιδεώδη του $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$, δηλαδή $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1 - \zeta_{p^r})^{\phi(p^r)}$. Συνεπώς, το ιδεώδες $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ έχει τουλάχιστον $\phi(p^r)$ πρώτους παράγοντες στο $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Άρα (;) παίρνουμε $[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] \geq \phi(p^r)$ και συνεπώς

$$[\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \phi(p^r) = p^r - p^{r-1}$$

Επιπλέον, το $(1 - \zeta_{p^r})$ παράγει πρώτο ιδεώδες αλλιώς θα είχαμε παραπάνω από $\phi(p^r)$ πρώτους στην παραγοντοποίηση του $p\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Για την διακρίνουσα, χρησιμοποιούμε τον τύπο με την παράγωγο από την βιβλιογραφία (π.χ. Milne ANT prop 2.33)

$$disc(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z}) = \pm N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Phi'_{p^r}(\zeta_{p^r}))$$

. Έχουμε

$$\Phi'_{p^r}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{p^r-1}}{\zeta_{p^r}^{p^{r-1}} - 1}$$

και

$$N(\zeta_{p^r}) = \pm 1$$

αρα

$$N(p^r) = (p^r)^{\phi(p^r)} = p^{r\phi(p^r)}$$

και ισχυριζόμαστε ότι:

$$N(1-\zeta_{p^r}^{p^s}) = p^{p^s},\ 0 \le s < r$$

Πράγματι, το ελάχιστο πολυώνυμο του $1-\zeta_{p^r}$ είναι το $\Phi_{p^r}(1-x)$ που έχει σταθερό όρο $\Phi_{p^r}(1) = p$. Αρα $N(1-\zeta_{p^r}) = \pm p$. Έστω $s < r$, το $\zeta_{p^r}^{p^s}$ είναι πρωταρχική p^{r-s}-οστή ρίζα της μονάδας, άρα ο ίδιος υπολογισμός για $r-s$ αντί για r δίνει $N_{\mathbb{Q}(\zeta_{p^r}^{p^s})/\mathbb{Q}}(1-\zeta_{p^r}^{p^s}) = \pm p$. Χρησιμοποιώντας την προσεταιριστικότητα της νόρμας, μαζί με $N_{M/L}(a) = a^{[M:L]}$ για σώματα $M \supset L$, παίρνουμε ότι:

$$N_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(1-\zeta_{p^r}^{p^s}) = p^a$$

όπου

$$a = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_{p^r}^{p^s})] = \phi(p^r)/\phi(p^{r-s}) = p^s$$

Συνεπώς, $N(\Phi'_{p^r}(\zeta_{p^r})) = \pm p^c$ όπου $c = p^{r-1}(pr-r-1)$. Άρα η διακρίνουσα του $\mathbb{Z}[\zeta_{p^r}]$ πάνω από το $\mathbb{Z}$ είναι δύναμη του p. Άρα και η διακρίνουσα του $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ πάνω από το $\mathbb{Z}$ είναι δύναμη του p από τον τύπο:

$$disc(\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/\mathbb{Z})[\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} : \mathbb{Z}[\zeta_{p^r}]]^2 = disc(\mathbb{Z}[\zeta_{p^r}/\mathbb{Z}])$$

(Milne remark 2.24)

Επιπλέον, έχουμε ότι το $[\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} : \mathbb{Z}[\zeta_{p^r}]]$ είναι δύναμη του p, άρα $p^M(\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}/\mathbb{Z}[\zeta_{p^r}]) = 0$ για κάποιο M. Δηλαδή, $p^M\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \subseteq \mathbb{Z}[\zeta_{p^r}]$. Το χρησιμοποιούμε αυτό για το ιδεώδες $\mathfrak{p} = (1-\zeta_{p^r})$ και έχουμε $f(\mathfrak{p}/p) = 1$ και άρα η παρακάτω απεικόνιση είναι ισομορφισμός:

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})/(1-\zeta_{p^r})}$$

Άρα $\mathbb{Z} + (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ και άρα επίσης:

$$\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \tag{2.4}$$

η οποία δίνει:

$$(1-\zeta_{p^r})\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \tag{2.5}$$

Έστω $a \in \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Τότε από την εξίσωση 2.4 παίρνουμε ότι $a = a' + \gamma$ με $a' \in (1-\zeta_{p^r})\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ και $\gamma \in \mathbb{Z}[\zeta_{p^r}]$. Η εξίσωση 2.5 δίνει $a' = a'' + \gamma'$ με $a'' \in (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ και $\gamma' \in \mathbb{Z}[\zeta_{p^r}]$. Άρα $a = (\gamma+\gamma') + a''$. Συνεπώς:

$$\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^2\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$$

Με επανάληψη, μπορούμε να πάρουμε $\mathbb{Z}[\zeta_{p^r}] + (1-\zeta_{p^r})^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ για $m \in \mathbb{N}$. Καθώς $(1-\zeta_{p^r})^{\phi(p^r)} = p \cdot u$, u αντιστρέψιμο, έχουμε $\mathbb{Z}[\zeta_{p^r}] + p^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ για κάθε $m \in \mathbb{N}$. Ωστόσο, για αρκετά μεγάλο m έχουμε δείξει ότι $p^m\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} \subseteq \mathbb{Z}[\zeta_{p^r}]$. Άρα πράγματι $\mathbb{Z}[\zeta_{p^r}] = \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$. Αυτό μαζί με τον υπολογισμό του $disc(\mathbb{Z}[\zeta_{p^r}]/\mathbb{Z})$ ολοκληρώνουν την απόδειξη. □

Μαζί με το ακόλουθο λήμμα, θα γενικεύσουμε την πρόταση για $n \in \mathbb{N}$.

Λήμμα 2.14. *Έστω K, L πεπερασμένες επεκτάσεις του $\mathbb{Q}$ με*

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$$

και έστω $d = \gcd(\mathrm{disc}(\mathcal{O}_K/\mathbb{Z}), \mathrm{disc}(\mathcal{O}_L/\mathbb{Z}))$. Τότε

$$O_{KL} \subset d^{-1}\mathcal{O}_K\mathcal{O}_L$$

Πρόταση 2.15. *Έστω ζ_n μια πρωταρχική n-οστή ρίζα της μονάδας και $K = \mathbb{Q}(\zeta_n)$. Ισχύουν τα ακόλουθα:*

(1) $[K : \mathbb{Q}] = \phi(n)$.

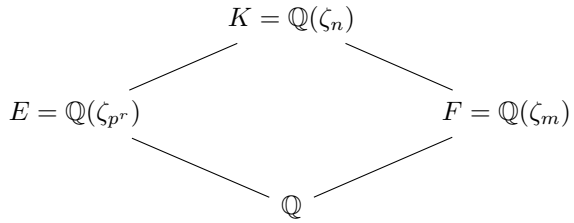
(2) $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

(3) *Ο πρώτος p διακλαδίζεται στο K αν και μόνο αν $p \mid n$ (εκτός αν $n = 2 \cdot$περιττός και $p = 2$). Ειδικότερα, αν $n = p^r$ με $\gcd(p, m) = 1$, τότε*

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_s)^{\phi(p^r)}$$

στο K με τα $\mathfrak{p}_i$ να είναι διακεκριμένοι πρώτοι στο K.

Απόδειξη. Με επαγωγή στο πλήθος των πρώτων που διαιρούν το n. Θεωρούμε τα σώματα:



και κοιτάμε πώς το p παραγοντοποιείται στα E, F. $p\mathcal{O}_E = \mathfrak{p}^{\phi(p^r)}$ διακλαδίζεται πλήρως όπως δίνεται από το προηγούμενη πρόταση. $p\mathcal{O}_F = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ δεν διακλαδίζεται καθώς το p είναι σχετικά πρώτο με την διακρίνουσα.

Τώρα, κοιτάμε την παραγοντοίηση □

2.3 Άπειρη Θεωρία Galois

2.4 Θεωρία Κλάσεων Σωμάτων