Το θεώρημα των Kronecker-Weber

Κωνστάντια Μανούσου-Σωτηροπούλου

Επιβλέπων Καθηγητής

Ιωάννης Α. Αντωνιάδης

Πτυχιακή εργασία

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης

Η παρούσα πτυχιακή εργασία παρουσιάστηκε στο Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών την 30η Σεπτεμβρίου 2014. Την επιτροπή αξιολόγησης αποτέλεσαν οι : Ιωάννης Α. Αντωνιάδης, Μαρία Λουκάκη, Νικόλαος Τζανάκης.

Θα επιθυμούσα να ευχαριστήσω τους καθηγητές μου κ. Ι. Αντωνιάδη, Μ.Λουκάκη και Ν.Τζανάκη που συμμετείχαν στην εξεταστική επιτροπή. Ιδιαιτέρως ευχαριστώ τον κ.Αντωνιάδη υπό την επίβλεψη και την καθοδήγηση του οποίου εκπονήθηκε αυτή η εργασία.

Περιεχόμενα

Εισαγωγή

Το κύριο θέμα της παρούσης πτυχιακής εργασίας είναι η απόδειξη του θεωρήματος Kronecker-Weber:

Αν L αλγεβρικό σώμα αριθμών και $L/\mathbb{Q}$ αβελιανή επέκταση, τότε υπάρχει ρίζα της μονάδας ζ, τέτοια ώστε

$$L \subseteq \mathbb{Q}(\zeta).$$

Το θεώρημα διατυπώθηκε και 'αποδείχτηκε' για πρώτη φορά από τον L.Kronecker [10]. "... ergibt namlich das bemerkenswerthe... Resultat : das die Wurzel jeder Abelschen Gleichung mit ganzzahligen Coeffizienten als rational Function von Wurzeln der Einheit dargestellt werden kan..". Ἠροκύπτει το αξιοσημείωτο αποτέλεσμα : Οι ρίζες κάθε αβελιανής εξίσωσης με ακέραιους συντελεστές μπορούν να παρασταθούν σαν ρητές συναρτήσεις ριζών της μονάδας...' Δυστυχώς η απόδειξη δεν ήταν πλήρης. Η πρώτη πλήρης απόδειξη δόθηκε από τον H.Weber [21]. Φαίνεται ότι και στην απόδειξη του H.Weber υπήρχε κάποιο κενό, Olaf Neumann [15]. Τόσο ο Kronecker όσο και ο Weber χρησιμοποιούν την θεωρία των επιλυτών του Lagrange (Lagrange resolvents).

Πλήρης απόδειξη έχει δοθεί από τον D.Hilbert [9]. (το βιβλίο έχει μεταφραστεί στα αγγλικά)

Ο Hilbert αναπτύσσει στο έργο του την (ομώνυμη) Θεωρία Διακλαδώσεων, σε Galois επεκτάσεις αλγεβρικών σωμάτων αριθμών και χρησιμοποιεί τη θεωρία αυτή για την απόδειξη του θεωρήματος των Kronecker-Weber. Η βασική ιδέα της απόδειξης είναι ότι υπάρχει ακριβώς μια κυκλική επέκταση του $\mathbb{Q}$ βαθμού p, όπου p κάποιος περιττός πρώτος , η οποία διακλαδίζεται μόνο στον πρώτο p. Το σώμα αυτό είναι το μοναδικό υπόσωμα βαθμού p του κυκλοτομικού σώματος των p^2-ριζών της μονάδας. Ακολούθησαν, στηριζόμενες στην ιδέα του *Hilbert*, αποδείξεις των H.Weber [22] καθώς και των A.Speiser [19] και B.Delaunay [5] .

Το θεώρημα των Kronecker-Weber αποτελεί θεμελιώδες βήμα για την κατανόηση της αριθμητικής όλων των αβελιανών επεκτάσεων του σώματος των ρητών αριθμών. Η προσπάθεια γενίκευσης του σε οποιαδήποτε αβελιανή επέκταση αλγεβρικών σωμάτων αρθμών, έδωσε ώθηση στη δημιουργία της Θεωρίας Κλάσεων Σωμάτων, ενός από τους πιο σημαντικούς κλάδους των μαθηματικών κατά τον 20ο αιώνα. Στα πλαίσια της θεωρίας αυτής το θεώρημα των

Kronecker-Weber είναι πόρισμα του αντίστοιχου θεωρήματος (για K=$\mathbb{Q}$ και modulus m=1) .

Στην παρούσα εργασία αποδεικνύουμε το θεώρημα των Kronecker-Weber. Ακολουθούμε την απόδειξη όπως αυτή εκτίθεται στο βιβλίο του P.Ribenboim [16]. Μια ανάλογη απόδειξη έχει δοθεί από τον M.J.Greenberg [7]. Η εργασία αυτή είχε ένα κενό, το οποίο συμπληρώθηκε με χρήση αντίστοιχου θεωρήματος από το βιβλίο του P.Ribenboim . Ο F.Lemmermeyer [11] υποκαθιστά ένα μέρος μόνο της κλασικής απόδειξης με ένα θεώρημα που αφορά στο στοιχείο Stickelberger της επέκτασης $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Το 1951, ο Igor Shafarevich [17] δίνει μια εντελώς διαφορετική και πιο απλή, όπως ο ίδιος ισχυρίζεται, απόδειξη του θεωρήματος. Θεωρεί ότι το θεώρημα των Kronecker-Weber είναι στην ουσία του ένα αποτέλεσμα που αφορά στο πρώτο αριθμό p ("It is essentially a p-adic fact"). Έτσι σε πρώτο βήμα αποδεικνύει την $p-$αδική μορφή του θεωρήματος:

Αν $K/\mathbb{Q}_p$ είναι αβελιανή επέκταση του σώματος των $p-$αδικών αριθμών τότε $\exists n \in \mathbb{N}$ τέτοιος ώστε $K \subseteq \mathbb{Q}_p(\zeta_n)$.

Στη συνέχεια κάνοντας χρήση του "local global principle" αποδεικνύεται το γενικό (global) θεώρημα. Ένα μέρος της απόδειξης του Shafarevich, περιέχεται στην παρούσα εργασία.

Η απόδειξη του Shafarevich έχει μεταφερθεί στο βιβλίο του Wladyslaw Narkievicz [13], καθώς και στα βιβλία J.W.S Cassels [1], Jurgen Neukirch [14] και L.C. Washington [20].

Ανάλογο θεώρημα, που αφορά στην περιγραφή της maximal αβελιανής επέκτασης ρητών σωμάτων συναρτήσεων υπέρ του $\mathbb{F}_p$, έχει δοθεί από τον D.R. Hayes [8]. Η εργασία αυτή περιέχεται και στο βιβλίο των Gabriel Daniel, Villa Salvador [4].

Τέλος, ένα ανάλογο θεώρημα για σώματα χαρακτηριστικής p, έχει αποδειχθεί απο τους Julio Cesar Salas-Torres, Martha Rzedowski-Calderon και Gabriel Villa-Solvador [3].

"The deepest results of algebraic number theory are related to generalizations of the Kronecker-Weber theorem. [12]"

Κεφάλαιο 1

Αλγεβρικά σώματα αριθμών

1.1 Βασικές έννοιες

Σε αυτή την παράγραφο θα παρουσιάσουμε ,χωρίς αποδείξεις, βασικές έννοιες και προτάσεις της αλγεβρικής θεωρίας αριθμών που θα χρησιμοποιηθούν για την απόδειξη του θεωρήματος των Kronecker-Weber.

Ορισμός 1.1.1. *Ένα σώμα $K \subseteq \mathbb{C}$ θα λέγεται αλγεβρικό σώμα αριθμών αν είναι επέκταση πεπερασμένου βαθμού πάνω από το $\mathbb{Q}$.*

Έστω R ένας υποδακτύλιος ενός μεταθετικού δακτυλίου S. Θα λέμε ότι ένα στοιχείο $s \in S$ είναι **ακέραιο** πάνω από τον R όταν υπάρχει μονικό πολυώνυμο $f \in R[X]$ τέτοιο ώστε $f(s) = 0$.
Το σύνολο

$$R' := \{s \in S : s \text{ ακέραιο πάνω από τον } R\}$$

είναι υποδακτύλιος του S που περιέχει τον R και λέγεται **ακέραια κλειστότητα** του R στον S. Θα λέμε ότι ο R είναι ακέραια κλειστός στον S όταν $R = R'$.

Θεώρημα 1.1.1. *Το σύνολο των στοιχείων του K που είναι ακέραια πάνω από το $\mathbb{Z}$ αποτελεί ακεραία περιοχή.*

Ορισμός 1.1.2. *Η ακέραια κλειστότητα του $\mathbb{Z}$ σε ένα αλγεβρικό σώμα αριθμών K θα λέγεται δακτύλιος των ακεραίων R_K του K.*

Θεώρημα 1.1.2. *Έστω R μια ακεραία περιοχή. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες :*
(1) Η R είναι περιοχή της Noether , ακέραια κλειστή και κάθε μη μεδενικό πρώτο ιδεώδες της είναι μέγιστο.
(2) Κάθε μη μηδενικό ιδεώδες της R μπορεί να εκφραστεί με μοναδικό τρόπο ως γινόμενο πρώτων ιδεωδών.
(3) Κάθε μη μηδενικό ιδεώδες της R είναι γινόμενο πρώτων ιδεωδών.

Μια ακέραια περιοχή που ικανοποιεί μια από τις παραπάνω συνθήκες θα λέγεται περιοχή του *Dedekind*.

Θεώρημα 1.1.3. *Ο δακτύλιος των ακεραίων ενός αλγεβρικού σώματος αριθμών είναι περιοχή του Dedekind.*

Αποδεικνύεται ότι ο δακτύλιος των ακεραίων R_K του K είναι ελεύθερη αβελιανή ομάδα. Κάθε βάση της ελεύθερης αβελιανής ομάδας R_K θα λέγεται **βάση ακεραιότητας** του K.

Στη συνέχεια θα ορίσουμε την έννοια της διακρίνουσας. Έστω L/K μια επέκταση αλγεβρικών σωμάτων βαθμού n και $(x_1, x_2, ..., x_n)$ μια $n-$άδα στοιχείων του L. Ορίζουμε διακρίνουσα της $n-$άδας $(x_1, ..., x_n)$ να είναι

$$discr_{L/K}(x_1, x_2, ..., x_n) = det(Tr_{L/K}(x_i x_j))$$

δηλαδή η ορίζουσα του πίνακα του οποίου το (i, j) στοιχείο ισούται με $Tr_{L/K}(x_i x_j)$, για i,j = 1, 2, ..., n. Συμπεραίνουμε ότι η διακρίνουσα της $n-$άδας $(x_1, ..., x_n)$ ανήκει στο K.

Αν $(x'_1, x'_2, ..., x'_n)$ είναι μια άλη $n-$άδα στοιχείων του L και

$$x'_j = \sum_{i=1}^{n} \alpha_{ij} x_i \tag{1.1}$$

για κάθε $j = 1, ..., n$ όπου $\alpha_{ij} \in K$, τότε

$$discr_{L/K}(x'_1, x'_2, ..., x'_n) = (det(\alpha_{ij}))^2 discr_{L/K}(x_1, x_2, ..., x_n) \tag{1.2}$$

Μια άλλη έκφραση της διακρίνουσας δίνεται μέσω των $K-$ μονομορφισμών $\sigma_1, ..., \sigma_n$ του L σε μία αλγεβρική θήκη του : $discr_{L/K}(x_1, x_2, ..., x_n) = det[(\sigma_i(x_j))]^2$.

Θεωρούμε μια ειδική βάση της επέκτασης L/K $1, t, t^2, ..., t^{n-1}$ όπου t είναι πρωταρχικό στοιχείο, $L = K(t)$ και συμπεραίνουμε ότι

$$discr_{L/K}(1, t, ..., t^{n-1}) = \prod_{i<j} (t_i - t_j)^2$$

όπου $t_1 = t, t_2, ..., t_n$ είναι οι συζυγείς του t. Σε αυτήν την περίπτωση συνηθίζουμε να λέμε την παραπάνω έκφραση **διακρίνουσα του** t πάνω από το K. Όλοι οι συζυγείς του t έχουν την ίδια διακρίνουσα.

Έστω $f(X) \in K[X]$ ένα πολυώνυμο βαθμού n, με ρίζες $a_1, a_2, ..., a_n$ και μεγιστοβάθμιο όρο b_0, ορίζουμε διακρίνουσα του f με

$$discr(f) = b_0^{2n-2} \prod_{i<j} (a_i - a_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (a_i - a_j).$$

Οπότε $discr(f) \in K$ και $discr(f) \neq 0$ αν και μόνο αν το f έχει διακεκριμένες ρίζες. Αν $L = K(t), t \in L$ και f είναι το ελάχιστο πολυώνυμό του, τότε $discr_{L/K}(t) = discr(f)$.

Η διακρίνουσα του f υπολογίζεται από τον τύπο

$$discr(f) = (-1)^{\frac{n(n-1)}{2}} b_0 N_{K(t)/K}(f'(t))$$

όπου t μια ρίζα του f και f' η παράγωγος του f.

Άμεση συνέπεια της σχέσης 1.2 είναι ότι οι διακρίνουσες δύο βάσεων ακεραιότητας της επέκτασης L/K είναι ίσες.

Ορισμός 1.1.3. *Η διακρίνουσα της επέκτασης $K/\mathbb{Q}$ οποιασδήποτε βάσης ακεραιότητας του σώματος K, θα λέγεται διακρίνουσα του K και θα συμβολίζεται με $\delta_K = \delta_{K/\mathbb{Q}}$. Δηλαδή $\delta_K \in \mathbb{Z}, \delta_K \neq 0$.*

Θεώρημα Minkowski . *Αν K είναι αλγεβρικό σώμα αριθμών διαφορετικό από το $\mathbb{Q}$, τότε $|\delta_K| \geq 2$.*

1.2 Επεκτάσεις ιδεωδών

Έστω K αλγεβρικό σώμα αριθμών , L/K επέκταση πεπερασμένου βαθμού και R_K, R_L οι αντίστοιχοι δακτύλιοι των ακεραίων.

Γνωρίζουμε ότι αν $P \in Spec(R_K)$ τότε το PR_L μπορεί να γραφτεί με μοναδικό τρόπο ως γινόμενο δυνάμεων πρώτων ιδεωδών του R_L :

$$PR_L = \prod_{i=1}^{r} Q_i^{e_i}, Q_i \in Spec(R_L) \tag{1.3}$$

Ορισμός 1.2.1. *Ο παραπάνω αριθμός r θα λέγεται* ***αριθμός ανάλυσης*** *του P στην επέκταση L/K. Αν κριθεί απαραίτητο θα χρησιμοποιήσουμε τον συμβολισμό $r_P(L/K)$ ή απλά r_P.*

Ισχύει ότι $r \geq 1$, επειδή $PR_L \neq R_L$. Αν PR_L είναι πρώτο ιδεώδες του R_L θα λέμε ότι το P **αδρανεί** στην L/K.

Ορισμός 1.2.2. *Για κάθε $i = 1, 2, ..., r$ το e_i θα λέγεται* ***δείκτης διακλάδωσης*** *του Q_i στην L/K. Αν $e_i = 1$ θα λέμε ότι το Q_i δεν διακλαδίζεται στην L/K. Μερικές φορές θα χρησιμοποιούμε τους συμβολισμούς $e_{Q_i}(L/K)$ ή $e(Q_i|P)$*

Αποδεικνύεται ότι ο R_L/PR_L είναι διανυσματικός χώρος πάνω από το σώμα R_K/P διάστασης $[R_L/PR_L : R_K/P] \leq [L : K]$. Από την παραπάνω σχέση και τον ισμορφισμό μεταξύ των $R_K/P-$ διανυσματικών χώρων $(R_L/PR_L)/(Q_i/PR_L) \cong R_L/Q_i$ έπεται ότι $[R_L/Q_i : R_K/P] \leq [L : K]$.

Ορισμός 1.2.3. *Η διάσταση f_i του R_L/Q_i πάνω από το σώμα R_K/P θα λέγεται* ***βαθμός αδρανείας*** *του Q_i στην L/K. Ισοδύναμοι συμβολισμοί : $f_i = f_{Q_i}(L/K) = f(Q_i|P)$.*

Έστω τώρα L'/L επέκταση πεπερασμένου βαθμού και $R_{L'}$ η ακέραια κλειστότητα του R_L στο L'. Θα δούμε κάποιες βασικές ιδιότητες των αριθμών που ορίσαμε παραπάνω.

Μεταβατικότητα. *Έστω $Q' \in Spec(R_{L'})$ και $Q = Q' \cap R_L, P = Q \cap R_K$ και υποθέτουμε ότι $P \neq 0$. Τότε*

$$e(Q'|P) = e(Q'|Q)e(Q|P),$$

$$f(Q'|P) = f(Q'|Q)f(Q|P)$$

Επίσης ισχύει ότι αν $PR_L = \prod_{i=1}^{r} {Q_i}^{e_i}$ και αν r_i' είναι ο αριθμός ανάλυσης του Q_i στην L'/L τότε ο αριθμός ανάλυσης του P στην L'/K ισούται με $r_P(L'/K) = \sum_{i=1}^{r} r_i'$.

Θεώρημα 1.2.1. *Με τους παραπάνω συμβολισμούς ισχύει* $[R_L/PR_L : R_K/P] = [L : K]$ *και* $[L : K] = \sum_{i=1}^{r} e_i f_i$

Στην περίπτωση που η επέκταση L/K είναι $Galois$ τα πράγματα γίνονται πιο απλά. Έστω λοιπόν L/K μια επέκταση $Galois$ βαθμού n, G η ομάδα $Galois$ της επέκτασης αυτης. Τα στοιχεία της G αφήνουν κάθε στοιχείο του K αναλλοίωτο και στέλνουν κάθε στοιχείο του L στους συζυγείς του. Δηλαδή, $\sigma(R_L) \subseteq R_L \forall \sigma \in G$, οπότε επίσης $R_L = \sigma(\sigma^{-1}(R_L)) \subseteq R_L$ δείχνοντας ότι $\sigma(R_L) = R_L$.

Ενδιαφέρουσα είναι η μεταβατικότητα της δράσης της G στο σύνολο των πρώτων ιδεωδών του R_L που έχουν δεδομένη τομή με τον R_K :

Πρόταση 1.2.1. *Αν* $Q, Q' \in Spec(R_L)$ *τέτοια ώστε* $Q \cap R_K = Q' \cap R_K$ *τότε* $\exists \sigma \in G$ *με* $\sigma(Q) = Q'$

Πόρισμα 1.2.1. *Αν η* L/K *είναι* $Galois$ *βαθμού* n *και* $PR_L = \prod_{i=1}^{r} {Q_i}^{e_i}$, $[R_L/Q_i : R_K/P] = f_i$ *τότε* $e_1 = e_2 = ... = e_r, f_1 = f_2 = ... = f_r$ *και αν* R_K/P *είναι πεπερασμένο σώμα τότε* R_L/Q_i *είναι ισόμορφο με μια επέκταση βαθμού* f_i *του* R_K/P

Πόρισμα 1.2.2. *Άμεση συνέπεια του Θεωρήματος 1.2.1 και του Πορίσματος 1.2.1 είναι ότι αν* L/K *είναι* $Galois$, *τότε* $[L : K] = efr$

Κεφάλαιο 2

Διακρίνουσα και διαφορίζουσα

2.1 Διακρίνουσα

Θεωρούμε K αλγεβρικό σώμα αριθμών, L/K επέκταση βαθμού n και R_K, R_L τους αντίστοιχους δακτυλίους των ακεραίων.

Ορισμός 2.1.1. *Η **σχετική διακρίνουσα** της επέκτασης L/K είναι το ιδεώδες $\delta_{L/K}$ του R_K που παράγεται από τα στοιχεία $discr_{L/K}(x_1, ..., x_n)$ όπου $\{x_1, ..., x_n\}$ είναι μια $K-$ βάση του L με $x_i \in R_L$.*

Πρόταση 2.1.1. *Έστω $\{x_1, ..., x_n\}$ μια βάση της L/K με $x_i \in R_L$. Τότε $\delta_{L/K} = discr_{L/K}(x_1, ..., x_n)R_K$ αν και μόνο αν ο R_L είναι ελεύθερο $R_K-module$ και $\{x_1, ..., x_n\}$ είναι μια R_K- βάση του R_L.*

Απόδειξη. ($\Leftarrow$) Έξ ορισμού $discr_{L/K}(x_1, ..., x_n)R_K \subseteq \delta_{L/K}$. Έστω τώρα $\{x'_1, ..., x'_n\}$ οποιαδήποτε $K-$ βάση του L με $x'_j \in R_L$. Τότε έχουμε

$$x'_j = \sum_{i=1}^{n} a_{ij}x_i, a_{ij} \in R_K$$

οπότε

$$discr_{L/K}(x'_1, ..., x'_n) = [det(a_{ij})]^2 discr_{L/K}(x_1, ..., x_n)$$

όπου $[det(a_{ij})]^2 \in R_K$. Άρα $\delta_{L/K} \subseteq discr_{L/K}(x_1, ..., x_n)R_K$

($\Rightarrow$) Υποθέτουμε ότι $\delta_{L/K} = discr_{L/K}(x_1, ..., x_n)R_K$, όπου $\{x_1, ..., x_n\}$ είναι μια $K-$ βάση του L με $x_i \in R_L$.

Λήμμα 2.1.1. *Κάθε πεπερασμένα παραγόμενο torsionfree $R-module$, όπου R είναι περιοχή κυρίων ιδεωδών, είναι ελεύθερο $R-module$. [18]*

Έστω $P \in Spec(R_K)\backslash\{0_{R_K}\}$ και $T = R_K \backslash P$, θεωρούμε $R' = (R_K)_P, S' = T^{-1}R_L, P' = P(R_K)_P$. Γνωρίζουμε ότι ο R' είναι περιοχή κυρίων ιδεωδών και χρησιμοποιώντας το Λήμμα 2.1.1, καθώς S' είναι η ακέραια κλειστότητα του R' στο L, έχουμε πως S' είναι πεπερασμένα παραγόμενο torsion-free ελεύθερο $R'-module$ με rank n. Έστω λοιπόν $\{x'_1, ..., x'_n\}$ μια βάση του. Τότε

$$x'_i = \frac{y_i}{s_i}, y_i \in R_L, s_i \in T(= R_K \setminus P). \tag{2.1}$$

Η $\{y_1, ..., y_n\}$ είναι μια $K-$ βάση του L. Πράγματι, αν $x \in L$ τότε το x γράφεται ως

$$x = \sum_{i=1}^{n} a_i x_i, a_i \in K \tag{2.2}$$

όμως $x_i \in R_L \subseteq S' \Rightarrow x_i$ γράφεται ως

$$x_i = \sum_{j=1}^{n} b_j x'_j = \sum_{j=1}^{n} (b_j \frac{1}{s_j}) y_j,$$

με $b_j \in R'$ επομένως $b_j \frac{1}{s_j} \in K$.

Επίσης από τη σχέση 2.1 προκύπτει ότι

$$discr_{L/K}(x'_1, ..., x'_n) \in discr_{L/K}(y_1, ..., y_n)R' \subseteq \delta_{L/K}R'. \tag{2.3}$$

Από την άλλη μεριά

$$x_j = \sum_{i=1}^{n} a'_{ij} x'_i, \text{ με } a'_{ij} \in R' \tag{2.4}$$

διότι $x_j \in R_L \subseteq S'$.Γνωρίζουμε πως S' είναι ελεύθερο $R'-module$ και $\{x'_1, ..., x'_n\}$ είναι μια βάση του. Οπότε

$$discr_{L/K}(x_1, ..., x_n) = [det(a'_{ij})]^2 discr_{L/K}(x'_1, ..., x'_n) \tag{2.5}$$

και άρα

$$\delta_{L/K}R' \subseteq discr_{L/K}(x'_1, ..., x'_n)R'$$

Από τις δύο παραπάνω σχέσεις παίρνουμε ότι

$$discr_{L/K}(x_1, ..., x_n)R' = discr_{L/K}(x'_1, ..., x'_n)R'$$

άρα από τη σχέση 2.5 $[det(a'_{ij})]^2 \in (R')^* \Rightarrow det(a'_{ij}) \in (R')^*$. Δηλαδή ο πίνακας $(a'_{ij})_{i,j}$ είναι αντιστρέψιμος και τα στοιχεία του αντιστρόφου πίνακα ανήκουν στον R'. Συνεπώς από τη σχέση 2.4 προκύπτει ότι τα x'_i ανήκουν στο $R' - module$ που παράγεται από τα $x_1, ..., x_n$. Το σύνολο $\{x'_1, ..., x'_n\}$ αποτελεί μια βάση του $R' - moduleS'$ και $< x'_1, ..., x'_n > \subseteq < x_1, ..., x_n > R'$. Επιπλέον τα $x_1, ..., x_n$ είναι γραμμικώς ανεξάρτητα πάνω από το K άρα και πάνω από τον R' οπότε το $\{x_1, ..., x_n\}$ είναι βάση του $R' - moduleS'$.

Τα παραπάνω ισχύουν για κάθε $P \in Spec(R_K) \setminus \{0_{R_K}\}$. Έστω λοιπόν $y \in R_L$, το y μπορεί να γραφτεί στη μορφή

$$y = \sum_{i=1}^{n} c_i x_i, c_i \in K.$$

Για κάθε $P \in Spec(R_K) \setminus \{0_{R_K}\}$ έχουμε δείξει παραπάνω ότι $c_i \in (R_K)_P$, επομένως $c_i \in \cap_{P \in Spec(R_K) \setminus \{0_{R_K}\}} (R_K)_P = R_K$, όπου η τελευταία ισότητα αποδεικνύεται παρακάτω Λήμμα . □

Λήμμα 2.1.2. *Έστω R ακέραια περιοχή και I ένα ιδεώδες αυτής. Τότε*

$$I = \cap IR_{P_i}, \text{ όπου } P_i \text{ μέγιστο ιδεώδες του } R.$$

Απόδειξη. Αν η R είναι σώμα τότε είναι προφανές.

Έστω λοιπόν ότι η R δεν είναι σώμα. Για κάθε ιδεώδες I του R έχουμε ότι $I \subseteq \cap IR_{P_i}$. Αν $x \in \cap\, IR_{P_i} \Rightarrow x = \frac{a_i}{b_i}$, όπου $a_i \in I$ και $b_i \notin P_i$.
Θεωρούμε $J := < b_1, ..., b_n >$ και παρατηρούμε πως $J \not\subseteq P_i$, για κάθε P_i μέγιστο ιδεώδες του R. Οπότε $J = R$, επομένως $1 = \sum_{i=1}^{n} c_i b_i$, για κάποια $c_i \in R$. Άρα

$$x = \sum_{i=1}^{n} xc_i b_i = \sum_{i=1}^{n} \frac{a_i}{b_i} c_i b_i = \sum_{i=1}^{n} a_i c_i \in I,$$

καθώς $a_i \in I$. □

Πριν προχωρήσουμε στο Θεώρημα του Dedekind θα αποδείξουμε το παρακάτω :

Λήμμα 2.1.3. *Έστω K (τέλειο) σώμα, S μεταθετική $K-$ άλγεβρα πεπερασμένης διάστασης και $x_1, ..., x_n$ μια βάση. Αν υπάρχει μη μηδενικό μηδενοδύναμο στοιχείο του S τότε $discr(S|K) = 0$*

Απόδειξη. Υποθέτουμε ότι ο S περιέχει ένα μηδενοδύναμο στοιχείο $x \neq 0$. Έστω $\{x_1, ..., x_n\}$ μια $K-$ βάση του S, τέτοια ώστε $x_1 = x$. Αφού ο S είναι μεταθετικός, τότε xx_j είναι επίσης μηδενοδύναμο.

Το ελάχιστο πολυώνυμο του ενδομορφισμού θ_{xx_j} ισούται με X^r, για κάποιο $r > 0$. Όπως είναι γνωστό από τη Γραμμική Άλγεβρα το χαρακτηριστικό πολυώνυμο του θ_{xx_j} είναι πολλαπλάσιο του ελαχίστου πολυωνύμου του, βαθμού n και έχει τους ίδιους παράγοντες. Άρα το χαρακτηριστικό πολυώνυμο είναι το X^n και $Tr_{S/K}(xx_j) = 0, \forall j = 1, 2, ..., n$. Οπότε $discr_{S/K}(x_1, ..., x_n) = det(Tr_{S/K}(x_i x_j)) = 0$, διότι στον πίνακα των Traces η πρώτη σειρά είναι μηδενική. Επομένως $discr(S|K) = 0$ □

Θεώρημα Dedekind. *Το μη μηδενικό πρώτο ιδεώδες P του R_K διακλαδίζεται στην επέκταση L/K αν και μόνο αν $\delta_{L/K} \subseteq P$. Δηλαδή, υπάρχουν μόνο πεπερασμένα το πλήθος πρώτα ιδεώδη που διακλαδίζονται στην επέκταση L/K.*

Απόδειξη. Γνωρίζουμε ότι $PR_L = \prod_{i=1}^{r} {Q_i}^{e_i}$, όπου $Q_i \in Spec(R_L)$ και $e_i \geq 1$. Επίσης $R_L/PR_L \cong \prod_{i=1}^{r} R_L/{Q_i}^{e_i}$ [18]. Το P διακλαδίζεται όταν $e_i > 1$, για κάποιο $i \in \{1, ..., r\}$, δηλαδή $R_L/{Q_i}^{e_i}$ έχει μη μηδενικό μηδενοδύναμο στοιχείο ή ισοδύναμα ο δακτύλιος R_L/PR_L έχει μη μηδενικό μηδενοδύναμο στοιχείο. Τότε από Λήμμα 2.1.3 έχουμε

$$discr((R_L/PR_L)/R_K/P) = 0. \tag{2.6}$$

Θεωρούμε $T = R_K \setminus P, R' = (R_K)_P, S' = T^{-1}R_L$ και $P' = P(R_K)_P$. Λόγω των ισομορφισμών $R'/PR' \cong (R_K)/P, S'/P'S' \cong R_L/PR_L$ προκύπτει ότι $discr((R'/PR')|(S'/P'S')) = 0$. Ο S' είναι ελεύθερο $R' - module$ με $rank; n$, άρα αν $\{x'_1, ..., x'_n\}$ είναι μια $R'-$βάση του S' τότε οι εικόνες $\overline{x'_i}$ μέσω του ομομορφισμού

$$S' \to S'/PS'$$

είναι μια $R'/PR'-$βάση του S'/PS'.

Τώρα $discr(S'/PS'|R'/P')$ είναι το ιδεώδες που παράγεται από τα στοιχεία $discr_{(S'/PS')|(R'/P')}(\overline{x'_1}, ..., \overline{x'_n})$ για όλες τις πιθανές βάσεις $\{\overline{x'_1}, ...\overline{x'_n}\}$ του S'/PS' πάνω από τον R'/P'. Οπότε $discr(S'/PS')|(R'/P') = 0$ ακριβώς όταν

$$discr_{(S'/PS')|(R'/P')}(\overline{x'_1}, ..., \overline{x'_n}) = \overline{discr_{S'|R'}(x'_1, ..., x'_n)} = \bar{0}$$

δηλαδή όταν $discr_{S'|R'}(x'_1, ..., x'_n) \in P'$, για κάθε βάση του $R' - moduleS'$.

Η τελευταία συνθήκη ισοδυναμεί με τη σχέση $\delta_{L/K} \subseteq P$. Πράγματι, έστω $\{x_1, ..., x_n\}$ μια $K-$βάση του L με $x_i \in R_L \forall i = 1, ..., n$. Αν $\{x'_1, ..., x'_n\}$ είναι μια $R'-$ βάση του S' τότε εκφράζοντας τα $x_1, ..., x_n$ ως γραμμικούς συνδιασμούς των $x'_1, ..., x'_n$ με συντελεστές στον R' παίρνουμε

$$discr_{L/K}(x_1, .., x_n) = discr_{S'|R'}(x_1, ..., x_n) \in discr_{S'|R'}(x'_1, ..., x'_n)R' \subseteq P'$$

όμως $discr_{L/K}(x_1, .., x_n) \in R_K$, διότι $x_i \in R_L$ για κάθε i. Επομένως $discr_{L/K}(x_1, .., x_n) \in R_K \cap P(R_K)_P = P$ και $\delta_{L/K} \subseteq P$.

Αντίστροφα, αν $\delta_{L/K} \subseteq P$ και $\{x'_1, ..., x'_n\}$ είναι μια $R'-$ βάση του S' έστω $x'_i = \frac{y_i}{s_i}, y_i \in R_L, s_i \in T$ τότε $\{x_1, .., x_n\}$ είναι μια $K-$ βάση του L. Οπότε

$$discr_{S'/R'}(x'_1, ..., x'_n) = discr_{L/K}(x'_1, ..., x'_n) =$$
$$= (\frac{1}{s_1...s_n})^2 discr_{L/K}(x_1, ..., x_n) \subseteq PR' = P(R_K)_P = P'.$$

□

2.2 Διαφορίζουσα

Έστω L/K πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών. Η θεωρία της διαφορίζουσας πηγάζει από την ύπαρξη μιας κανονικής μη εκφυλισμένης συμμετρικής διγραμμικής μορφής του $K-$ διανυσματικού χώρου L, του ίχνους,

$$T(x, y) = Tr_{L/K}(xy).$$

Έστω $M \subseteq L$, τότε το σύνολο $M^* := \{x \in L | Tr_{L/K}(xy) \in R \forall y \in M\}$ θα λέγεται **συμπληρωματικό σύνολο** του M ως προς τον R_K. Αποδεικνύεται ότι το M^* είναι κλασματικό ιδεώδες. Επίσης T^* είναι κλασματικό ιδεώδες του L (ως προς το R_L.)

Ορισμός 2.2.1. *Το κλασματικό ιδεώδες*

$$R_L{}^* = \{x \in L | Tr_{L/K}(xR_L) \subseteq R_K\}$$

θα λέγεται ***αντίστροφη διαφορίζουσα****. Το αντίστροφο ιδεώδες του,*

$$\Delta(R_L|R_K) = (R_L{}^*)^{-1}$$

θα λέγεται ***διαφορίζουσα*** *της* $R_L|R_K$.
$\Delta_{L/K} := \Delta(R_L|R_K)$ Επειδή $R_L \subseteq R_L{}^*$, προκύπτει ότι η $\Delta(R_L|R_K)$ είναι μη

μηδενικό ακέραιο ιδεώδες του T. Όμως ο R_L είναι περιοχή του Dedekind , άρα το ιδεώδες $\Delta(R_L|R_K)$ γράφεται με μοναδικό τρόπο στη μορφή $\Delta(R_L|R_K) = \prod Q^{s_Q}$ όπου Q είναι πρώτα ιδεώδη του R_L και $s_Q \geq 0$. Ο ακέραιος s_Q θα λέγεται **εκθέτης του Q στη διαφορίζουσα $\Delta(R_L|R_K)$.**

Ορισμός 2.2.2. *Έστω $t \in R_L$ και $f(X) \in R_K[X]$ το ανάγωγο πολυώνυμο του t πάνω από το K. Διαφορίζουσα(different) του στοιχείου t, ορίζεται*

$$\delta_{L/K}(t) := \begin{cases} f'(t), & L = K(t) \\ 0, & L \neq K(t). \end{cases}$$

Πρόταση 2.2.1. *Αν $R_L = R_K[t]$, τότε η διαφορίζουσα είναι το κύριο ιδεώδες*

$$\Delta_{L/K} =< \delta_{L/K}(t) > .$$

Απόδειξη. Έστω $f(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1} + X^n$ το ελάχιστο πολυώνυμο του t πάνω από το K και

$$\frac{f(X)}{X-t} = b_0 + b_1X + ... + b_{n-1}X^{n-1}. \tag{2.7}$$

Η δυική βάση της $1, t, ..., t^{n-1}$ ως προς το $Tr_{L/K}(xy)$ ισούται με

$$\frac{b_0}{f'(t)}, \frac{b_1}{f'(t)}, ..., \frac{b_{n-1}}{f'(t)},$$

όπου f' η παράγωγος του f. Πράγματι, αν $t_1 = t, ..., t_n$ είναι οι ρίζες του f, τότε ισχύει η ακόλουθη ισότητα

$$\sum_{i=1}^{n} \frac{f(X)}{X-t_i} \frac{{t_i}^r}{f'(t)} = X^r, 0 \leq r \leq n-1.$$

Επειδή η διαφορά των δυο μελών της παραπάνω ισότητας είναι ένα πολυώνυμο βαθμού το πολυ $n-1$ με n ρίζες, τις $t_1, ..., t_n$, θα είναι ταυτοτικά μηδέν. Επίσης η παραπάνω ισότητα είναι ισοδύναμη με την

$$Tr(\frac{f(X)}{X-t} \frac{t^r}{f'(t)}) = X^r.$$

Θεωρώντας τώρα τους συντελεστές κάθε δύναμης του X, συμπεραίνουμε ότι

$$Tr(t^i \frac{b_j}{f'(t)}) = \delta_{ij}$$

και το συμπέρασμα έπεται.

Αφού $T = R[t]$, έχουμε $T = R + tR + t^2R + ... + t^{n-1}R$. Οπότε $T^* = f'(t)^{-1}(b_0R + b_1R + ... + b_{n-1}R)$. Από τη σχέση 2.7 προκύπτει

$$\begin{aligned} b_{n-1} &= 1 \\ b_{n-2} - tb_{n-1} &= a_{n-1} \\ ... &= ... \end{aligned}$$

άρα

$$b_{n-i} = t^{n-i} + a_{n-1}t^{i-2} + ... + a_{n-i+1},$$

και $b_0R + ... + b_{n-1}R = R[t] = T$. Οπότε $(T^*)^{-1} = f'(t)^{-1}T$ και $\Delta_{L/K} =< f'(t) >$ □

Μεταβατικότητα της διαφορίζουσας. *Αν $K \subseteq L \subseteq M$, τότε $\Delta_{M/K} = \Delta_{M/L}\Delta_{L/K}$.*

Έστω $P \in Spec(R_K)$ και $S := R_K \setminus P$, $R' = (R_K)_P, T' = S^{-1}R_L$.

Ορισμός 2.2.3. *Η διαφορίζουσα $\Delta(R'|T')$ θα λέγεται διαφορίζουσα της L/K πάνω από το P και θα συμβολίζεται με $\Delta_P(L/K)$.*

Πρόταση 2.2.2. $\Delta_P(L|K) = \Delta_{L/K}T'$

Το θεώρημα του Dedekind χαρακτηρίζει τα ιδεώδη $P \in Spec(R_K)$ τα οποία διακλαδίζονται στην L/K. Είναι ακριβώς εκείνα τα οποία διαιρούν την διακρίνουσα.

Θεώρημα 2.2.1. *Η διαφορίζουσα χαρακτηρίζει τα ιδεώδη $Q \in Spec(R_L)$, τα οποία εμφανίζονται στην ανάλυση του $P := Q \cap R_K$, με εκθέτη $e \geq 2$. Είναι ακριβώς εκείνα που διαιρούν τη διαφορίζουσα.*

Κεφάλαιο 3

Κυκλοτομικά σώματα αριθμών

3.1 Ο δακτύλιος των ακεραίων και η διακρίνουσα

Έστω K= $\mathbb{Q}(\zeta)$, όπου ζ μιά πρωταρχική p- οστή ρίζα της μονάδας και p ένας περιττός πρώτος αριθμός (για p=2 τα αποτελέσματα είναι τετριμμένα). Το ελάχιστο πολυώνυμο του ζ πάνω απο το $\mathbb{Q}$ είναι το

$$\Phi_p(X) = X^{p-1} + X^{p-2} + ... + X + 1,$$

οπότε το ζ ανήκει στον δακτύλιο των ακεραίων R_K του $\mathbb{Q}(\zeta)$.Οι ρίζες του $\Phi_p(X)$ είναι οι $\zeta, \zeta^2, ..., \zeta^{p-1}$, άρα

$$\Phi_p(X) = \prod_{i=1}^{p-1} (X - \zeta^i)$$

ειδικά, p = $\Phi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta^i)$. Σε αυτό το σημείο παρατηρούμε ότι τα στοιχεία $1 - \zeta, 1 - \zeta^2, ..., 1 - \zeta^{p-1}$ είναι συνεταιρικά. Πράγματι, αν $1 \leq i, j \leq p - 1$ υπάρχει ακέραιος k τέτοιος ώστε $j \equiv ik \pmod{p}$, άρα

$$\frac{1 - \zeta^j}{1 - \zeta^i} = \frac{1 - \zeta^{ik}}{1 - \zeta^i} = 1 + \zeta^i + \zeta^{2i} + ... + \zeta^{(k-1)p} \in R_K.$$

Ομοίως, $\frac{1-\zeta^i}{1-\zeta^j} \in R_K$, οπότε $1 - \zeta^i = u_i(1 - \zeta)$, όπου το u_i είναι αντιστρέψιμο στοιχείο του R_K. Συμπεραίνουμε ότι $p = u(1 - \zeta)^{p-1}$ όπου $u = u_1...u_{p-1}$ είναι αντιστρέψιμο στοιχείο του R_K.

Το στοιχείο $\xi = 1 - \zeta$ είναι ρίζα του πολυωνύμου

$$\Phi_p(X+1) = (X+1)^{p-1} + (X+1)^{p-2} + ... + 1 = X^{p-1} + a_{p-2}X^{p-2} + ... + p$$

, για κάποια $a_i \in \mathbb{Z}$. Επομένως $N_{K/\mathbb{Q}}(\xi) = (-1)^{\frac{p-1}{2}}p$ και $N_{K/\mathbb{Q}}(< (1-\zeta) >) = |N_{K/\mathbb{Q}}(1-\zeta)| = p \in \mathbb{P}$. Άρα, το $< (1-\zeta) >$ είναι πρώτο ιδεώδες του R_K.

Πόρισμα 1. *Ο p διακλαδίζεται πλήρως στην επέκταση $\mathbb{Q}(\zeta_p)/\mathbb{Q}$*

Πρόταση 3.1.1. *Ο R_K είναι μία ελεύθερη αβελιανή ομάδα με βάση $1, \zeta, \zeta^2, ..., \zeta^{p-2}$, άρα $R_K = \mathbb{Z}[\zeta]$.*

Απόδειξη. Τα στοιχεία $1, \zeta, ..., \zeta^{p-2}$ είναι γραμμικά ανεξάρτητα πάνω από το $\mathbb{Q}$, διότι αλλιώς το ζ θα ήταν ρίζα ενός πολυωνύμου βαθμού το πολύ p-2 , κάτι που αντιφάσκει στο γεγονός ότι το Φ_p είναι το ελάχιστο πολυώνυμό του.

Άν $x \in R_K$, τότε υπάρχουν μοναδικοί ρητοί αριθμοί $a_o, a_1, ..., a_{p-2}$ τέτοιοι ώστε

$$x = a_0 + a_1\zeta + a_2\zeta^2 + ... + a_{p-2}\zeta^{p-2}. \tag{3.1}$$

Θα αποδείξουμε ότι τα a_i ανήκουν στο $\mathbb{Z}$.

Έχουμε ότι $x\zeta = a_o\zeta + a_1\zeta^2 + ... + a_{p-2}\zeta^{p-1}$ και αφαιρώντας τη σχέση 3.1:

$$x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta - \zeta^2) + ... + a_{p-2}(\zeta^{p-2} - \zeta^{p-1}).$$

Παρατηρούμε ότι τα ίχνη (στην επέκταση $\mathbb{Q}(\zeta)|\mathbb{Q}$) των $\zeta, \zeta^2, ..., \zeta^{p-1}$ είναι ίσα(αφού αυτά τα στοιχεία είναι συζυγή), επομένως $Tr(a_i(\zeta^i - \zeta^{i+1})) = 0$, για κάθε $i = 1, 2, ...p-2$. Οπότε

$$Tr(x(1-\zeta)) = Tr(a_0(1-\zeta)) = a_0Tr(1-\zeta) = a_0[(p-1)+1] = a_0p.$$

Για να δείξουμε ότι $a_0 \in \mathbb{Z}$, θα υπολογίσουμε το $Tr(x(1-\zeta))$.
Έστω $x_1 = x, x_2, ..., x_{p-1} \in R_K$ οι συζυγείς του x, άρα

$$\begin{aligned} Tr(x(1-\zeta)) &= x_1(1-\zeta) + x_2(1-\zeta^2) + ... + x_{p-1}(1-\zeta^{p-1}) \\ &= (1-\zeta)x' \in (1-\zeta)R_K, \end{aligned}$$

αφού $\frac{1-\zeta^{i+1}}{1-\zeta} = 1 + \zeta + ... + \zeta^i \in R_K$. Όμως $Tr(x(1-\zeta)) \in R_K \cap \mathbb{Q} = \mathbb{Z}$, άρα $Tr(x(1-\zeta)) \in (1-\zeta)R_K \cap \mathbb{Z} = p\mathbb{Z}$, δηλαδή $a_0 \in \mathbb{Z}$.

Τώρα με επαγωγή θα δείξουμε ότι και τα $a_1, a_2, ..., a_{p-2} \in \mathbb{Z}$. Για να δείξουμε ότι $a_j \in \mathbb{Z}$, πολλαπλασιάζουμε με ζ^{p-j} την 3.1 και έχουμε

$$x\zeta^{p-j} = a_0\zeta^{p-j} + a_1\zeta^{p-j+1} + ... + a_{j-1}\zeta^{p-1} + a_j + a_{j+1}\zeta + ... + a_{p-2}\zeta^{p-j-2},$$

και εκφράζοντας το ζ^{p-1} σε μικρότερες δυνάμεις του ζ, μπορούμε να γράψουμε το $x\zeta^{p-j}$ στη μορφή

$$x\zeta^{p-j} = (a_j - a_{j-1}) + a'_1\zeta + a'_2\zeta^2 + ... + a'_{p-2}\zeta^{p-2}.$$

Από επαγωγή $a_{j-1} \in \mathbb{Z}$, οπότε με το ίδιο επιχείρημα με πριν, $a_j - a_{j-1} \in \mathbb{Z}$, άρα $a_j \in \mathbb{Z}$. □

Πρόταση 3.1.2. *Η διακρίνουσα της επέκτασης $K|\mathbb{Q}$ ισούται με*

$$\delta = (-1)^{\frac{p-1}{2}} p^{p-2}$$

Απόδειξη. Από την Πρόταση 3.1.1 έχουμε ότι η $1, \zeta, ..., \zeta^{p-2}$ είναι μια βάση ακεραιότητας του $\mathbb{Q}(\zeta)$.
Το ελάχιστο πολυώνυμο του ζ πάνω απο το $\mathbb{Q}$ είναι το $p-$οστό κυκλοτομικό πολυώνυμο $\Phi_p(X) = X^{p-1} + X^{p-2} + ... + X + 1$. Γνωρίζουμε ότι:

$$\delta = discr(\Phi_p) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi'_p(\zeta))$$

όπου Φ'_p η παράγωγος του Φ_p. Όμως $x^p - 1 = (x-1)\Phi_p(X)$, οπότε παραγωγίζοντας, $pX^{p-1} = \Phi_p(X) + (x-1)\Phi'_p(X)$, άρα για κάθε ρίζα ζ^j του Φ_p (για $j = 1, 2, ..., p-1$), έχουμε $p(\zeta^j)^{p-1} = (\zeta^j - 1)\Phi'_p(\zeta^j)$.

Τώρα, $N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi'_p(\zeta)) = \prod_{i=1}^{p-1} \Phi'_p(\zeta^j)$, άρα υπολογίζουμε

$$\prod_{j=1}^{p-1} \zeta^j = N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\zeta) = (-1)^{p-1} = 1$$

$$\prod_{j=1}^{p-1} (\zeta^j - 1) = \prod_{j=1}^{p-1} (1 - \zeta^j) = \Phi_p(1) = p$$

οπότε,

$$N_{\mathbb{Q}(\zeta)|\mathbb{Q}}(\Phi'_p(\zeta)) = \frac{p^{p-1}}{p} = p^{p-2}$$

συνεπώς

$$\delta = (-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$$

αφού $\frac{(p-1)(p-2)}{2} \equiv \frac{p-1}{2} \pmod 2$.

□

Στις δύο προηγούμενες προτάσεις προσδιορίσαμε τον δακτύλιο των ακεραίων και την διακρίνουσσα του κυκλοτομικού σώματος $K = \mathbb{Q}(\zeta)$, όπου ζ μία πρωταρχική p-ρίζα της μονάδας και p περιττός πρώτος.

Τώρα θα επεκτείνουμε αυτά τα αποτελέσματα. Έστω λοιπόν $m = p^k > 2$, όπου p πρώτος αριθμός, $k \geq 1$, $K = \mathbb{Q}(\zeta)$, με ζ μία πρωταρχική $m-$οστή ρίζα της μονάδας. Εδώ επιτρέπεται ο $p = 2$, αλλά τότε $k \geq 1$.

Παρατηρούμε ότι αν $\mu = \varphi(p^k)$ τότε το σύνολο $\{1, \zeta, \zeta^2, ..., \zeta^{\mu-1}\}$ είναι μία $\mathbb{Q}$- βάση του K και φυσικά $\mathbb{Z}[\zeta] \subset R_K$.

Η $K/\mathbb{Q}$ είναι επέκταση Galois βαθμού $\varphi(p^k) = p^{k-1}(p-1)$ και η ομάδα Galois της είναι ισόμορφη με την πολλαπλασιαστική ομάδα $P(p^k)$ των πρώτων κλάσεων υπολοίπων modulo p^k.

Το ελάχιστο πολυώνυμο του ζ είναι το p^k-οστό κυκλοτομικό πολυώνυμο

$$\Phi_{p^k}(X) = \prod_{a \in P(p^k)} (X - \zeta^a).$$

Παρατηρούμε ότι αν a, b είναι μη μηδενικοί ακέραιοι, σχετικώς πρώτοι με το p^k, τότε $1-\zeta^a, 1-\zeta^b$ είναι συνεταιρικά στον R_K. Πράγματι, γράφοντας $b \equiv aa' \pmod{p^k}$ και $a \equiv bb' \pmod{p^k}$ έχουμε ότι

$$\frac{1-\zeta^b}{1-\zeta^a} = \frac{1-\zeta^{aa'}}{1-\zeta^a} = 1 + \zeta^a + \zeta^{2a} + ... + \zeta^{(a'-1)a} \in R_K$$

και ομοίως $[\frac{1-\zeta^a}{1-\zeta^b}] \in R_K$.

Πρόταση 3.1.3. *Έστω $\xi := 1 - \zeta$. Τότε $p = u\xi^{\varphi(p^k)}$, όπου $u \in (R_K)^*$. Το κύριο ιδεώδες ξR_K είναι πρώτο και $pR_K = (\xi R_K)^{\varphi(p^k)}$.*

Απόδειξη. Από τη σχέση $p = \Phi_{p^k}(1) = \prod_{a \in P(p^k)} (1 - \zeta^a)$ και την παραπάνω παράγραφο ;; έπεται ότι $p = u\xi^{\phi(p^k)}, u \in (R_K)^*$. Οπότε $pR_K = (\xi R_K)^{\varphi(p^k)}$. Παίρνοντας νόρμες έχουμε ότι $p^{\varphi(p^k)} = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(pR_K) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi)^{\varphi(p^k)}$, οπότε $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi R_K) = p$, δηλαδή το ξR_K είναι πρώτο ιδεώδες. □

Πρόταση 3.1.4. *$R_K = \mathbb{Z}[\zeta]$, οπότε $\{1, \zeta, \zeta^2, ..., \zeta^{\mu-1}\}$ είναι μια βάση ακεραιότητας. Επιπλέον*

$$\delta_{\mathbb{Q}} = (-1)^{\frac{\varphi(p^k)}{2}} p^{p^{k-1}[k(p-1)-1]}$$

Απόδειξη. Αρχικά θα υπολογίσουμε την διακρίνουσα $d = discr_{K|\mathbb{Q}}(1, \zeta, ..., \zeta^{\mu-1})$. Γνωρίζουμε ότι $d = (-1)^{\frac{\mu(\mu-1)}{2}} N_{K|\mathbb{Q}}(\Phi'_m(\zeta))$, όπου $\Phi_m(X) \in \mathbb{Z}[X]$ είναι το $m-$οστό κυλοτομικό πολυώνυμο. Όμως,

$$X^m - 1 = (X^{\frac{m}{p}} - 1)\Phi_m(X)$$

οπότε

$$mX^{m-1} = \frac{m}{p} X^{\frac{m}{p}-1}\Phi_m(X) + X^{\frac{m}{p}-1}\Phi'_m(X)$$

και για $X = \zeta$ έχουμε

$$m\zeta^{m-1} = \zeta^{\frac{m}{p}-1}\Phi'_m(\zeta)$$

Θεωρώντας τους συζυγείς της παραπάνω σχέσης και παίρνοντας το γινόμενο τους έχουμε ότι :

$$m^{\mu}(\prod_{a\in P(m)} \zeta^a)^{m-1} = \prod_{a\in P(m)} (\zeta^{ap^{k-1}} - 1) \prod_{a\in P(m)} \Phi'_m(\zeta^a)$$

Όμως

$$\prod_{a\in P(m)} \zeta^a = N_{K|\mathbb{Q}}(\zeta) = (-1)^{\mu} \cdot 1 = 1$$

και

$$\prod_{a\in P(m)} (\zeta^{ap^{k-1}} - 1) = \prod_{a\in P(m)} (1 - \zeta^{ap^{k-1}}) = p^{p^{k-1}}$$

διότι $\zeta^{p^{k-1}}$ είναι πρωταρχική $p-$ρίζα της μονάδας, $\prod_{a\in P(p)} (1-\zeta^a) = \Phi_p(1) = p$ και ένα σύστημα αντιπροσώπων των πρώτων κλάσεων modulo $m = p^k$ δίνει p^{k-1} συστήματα αντιπροσώπων των πρώτων κλάσεων modulo p. Δηλαδή, υπολογίζοντας την norm και των δύο μελών,

$$m^{\mu} = p^{p^{k-1}} N_{K|\mathbb{Q}}(\Phi'_m(\zeta))$$

οπότε $d = (-1)^{\frac{\mu\mu-1}{2}} p^{p^{k-1}[k(p-1)-1]}$ άρα

$$d = (-1)^{\frac{\mu(\mu-1)}{2}} p^{p^{k-1}[k(p-1)-1]}$$

και λόγω του ότι $\frac{\mu(\mu-1)}{2} \equiv \frac{\mu}{2} \pmod 2$ έχουμε $d = (-1)^{\frac{\mu}{2}} p^{p^{k-1}[k(p-1)-1]}$.

Για να δείξουμε ότι $\mathbb{Z}[\zeta] = R_K$, θεωρούμε τυχαίο $x \in R_K$. Τότε το x γράφεται με μοναδικό τρόπο ως

$$x = x_0 + x_1\zeta + x_2\zeta^2 + ... + x_{\mu-1}\zeta^{\mu-1} \tag{3.2}$$

, όπου $x_i \in \mathbb{Q}$ για $i = 0, ..., \mu - 1$. Αν δείξουμε ότι $x_i \in \mathbb{Z}, \forall i = 0, ..., \mu - 1$ τότε $R_K \subseteq \mathbb{Z}[\zeta]$.

Ισχυρισμός 1. *Αν $q \in \mathbb{P}$ και $x \in qR_K$ τότε $x_i \in q\mathbb{Z}$.*

Αν υποθέσουμε τον ισχυρισμό τότε προκύπτει το ζητούμενο. Πράγματι, αν $x_i = \frac{a_i}{b_i}, a_i, b_i \in \mathbb{Z}$ και $(a_i, b_i) = 1$, θεωρούμε $l :=$εκπ$(b_0, b_1, ..., b_{\mu-1})$. Τότε $l = b_i l'_i$, για κάποια $l'_i \in \mathbb{Z}$, $i = 0, 1, ..., \mu - 1$.

Έστω q πρώτος, με $q^r \mid\mid l, r \geq 1$. Επομένως $q^r \mid\mid b_j$, για κάποιο $j \in \{0, 1, ..., \mu - 1\}$ και $q \nmid l'_j$, διότι αλλιώς $q^{r+1} \mid l$, άτοπο. Γράφουμε το l ως $l = q^r l'$ και έχουμε

$$lx = \sum_{i=0}^{\mu-1} l(\frac{a_i}{b_i}\zeta^i) = \sum_{i=0}^{\mu-1} (l'_i a_i)\zeta^i = (l'x)q^r \in q^r R_K \subseteq qR_K \tag{3.3}$$

οπότε λόγω του ισχυρισμού $q \mid a_i l'_i, \forall i = 0, 1, ..., \mu - 1$. Επομένως $q \mid a_j l'_j \Rightarrow q \mid a_j$, άτοπο. Άρα $l = 1$ και $x_i \in \mathbb{Z}$.

Λόγω της σχέσης (3) και επειδή $a_i l'_i \in \mathbb{Z}$ αρκεί να αποδειξούμε τον ισχυρισμό με την επιπλέον υπόθεση ότι $x_i \in \mathbb{Z}$. Θεωρώντας τους συζυγείς της σχέσης (2) στην επέκταση $K/\mathbb{Q}$ παίρνουμε μ σχέσεις

$$\sigma_i(x) = \sum_{j=0}^{\mu-1} x_j \sigma_i(\zeta^j)$$

, για $i = 1, ..., \mu$. Άρα η $(x_0, x_1, ..., x_{\mu-1})$ είναι μια λύση του συστήματος των γραμμικών εξισώσεων με συντελεστές $\sigma_i(\zeta^j) \in R_K$, όπου $i \in \{1, ..., \mu\}, j \in \{0, .., \mu - 1\}$ και ορίζουσας της οποίας το τετράγωνο ισούται με

$$[det(\sigma_i(\zeta^j))]^2 = discr_{K/\mathbb{Q}}(1, \zeta, \zeta^2, ..., \zeta^{\mu-1}) = d.$$

Έστω c_j να είναι η ορίζουσα του $\mu \times \mu$ πίνακα $\sigma_i(\zeta^j)$ όταν αντικαταστήσουμε την $j-$ στήλη με την $\sigma_1(x), ..., \sigma_\mu(x) \in R_K$. Επομένως $c_j \in R_K$ και από τον κανόνα Cramer ([18]) προκύπτει ότι $dx_j = c_j\sqrt{d} \in R_K \cap \mathbb{Q} = \mathbb{Z}$.

Αν $q \neq p$ τέτοιος ώστε $x \in qR_K$, τότε $x = qy$, για κάποιο $y \in R_K$. Το y γράφεται με μοναδικό τρόπο στη μορφή

$$y = y_0 + y_1\zeta + y_2\zeta^2 + ... + y_{\mu-1}\zeta^{\mu-1}, y_i \in \mathbb{Q}.$$

Οπότε $x_j = qy_j, \forall j = 0, 1, ..., \mu-1 \Rightarrow dx_j = dy_j q$ με $dy_j \in \mathbb{Z}, \forall j = 0, 1, ..., \mu-1$, σύμφωνα με αυτά που αποδείξαμε προηγουμένως. Τότε $q \mid dx_j$ και εφόσον $q \nmid d$ (= δύναμη του p) έχουμε $q \mid x_j$, δηλαδή $x_j \in q\mathbb{Z}, \forall j = 0, 1, ..., \mu - 1$.

Μένει να αποδείξουμε τον ισχυρισμό για τον πρώτο p. Δηλαδή ότι αν $x \in pR_K$ τότε $x_i \in p\mathbb{Z} \forall i = 0, 1, ..., \mu - 1$. Έστω $h(X) = x_0 + x_1X + x_2X^2 + ... + x_{\mu-1}X^{\mu-1}$, αν $\xi := 1 - \zeta$ τότε

$$x = h(\zeta) = h(1 - \xi) = h(1) - \xi h'(1) + \xi^2\frac{h''(1)}{2!} - \xi^3\frac{h'''(1)}{3!} + ... + (-1)^{\mu-1}\frac{h^{(\mu-1)}(1)}{(\mu-1)!}$$

Οι συντελεστές $\frac{h^k(1)}{k!}$ είναι ακέραιοι, τους οποίους μπορούμε να υπολογίσουμε :

$$\frac{h^{(\mu-1)}(1)}{(\mu-1)!} = x_{\mu-1}$$

$$\frac{h^{(\mu-2)}(1)}{(\mu-2)!} = x_{\mu-2} + (\mu-1)x_{\mu-1}$$

$$\frac{h^{(\mu-3)}(1)}{(\mu-3)!} = x_{\mu-3} + (\mu-2)x_{\mu-2} + \binom{\mu-1}{2}x_{\mu-1}$$

$$\frac{h''(1)}{2!} = x_2 + \binom{3}{2}x_3 + ... + \binom{k}{2}x_k + ... + \binom{\mu-1}{2}x_{\mu-1}$$

$$\frac{h'(1)}{1!} = x_1 + 2x_2 + ... + (\mu-1)x_{\mu-1}$$

$$h(1) = x_0 + x_1 + ... + x_{\mu-1}$$

Γνωρίζουμε ότι $p = u\xi^\mu$ (πρόταση 3.1.3) και $x \in pR_K \subseteq \xi R_K \Rightarrow h(1) \in \xi R_K$. Άρα $h(1) \in \xi R_K \cap \mathbb{Z} = p\mathbb{Z}$. Όμως $\mu > 1$, άρα $\frac{p}{\xi} = u\xi^{\mu-1} \in \xi R_K$ και

$$\frac{p}{\xi} \mid \frac{-x - h(1)}{\xi} = h'(1) - \xi\frac{h''(1)}{2!} + ... + (-1)^{\mu-1}\frac{h^{\mu-1}(1)}{(\mu-1)!}$$

άρα $h'(1) \in_K \cap\mathbb{Z} = p\mathbb{Z}$ και $p \mid h'(1)$. Συνεχίζοντας με τον ίδιο τρόπο δείχνουμε ότι ο p διαιρεί τα $\frac{h''(1)}{2!}, \frac{h'''(1)}{3!}, ..., \frac{h^{\mu-1}}{(\mu-1)!}$. Άρα $p \mid x_{\mu-1}, p \mid x_{\mu-2} + (\mu-1)x_{\mu-1} \Rightarrow p \mid x_{\mu-2}$. Ομοίως $p \mid x_{\mu-3}, ..., p \mid x_0$ □

Πρόταση 3.1.5. *Έστω K_1, K_2 αλγεβρικά σώματα αριθμών βαθμού n_1, n_2 αντίστοιχα πάνω από το $\mathbb{Q}$ τέτοια ώστε $(\delta_{K_1}, \delta_{K_2}) = 1$.*

Αν $L := K_1K_2$ τότε :
(1) $[L : \mathbb{Q}] = n_1n_2$
(2) $\delta_L = {\delta_{K_1}}^{n_2}{\delta_{K_2}}^{n_1}$
(3) $R_L = R_{K_1}R_{K_2}$.
(χωρίς απόδειξη)

Θεωρούμε το κυκλοτομικό σώμα $\mathbb{Q}(\zeta)$ που παράγεται από μια $m-$ οστή ρίζα της μονάδας ζ, όπου $m > 2, m \in \mathbb{Z}$.

Πρόταση 3.1.6. *Με τις παραπάνω υποθέσεις*

$$(1) \qquad \delta_{\mathbb{Q}(\zeta)} = (-1)^{s\frac{\varphi(m)}{2}} \frac{m^{\varphi(m)}}{\prod_{q|m} q^{\frac{\varphi(m)}{q-1}}}$$

$$(2) \qquad R_K = \mathbb{Z}[\zeta]$$

Απόδειξη. (1) Η απόδειξη θα γίνει με επαγωγή. Από (Πρόταση 3.1.4), το (1) ισχύει για $s = 1$. Υποθέτουμε ότι ισχύει για $s-1$.

Έστω p ένας πρώτος που διαιρεί το m και $m = p^km'$, όπου $k \geq 1$ και $p \nmid m'$. Τότε υπάρχουν ακέραιοι a, b τέτοιοι ώστε $1 = ap^k + bm'$ και $\zeta = \zeta^{ap^k}\zeta^{bm'}$, με $(\zeta^{ap^k})^{m'} = 1$ και $(\zeta^{bm'})^{p^k} = 1$. Οπότε αν ξ είναι μια πρωταρχική $m'-$ ρίζα της μονάδας και η μια πρωταρχική p^k- ρίζα της μονάδας τότε ζ^{ap^k} είναι μια δύναμη του ξ, $\zeta^{bm'}$ είναι μια δύναμη του η και συμπεραίνουμε ότι $\mathbb{Q}(\zeta) = \mathbb{Q}(\xi)\mathbb{Q}(\eta)$. Από επαγωγή οι $\delta_{\mathbb{Q}(\xi)}, \delta_{\mathbb{Q}(\eta)}$ είναι σχετικώς πρώτες. Χρησιμοποιώντας την πρόταση 3.1.5 έχουμε

$$\delta_{\mathbb{Q}(\zeta)} = {\delta_{\mathbb{Q}(\xi)}}^{\varphi(p^k)}{\delta_{\mathbb{Q}(\eta)}}^{\varphi(m')} = (-1)^{s-1[\frac{\varphi(m')}{2}]\varphi(p^k)} \frac{{m'}^{\varphi(m')\varphi(p^k)}}{\prod_{q|m} q^{[\frac{\varphi(m')}{q-1}]\varphi(p^k)}} \times$$
$$\times (-1)^{[\frac{\varphi(p^k)}{2}]\varphi(m')} \frac{p^{\varphi(p^k)\varphi(m')}}{p^{[\frac{p^{\varphi(p^k)}}{p-1}]\varphi(m')}} = (-1)^{[\frac{\varphi(m)}{2}s]} \frac{m^{\varphi(m)}}{\prod_{q|m} q^{\frac{\varphi(m)}{q-1}}}.$$

(2) Από επαγωγή έχουμε ότι $R_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi]$ και $R_{\mathbb{Q}(\eta)} = \mathbb{Z}[\eta]$. Λόγω της (Πρόταση 3.1.5) έχουμε $R_K = R_{\mathbb{Q}(\eta)}R_{\mathbb{Q}(\xi)} = \mathbb{Z}[\xi, \eta] = \mathbb{Z}[\zeta]$. □

Κεφάλαιο 4

Θεωρία διακλαδώσεως πρώτων ιδεωδών σε επεκτάσεις Galois

4.1 Ομάδες ανάλυσης και αδράνειας

Έστω K αλγεβρικό σώμα αριθμών, $L|K$ πεπερασμένη επέκταση βαθμού n. Άν P είναι πρώτο ιδεώδες του δακτυλίου R_K , τότε έστω $PR_L = \prod_{i=1}^{r} Q_i^{e_i}$ η ανάλυση του PR_L σε πρώτα ιδεώδη του R_L, με $f_i = [R_L/Q_i : R_K/P]$.

Υποθέτουμε ότι η $L|K$ είναι επέκταση του $Galois$ και έστω $G = Gal(L|K)$, οπότε η G έχει n στοιχεία, τους $K-$ αυτομορφισμούς του L. Γνωρίζουμε ότι $e := e_1 = ... = e_r$, $f := f_1 = ... = f_r$. Θα υιοθετήσουμε τους ακόλουθους συμβολισμούς : $\overline{K} = R_K/P, \overline{L_i} = R_L/Q_i$.

Ορισμός 4.1.1. *Η υποομάδα G_{Z_i} της G, που ορίζεται ως*

$$G_{Z_i} = G_Z(Q_i|P) = \{\sigma \in G | \sigma(Q_i) = Q_i\}$$

θα λέγεται ***ομάδα ανάλυσης*** *του Q_i στην επέκταση $L|K$. Το σώμα των σταθερών στοιχείων της G_{Z_i} θα συμβολίζεται με $K_{Z_i} = K_Z(Q_i|P)$ και θα λέγεται σώμα ανάλυσης του Q_i στην επέκταση $L|K$.*

Πρόταση 4.1.1. *Οι υποομάδες $G_{Z_1}, ..., G_{Z_r}$ της G είναι συζυγείς. Δηλαδή αν η G είναι αβελιανή ομάδα, τότε $G_{Z_1} = ... = G_{Z_r}$*

Απόδειξη. Έστω Q_i, Q_j να είναι διαφορετικά πρώτα ιδεώδη του S τέτοια ώστε $Q_i \cap R_K = Q_j \cap R_K = P$. Αφού η G δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών $\{Q_1, ..., Q_r\}$, υπάρχει $\sigma \in G$ τέτοιο ώστε $\sigma(Q_i) = Q_j$. Τότε $G_{Z_i} = \sigma^{-1} G_{Z_j} \sigma$. □

Πρόταση 4.1.2. *Για κάθε $i = 1, ..., r$ έχουμε : $[K_{Z_i} : K] = (G : G_{Z_i}) = r$.*

Απόδειξη. Έχουμε ότι $\sigma G_{Z_i} = \tau G_{Z_i}$, όπου $\sigma, \tau \in G$ αν και μόνο αν $\sigma(Q_i) = \tau(Q_i)$. Πράγματι, αν $\sigma G_{Z_i} = \tau G_{Z_i}$, τότε $\sigma^{-1}\tau \in G_{Z_i}$, οπότε $\sigma^{-1}\tau(Q_i) = Q_i$, δηλαδή $\sigma(Q_i) = \tau(Q_i)$. Αντίστροφα αν $\sigma(Q_i) = \tau(Q_i)$ τότε $\sigma^{-1}\tau \in G_{Z_i}$ άρα $\tau G_{Z_i} = \sigma G_{Z_i}$.

Άρα ο αριθμός r των διαφορετικών πρώτων ιδεωδών Q_i ισούται με τον αριθμό των διαφορετικών συμπλόκων modulo G_{Z_i}, δηλαδή $r = (G : G_{Z_i})$. Και από θεωρία Galois έχουμε $(G : G_{Z_i}) = [K_{Z_i} : K]$. □

Πρόταση 4.1.3. *Αν K' σώμα με $K \subseteq K' \subseteq L$ και $Q \in Spec(R_L)$ τότε*

$$G_Z(Q|Q \cap R_{K'}) = G_Z(Q|Q \cap R_K) \cap Gal(L/K').$$

Το σώμα ανάλυσης έχει την ακόλουθη σχέση ελαχιστικότητας :

Πρόταση 4.1.4. *Άν $J_i = Q_i \cap K_{Z_i}$ (το οποίο είναι ένα πρωτο ιδεώδες του δακτυλίου των ακεραίων$R_{K_{Z_i}}$ του K_{Z_i}), τότε το Q_i είναι το μόνο ιδεώδες του R_L που επεκτείνει το J_i.*
Αντίστροφα, αν K' είναι ένα σώμα με $K \subset K' \subset L$, τότε αν $J_i' = Q_i \cap R_{K'}$ και Q_i είναι η μοναδική επέκταση του J_i' στο L, τότε $K_{Z_i} \subset K'$.

Απόδειξη. Έχουμε ότι $G_{Z_i} = Gal(L|K_{Z_i})$. Η G_{Z_i} δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών του R_L που επεκτείνουν το J_i, όμως εξ ορισμού $\sigma(Q_i) = Q_i$ για κάθε $\sigma \in G_{Z_i}$, άρα το Q_i είναι η μοναδική επέκταση του J_i.

Έπειτα, αν Q_i είναι η μόνη επέκταση του $J_i' = Q_i \cap R_{K'}$, τότε κάθε στοιχείο της ομάδας Galois $G' = Gal(L|K')$ στέλνει το Q_i στο Q_i, δηλαδή ανήκει στη G_{Z_i}. Άρα τα σώματα των σταθερών στοιχείων ικανοποιούν τον αντίστροφο εγκλεισμό : $K_{Z_i} \subset K'$. □

Τώρα εστιάζουμε την προσοχή μας σε ένα από τα πρώτα ιδεώδη Q_i, το οποίο θα συμβολίζουμε Q για απλότητα.

Έστω $K_Z = K_Z(Q|P), G_Z = G_Z(Q|P), \bar{L} = R_L/Q, \bar{G} = Gal(\bar{L}|\bar{K})$. Συμβολίζουμε με $Q_{K_Z} := Q \cap K_Z$ (πρώτο ιδεώδες του R_{K_Z}) και $\bar{K_Z} = R_{K_Z}/Q_{K_Z}$. Επίσης θα συμβολίζουμε με e τον δείκτη διακλάδωσης και με f τον βαθμό αδρανείας του Q πάνω από το P.

Πρόταση 4.1.5. ***(1)*** *$\bar{K} = \bar{K_Z}$, οπότε οι βαθμοί αδρανείας είναι $f(Q_{K_Z}|P) = 1$, $f(Q|Q_{K_Z}) = f$ και οι δείκτες διακλάδωσης είναι $e(Q|Q_{K_Z}) = e$, $e(Q_{K_Z}|Q) = 1$.*

(2) *Η απεικόνιση $\sigma \in G_Z \to \bar{\sigma} \in \bar{G} = Gal(\bar{L}|\bar{K})$ είναι επιμομορφισμός ομάδων και ο πυρήνας του ισούται με*

$$G_T = \{\sigma \in G_Z | \sigma(x) \equiv x \pmod{Q}, \forall x \in R_L\}$$

Απόδειξη. **(1)** Από Πόρισμα 1.2.2 και λόγω της Πρότασης 4.1.4 έχουμε ότι :

$$[L : K_Z] = e(Q|Q_{K_Z}) f(Q|Q_{K_Z}).$$

Από την άλλη μεριά, $[L : K] = efr$ και από την πρόταση 4.1.2, $[K_Z : K] = r$. Οπότε $ef = e(Q|Q_{K_Z}) f(Q|Q_{K_Z})$. Λόγω της μεταβατικότητας των βαθμών αδρανείας και των δεικτών διακλάδωσης προκύπτει ότι $e(Q|Q_{K_Z}) = e, f(Q|Q_{K_Z}) = f$ και $e(Q_{K_Z}|P) = 1, f(Q_{K_Z}|P) = 1$. Άρα

$$[\bar{L} : \bar{K_Z}] = f(Q|Q_{K_Z}) = f = [\bar{L} : \bar{K}] \Rightarrow \bar{K} = \bar{K_Z} \tag{4.1}$$

(2) Άν $\sigma \in G_Z$ τότε $\sigma(Q) = Q$, οπότε ο σ επάγει μια απεικόνιση $\bar{\sigma} : \bar{L} \to \bar{L}$, που ορίζεται ως $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$, για κάθε $x \in R_L$. Ο $\bar{\sigma}$ είναι $\bar{K_Z}$- αυτομορφισμός. Πράγματι, αρχικά θα δείξουμε ότι η απεικόνιση $\bar{\sigma}$ είναι καλά ορισμένη. Έστω λοιπόν $\bar{x} = \bar{y} \in \bar{L}(= R_L/Q) \Rightarrow x - y \in Q \Rightarrow \sigma(x - y) \in Q (\sigma \in G_Z) \Rightarrow \overline{\sigma(x - y)} = \bar{0} \Rightarrow \overline{\sigma(x)} = \overline{\sigma(y)}$.
Ο $\bar{\sigma}$ είναι ομομορφισμός δακτυλίων : αν $\bar{x} = \bar{y} \Rightarrow \bar{\sigma}(\bar{x} + \bar{y}) = \bar{\sigma}(\overline{x + y}) = \overline{\sigma(x + y)} = \overline{\sigma(x) + \sigma(y)} = \overline{\sigma(x)} + \overline{\sigma(y)} = \bar{\sigma}(\bar{x}) + \bar{\sigma}(\bar{y})$.
$\bar{\sigma}(\bar{x}\bar{y}) = \bar{\sigma}(\overline{xy}) = \overline{\sigma(xy)} = \overline{\sigma(x)\sigma(y)} = \overline{\sigma(x)}\overline{\sigma(y)} = \bar{\sigma}(\bar{x})\bar{\sigma}(\bar{y})$.
Ο $\bar{\sigma}$ είναι $1-1$ αφού $\bar{L}$ είναι σώμα και προφανώς είναι επί. Έστω τώρα $\bar{x} \in \overline{K_Z}$ τότε $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)} = \bar{x}$, αφού $x \in K_Z = \{x \in L | \sigma(x) = x$, για κάθε $\sigma \in G_Z\}$.Άρα $\bar{\sigma} \in Gal(\bar{L}|\overline{K_Z}) = Gal(\bar{L}|\bar{K})$, όπου η τελευταία ισότητα προκύπτει από το (1).

Τώρα θα αποδείξουμε ότι η εικόνα ισούται με $Gal(\bar{L}|\bar{K})$. Αφού το $\bar{K}$ είναι πεπερασμένο σώμα υπάρχει $s \in R_L$ τέτοιο ώστε $\bar{L} = \bar{K}(\bar{s})$. Άν $\xi \in Gal(\bar{L}|\bar{K})$ τότε $\xi(\bar{s})$ είναι συζυγής του $\bar{s}$ πάνω από το $\bar{K}$.

Έστω $h(X)$ να είναι το ελάχιστο πολυώνυμο του s πάνω από το K_Z. Επειδή η $L|K_Z$ είναι επέκταση $Galois$ όλοι οι συζυγείς του s πάνω απο το K_Z ανήκουν στο L και μάλιστα στο R_L (αφού $s \in R_L$). Άρα το h αναλύεται ως $h(X) =$

$\prod_{\sigma\in G_Z}(X-\sigma(s))$. Θεωρώντας τώρα τις εικόνες των συντελεστών του h μέσω της απεικόνισης $R_L \to R_L/Q = \bar{L}$(η οποία επεκτείνει την $R_{K_Z} \to R_{K_Z}/Q_{K_Z} = \bar{K}_Z = \bar{K}$) παίρνουμε ότι $\overline{h(X)} = \prod_{\sigma\in G_Z}(X-\overline{\sigma(s)}) \in \bar{K}[X]$. Φυσικά το $\bar{s}$ είναι ανάμεσα στις ρίζες του $\bar{h}$.
Οι συζυγείς του $\bar{s}$ πάνω από το $\bar{K}$ είναι οι ρίζες του ελαχίστου πολυωνύμου $Irr(\bar{s},\bar{K})$ που διαιρεί το $\bar{h}$. Άρα οι συζυγείς του $\bar{s}$ πάνω από το $\bar{K}$ είναι ανάμεσα στα στοιχεία $\overline{\sigma(s)} \in \bar{L}$. Δηλαδή $\xi(\bar{s}) = \overline{\sigma(s)} = \bar{\sigma}(\bar{s})$, για κάποιο $\sigma \in G_Z$, αυτό συνεπάγεται ότι τα ξ και $\bar{\sigma}$ ταυτίζονται σε κάθε σημείο του Ł.

Ο πυρήνας του παραπάνω ομομορφισμού ομάδων είναι το σύνολο όλων των $\sigma \in G_Z$ τέτοιο ώστε $\bar{\sigma}(\bar{x}) = \bar{x}$ για κάθε $\bar{x} \in \bar{L}$, δηλαδή $\sigma(x) \equiv x \pmod{Q}$ για κάθε $x \in R_L$. □

Αποδείξαμε λοιπόν ότι $G_Z/G_T \cong \overline{G} = Gal(\bar{L}|\bar{K})$ για κάθε πρώτο ιδεώδες Q.

Ορισμός 4.1.2. *Για κάθε πρώτο ιδεώδες Q_i του R_L, η $G_{T_i} = \{\sigma \in G_{Z_i} | \sigma(x) \equiv x \pmod{Q_i}, \forall x \in R_L\}$ θα λέγεται ομάδα αδρανείας του Q_i στην επέκταση $L|K$. Το σώμα των σταθερών στοιχείων της G_{T_i} θα συμβολίζεται με K_{T_i} και θα λέγεται σώμα αδρανείας του Q_i στην $L|K$.*

Επίσης θα χρησιμοποιήσουμε και τους ακόλουθους συμβολισμούς:

$$G_{T_i} = G_T(Q_i|P),$$
$$K_{T_i} = K_T(Q_i|P)$$

Όταν θα εστιάζουμε την προσοχή μας σε ένα από τα πρώτα ιδεώδη Q_i, το οποίο θα συμβολίζουμε Q για απλότητα, τότε θα γράφουμε $K_T = K_T(Q|P)$ και $G_T = G_T(Q|P)$. Επίσης συμβολίζουμε με Q_{K_T} το πρώτο ιδεώδες $Q \cap R_{K_T} = Q_{K_T}$ και με $\overline{K_T} = R_{K_T}/Q_{K_T}$.

Θεώρημα 4.1.1. ***(1)*** *Η επέκταση $K_T|K_Z$ είναι Galois και $Gal(K_T|K_Z) = G_Z/G_T \cong \overline{G}$*
(2) *$[K_T : K_Z] = f, [L : K_T] = e$*
(3) *$\overline{L} = \overline{K_T}$ οπότε οι βαθμοί αδρανείας είναι*

$$f(Q_{K_T}|Q_{K_Z}) = f, f(Q|Q_{K_T}) = 1$$

(4) *$e(Q_{K_T}|Q_{K_Z}) = 1$, $e(Q|Q_{K_T}) = e$*

Απόδειξη. **(1)** Από την Πρόταση 4.1.5 η G_T είναι κανονική υποομάδα της G_Z, ως πυρήνας ομομορφισμού ομάδων και $G_Z/G_T \cong \bar{G}$. Οπότε απο το θεμελιώδες θεώρημα της θεωρίας *Galois* έχουμε ότι K_T/K_Z είναι επέκταση *Galois* και ότι $Gal(K_T|K_Z) = G_Z/G_T$.
(2) Από το **(1)** έχουμε ότι $[K_T : K_Z] = |G_Z/G_T| = |\bar{G}| = [\bar{L} : \bar{K}] = f$.
Έχουμε ότι $n = efr$, και από την Πρόταση 4.1.2, $[K_Z : K] = r$ οπότε $[L : K_T] = e$, αφού $[L : K] = [L : K_T][K_T : K_Z][K_Z : K]$.
(3) Για να δείξουμε τώρα ότι $\bar{L} = \overline{K_T}$ θεωρούμε την επέκταση $L|K_T$.

$$G_Z(Q|Q_{K_T}) = Gal(L|K_T) \cap G_Z = G_T \cap G_Z = G_T,$$
$$G_T(Q|Q_{K_T}) = Gal(L|K_T) \cap G_T = G_T \cap G_T = G_T$$

Άρα από το **(1)** παίρνουμε ότι η $Gal(\bar{L}|\overline{K_T})$ είναι τετριμμένη , δηλαδή $\bar{L} = \overline{K_T}$. Οπότε εξ ορισμού $f(Q|Q_{K_T}) = [\bar{L} : \overline{K_T}] = 1$ και λογω της μεταβατικότητας των βαθμών αδρανείας και από το (1) της Πρότασης 4.1.5 $f(Q_{K_T}|Q_{K_Z}) = f$.
(4) Θεωρούμε την επέκταση Galois $L|K_T$. Από το **(2)** και από την Πρόταση 4.1.4 έχουμε :

$$[L : K_T] = e = e(Q|Q_{K_T})f(Q|Q_{K_T})$$

όμως $f(Q|Q_{K_T}) = 1$, οπότε $e(Q|Q_{K_T}) = e$ και λόγω της μεταβατικότητας των δεικτών διακλάδωσης $e(Q_{K_T}|Q_{K_Z}) = 1$. □

4.2 Η διακλάδωση

Τώρα θα μελετήσουμε τη διακλάδωση που προκύπτει από το Θεώρημα 4.1.1 στην επέκταση $L|K_T$. Αφού $[L : K_T] = e(Q|Q_{K_T})$, το Q_{K_T} *διακλαδίζεται πλήρως* στην $L|K_T$.

Βρισκόμαστε λοιπόν στην ακόλουθη κατάσταση :

$L|K_T$ είναι επέκταση *Galois* βαθμού e με ομάδα *Galois* την G_T, το πρώτο ιδεώδες Q_{K_T} του R_{K_T} του K_T έχει μόνο μια επέκταση Q στον R_L. Άρα $Q_{K_T}R_L = Q^e$, $\bar{L} = \overline{K_T}$ και $G_Z(Q|Q_{K_T}) = G_T(Q|Q_{K_T}) = G_T$.

Λήμμα 4.2.1. *Έστω R μια περιοχή του Dedekind, K το σώμα κλασμάτων της, L/K μια επέκταση Galois πεπερασμένου βαθμού και T η ακέραια κλειστότητα της R στο L. Έστω P πρώτο ιδεώδες της R και υποθέτουμε ότι υπάρχει μοναδικό πρώτο ιδεώδες Q του T τέτοιο ώστε $Q \cap R = P$. Αν $S = R \setminus P$ και $S' = R_P, T' = S^{-1}T$ τότε $T' = T_Q$.*

Απόδειξη. Αφού $S \subseteq T \setminus Q \Rightarrow T' = S^{-1}T \subseteq T_Q$. Για να δείξουμε τον αντίστροφο εγκλεισμό αρκεί να αποδείξουμε ότι το T_Q είναι ακέραιο πάνω από τον R', λόγω του ότι T' είναι η ακέραια κλειστότητα του R' στο L.

Αν $x \in T$ τότε το x είναι ακέραιο πάνω από τον R, δηλαδή είναι ακέραιο και πάνω από τον R'. Οπότε αρκεί να δείξουμε ότι τα στοιχεία της μορφής $\frac{1}{t}$ είναι ακέραια πάνω από τον R', όπου $t \in T \setminus Q$.

Έστω $X^m + a_{m-1}X^{m-1} + ... + a_0 \in R[X]$ το ελάχιστο πολυώνυμο του t πάνω από το K. Τότε επειδή η επέκταση L/K είναι Galois και το Q είναι το μοναδικό πρώτο ιδεώδες του T με $Q \cap R = P$ έχουμε ότι κανείς από τους συζυγείς του t δεν ανήκει στο Q (Πρόταση 1.2.1). Συνεπώς $a_0 \notin R \cap Q = P$. Παρατηρούμε ότι το $\frac{1}{t}$ είναι ρίζα του πολυωνύμου

$$X^m + \frac{a_{m-1}}{a_0}X^{m-1} + \frac{a_{m-2}}{a_0}X^{m-2} + ... + 1 \in R'[X]$$

οπότε το $\frac{1}{t}$ είναι ακέραιο πάνω από τον R'. □

Πρόταση 4.2.1. *Με τις παραπάνω υποθέσεις, έστω $t \in (R_L)_Q$ ένας γεννήτορας του πρώτου ιδεώδους $Q(R_L)_Q$ του $(R_L)_Q$, δηλαδή $t(R_L)_Q = Q(R_L)_Q$, Τότε η $\{1, t, ..., t^{e-1}\}$ είναι μία βάση του ελεύθερου module $(R_L)_Q$ πάνω από το $(R_{K_T})_{Q_{K_T}}$, δηλαδή $(R_L)_Q = (R_{K_T})_{Q_{K_T}}[t]$. Επιπλέον, το t είναι ρίζα ενός Eisenstein πολυωνύμου με συντελεστές στο $(R_{K_T})_{Q_{K_T}}$.*

Απόδειξη. Αρχικά θα δείξουμε ότι αν $a \in K_T, a \neq 0$, τότε $a(R_L)_Q = Q^{se}(R_L)_Q$, για κάποιο $s \in \mathbb{Z}$.
Πράγματι, αφου $(R_{K_T})_{Q_{K_T}}$ είναι περιοχή κυρίων ιδεωδων (τοπικοποίηση του R_{K_T} που είναι δακτύλιος του *Dedekind*, [18]), υπάρχει ένα $s \in \mathbb{Z}$ τέτοιο ώστε $a(R_{K_T})_{Q_{K_T}} = {Q_{K_T}}^s(R_{K_T})_{Q_{K_T}}$, οπότε

$$\begin{aligned} a(R_L)_Q = (a(R_{K_T})_{Q_{K_T}})(R_L)_Q = ({Q_{K_T}}^s(R_{K_T})_{Q_{K_T}})(R_L)_Q = \\ = {Q^s}_{K_T}(R_L)_Q = ({Q^s}_{K_T}R_L)(R_L)_Q = Q^{se}(R_L)_Q. \end{aligned}$$

Στη συνέχεια θα δείξουμε ότι αν $x = \sum_{i=0}^{e-1} a_i t^i$, με $a_i \in K_T$ τότε αν $i, j \in \{0, ..., e-1\}$ με $i \neq j$ και $a_i, a_j \neq 0$ έχουμε ότι $s_i e + i \neq s_j e + j$ (όπου $a_i(R_L)_Q = Q^{s_i e}(R_L)_Q$). Όντως ισχύει διότι αν $s_i e + i = s_j e + j$ τότε $i - j = e(s_i - s_j)$ όμως $i - j \neq 0 \Rightarrow (s_i - s_j)e \neq 0$ και $|i - j| > e$ κάτι το οποίο είναι αδύνατον καθώς $i, j \in \{0, ..., e-1\}$.

Οπότε, αν $x = \sum_{i=0}^{e-1} a_i t^i$, με $a_i \in K_T$ και $a_i \neq 0$, για κάποιο i θεωρώντας

$$m = min\{s_i e + i | a_i \neq 0, a_i (R_L)_Q = Q^{s_i e}(R_L)_Q\}$$

έχουμε ότι $x(R_L)_Q = Q^m(R_L)_Q$.

Πράγματι, αν i είναι τέτοιο ώστε $m = s_i e + i$ τότε για κάθε $j \in \{0, 1, ..., e-1\}$ με $a_j \neq 0$ έχουμε ότι $m \leq s_j e + j$ οπότε $x \in Q^m(R_L)_Q$, αφού $a_j t^j \in Q^{s_j e + j}(R_L)_Q$ για κάθε $j \in \{0, ..., e-1\}$ και εάν $x \in Q^{m+1}(R_L)_Q$ τότε $a_i t^i = x - \sum_{i \neq j} a_j t^j \in Q^{m+1}(R_L)_Q$, άρα $a_i t^i = Q^m(R_L)_Q \subseteq Q^{m+1}(R_L)_Q$, άτοπο.

Λόγω των παραπάνω τα στοιχεία $\{1, t, ..., t^{e-1}\}$ είναι γραμμικώς ανεξάρτητα πάνω από το K_T διότι αν $\sum_{i=0}^{e-1} a_i t^i = 0$ με $a_i \in K_T$ και κάποιο $a_i \neq 0$, τότε $Q^m(R_L)_Q = 0$, με $m \in \mathbb{Z}$, άτοπο ([18]).

Αφού $[L : K_T] = e$, τότε η $\{1, t, ..., t^{e-1}\}$ είναι μία K_T-βάση του L.

Ισχυρισμός . *Τα στοιχεία $\{1, t, ..., t^{e-1}\}$ παράγουν το $(R_{K_T})_{Q_{K_T}}-$ module $(R_L)_Q$, οπότε αποτελούν μια βάση του.*

Απόδειξη. Αν $x \in (R_L)_Q$ από πριν μπορούμε να το γράψουμε στη μορφή $x = \sum_{i=0}^{e-1} a_i t^i$ με $a_i \in K_T$. Θα δείξουμε ότι $a_i \in (R_{K_T})_{Q_{K_T}}$. Υποθέτουμε ότι $x \neq 0$ άρα κάποιο $a_i \neq 0$. Αφού $x \in (R_L)_Q$, αν $x(R_L)_Q = Q^m(R_L)_Q$ τότε $m \geq 0$. Οπως αποδείξαμε πριν

$$m = min\{s_i e + i | a_i \neq 0, a_i (R_L)_Q = Q^{s_i e}(R_L)_Q\}$$

άρα $s_i e + i \geq 0 \Rightarrow s_i \geq -i/e > -1$ και $s_i \geq 0$. Επομένως $a_i \in (R_L)_Q \cap K_T = (R_{K_T})_{Q_{K_T}}$. □

Έστω τώρα $g(X) = X^e + a_1 X^{e-1} + ... + a_e \in K_T[X]$ το ελάχιστο πολυώνυμο του t πάνω από το K_T. Θα δείξουμε ότι $a_i \in Q_{K_T}(R_{K_T})_{Q_{K_T}}$ για $i = 1, ..., e$ και $a_e \notin {Q_{K_T}}^2(R_{K_T})_{Q_{K_T}}$, δηλαδή το g είναι ένα πολυώνυμο του *Eisenstein*. Λόγω του ότι $g(t) = 0$, έχουμε $-t^e = a_1 t^{e-1} + ... + a_e$, οπότε

$$e = min\{s_i e + (e - i) | a_i \neq 0, a_i (R_L)_Q = Q^{s_i e}(R_L)_Q\}.$$

Τότε $e \leq s_i e + (e - i) \Rightarrow 0 < i/e \leq s_i$ δηλαδή $a_i \in Q_{K_T}(R_{K_T})_{Q_{K_T}}$ για $i = 1, ...e$. Παρατηρούμε ότι αν $i \neq e$ τότε $s_i e + e - i \geq e + e - 1 > e$ άρα το παραπάνω ελάχιστο επιτυγχάνεται όταν $i = e$, δηλαδή, $s_e e = e \Rightarrow s_e = 1$ και από τον ορισμό του s_e παίρνουμε ότι $a_e \notin {Q_{K_T}}^2(R_{K_T})_{Q_{K_T}}$. □

Σημείωση . *Το ιδεώδες $Q(R_L)_Q$ έχει έναν γεννήτορα $t' \in R_L$ διότι αν $t(R_L)_Q = Q(R_L)_Q$, για κάποιο $t \in (R_L)_Q$ τότε $t = t'/s$ με $t', s \in R_L$ και $s \notin Q$ οπότε $t(R_L)_Q = t'(R_L)_Q$.*

Πρόταση 4.2.2. *Για κάθε $i = 0, 1, 2, ...$ έστω*
$G_{\Delta_i} = \{\sigma \in G_Z | \sigma(x) \equiv x \pmod{Q}^{i+1}$, για κάθε $x \in R_L\}$. Τότε :
(1) *Κάθε G_{Δ_i} είναι κανονική υποομάδα της G_T και*

$$G_T = G_{\Delta_0} \supseteq G_{\Delta_1} \supseteq G_{\Delta_2} \supseteq ...$$

(2) *Υπάρχει k τέτοιο ώστε η G_{Δ_k} να είναι τετριμμένη.*
(3) *Άν $t \in R_L$ τέτοιο ώστε $t(R_L)_Q = Q(R_L)_Q$ τότε*

$$G_{\Delta_i} = \{\sigma \in G_T | \sigma(t) \equiv t \pmod{Q^{i+1}(R_L)_Q}\}$$

για κάθε $i = 0, 1, 2, ...$

Απόδειξη. **(1)** Θεωρούμε τον δακτύλιο R_L/Q^{i+1}. Αν $\sigma \in G_Z$ τότε $\sigma(Q) = Q$ άρα $\sigma(Q^{i+1}) = Q^{i+1}$ οπότε ο σ δρα πάνω στον R_L/Q^{i+1} με φυσικό τρόπο : $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$, για κάθε $x \in R_L$. Η απεικόνιση ϕ με $\phi(\sigma) = \bar{\sigma}$ είναι ομομορφισμός ομάδων και $Ker\phi = G_{\Delta_i}$.

Πράγματι, η ϕ είναι προφανώς καλά ορισμένη και αν $\sigma, \tau \in G_T \subset G_Z$ τότε $\phi(\sigma\tau) = \overline{\sigma\tau} = \bar{\sigma}\bar{\tau} = \phi(\sigma)\phi(\tau)$.
Έχουμε ότι $\sigma \in G_{\Delta_i} \Leftrightarrow \sigma(x) \equiv x \pmod{Q^{i+1}}$, για κάθε $x \in R_L \Leftrightarrow \overline{\sigma(x)} = \bar{x} \Leftrightarrow \sigma \in Ker\phi$, άρα η G_{Δ_i} είναι κανονική υποομάδα της G_T. Προφανώς $G_T = G_{\Delta_0} \supseteq G_{\Delta_1} \supseteq G_{\Delta_2} \supseteq ....$

(2) Η $\cap_{i=0}^{\infty} G_{\Delta_i}$ είναι τετριμμένη διότι αν $\sigma \in \cap_{i=0}^{\infty} G_{\Delta_i}$ τότε $\sigma(x) - x \in \cap_{i=0}^{\infty} Q^{i+1} \subset \cap_{i=0}^{\infty} Q^{i+1}(R_L)_Q = 0_{(R_L)_Q}$ (από Krull's intersection theorem, [18]) και λόγω του ότι ο R_L είναι ακέραια περιοχή έχουμε $\cap_{i=0}^{\infty} Q^{i+1} = 0$ άρα $\sigma(x) = x$, για κάθε $x \in R_L$.

Αφού η G_T είναι πεπερασμένη ομάδα τότε υπάρχει k τέτοιο ώστε η G_{Δ_k} να είναι τετριμμένη.

(3) Αν $\sigma \in G_{\Delta_i}$ τότε $\sigma(t) - t \in Q^{i+1} \subset Q^{i+1}(R_L)_Q$ άρα $\sigma(t) \equiv t \pmod{Q^{i+1}(R_L)_Q}$.
Αντίστροφα, αν $\sigma \in G_T$ τέτοιο ώστε $\sigma(t) \equiv t \pmod{Q^{i+1}(R_L)_Q}$ τότε αφού $t \in R_L$ έχουμε $\sigma(t) - t \in Q^{i+1}(R_L)_Q \cap R_L = Q^{i+1}$. Τώρα άν $x \in R_L$ από προηγούμενη πρόταση το x μπορεί να γραφτεί στη μορφή $x = \sum_{i=0}^{e-1} a_i t^i$ με

$a_i \in (R_{K_T})_{Q_{K_T}} \subset (R_L)_Q$, οπότε

$$\sigma(x) - x = \sum_{i=0}^{e-1} a_i(\sigma(t)^i - t^i).$$

Όμως

$$\sigma(t)^i - t^i = [\sigma(t) - t] \cdot [\sigma(t)^{i-1} + \sigma(t)^{i-2}t + ... + t^{i-1}] \in Q^{i+1},$$

οπότε $\sigma(x) - x \in R_L \cap Q^{i+1}(R_L)_Q = Q^{i+1}$. □

Ορισμός 4.2.1. *Για κάθε $i = 0, 1, 2, ...$ η G_{Δ_i} θα λέγεται $i-$οστή ομάδα διακλάδωσης του Q στην επέκταση $L|K$. Το σταθερό σώμα της G_{Δ_i} θα το συμβολίζουμε ως K_{Δ_i} και θα λέγεται $i-$οστό σώμα διακλάδωσης του Q στην $L|K$.*

Αν χρειαστεί θα χρησιμοποιούμε τους παρακάτω πιο ακριβείς συμβολισμούς :

$$G_{\Delta_i} = G_{\Delta_i}(Q|P)$$
$$K_{\Delta_i} = K_{\Delta_i}(Q|P)$$

Άρα,

$$K \subseteq K_Z \subseteq K_T = K_{\Delta_0} \subseteq K_{\Delta_1} \subseteq ... \subseteq K_{\Delta_r} = L$$

Θεώρημα 4.2.1. ***(1)*** *Υπάρχει φυσικός ισομορφισμός ομάδων ϑ από την G_T/G_{Δ_1} εντός της $(\bar{L})^*$ (πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων του $\bar{L}$), οπότε η G_T/G_{Δ_1} είναι κυκλική ομάδα της οποίας η τάξη είναι σχετικά πρώτη με το p, όπου $p\mathbb{Z} = Q \cap \mathbb{Z}$.*
(2) *Για κάθε $i = 1, 2, ...$ υπάρχει ένας ισομορφισμός ϑ_i από την ομάδα $G_{\Delta_i}/G_{\Delta_{i+1}}$ μέσα στην προσθετική ομάδα του $\bar{L}$, οπότε $G_{\Delta_i}/G_{\Delta_{i+1}}$ είναι elementary abelian p- ομάδα (δηλαδή ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το σώμα $\mathbb{Z}_p$).*
(3) *Η G_{Δ_1} είναι p- ομάδα και η G_T είναι επιλύσιμη.*
(4) *Αν $m = [K_{\Delta_1} : K_T] = |G_T/G_{\Delta_1}|$, τότε ο p δεν διαιρεί το m και $e = mp^s$, για κάποιο $s \geq 0, p^s = [L : K_{\Delta_1}] = |G_{\Delta_1}|$.*

Απόδειξη. **(1)** Έστω $t \in R_L$ ένας γεννήτορας του κύριου ιδεώδους $Q(R_L)_Q$ οπότε $t \in Q(R_L)_Q \cap R_L = Q$. Αν $\sigma \in G_T$, αφού $\sigma(Q) = Q$, τότε $\sigma(t) \in Q \subseteq Q(R_L)_Q = t(R_L)_Q$, οπότε υπάρχει $c_\sigma \in (R_L)_Q$ τέτοιο ώστε $\sigma(t) = c_\sigma t$.

Θα δείξουμε ότι $c_\sigma \notin Q(R_L)_Q$. Πράγματι θεωρώντας τον $\sigma^{-1} \in G_T$, τότε $\sigma^{-1}(t) = c_{\sigma^{-1}}t$ με $c_{\sigma^{-1}} \in (R_L)_Q$. Έχουμε ότι $t = \sigma(\sigma^{-1}(t)) = \sigma(c_{\sigma^{-1}}t) = \sigma(c_{\sigma^{-1}})\sigma(t) = [\sigma(c_{\sigma^{-1}})c_\sigma]t$ οπότε $c_{\sigma^{-1}}c_\sigma = 1$, δηλαδή το c_σ είναι αντιστρέψιμο στοιχείο του $(R_L)_Q$, άρα $c_\sigma \notin Q(R_L)_Q$. Γνωρίζουμε ότι $(R_L)_Q/Q(R_L)_Q \cong R_L/Q = \bar{L}$ και η εικόνα του c_σ στο $\bar{L}$ είναι $\bar{c_\sigma} \neq \bar{0}$.

Ορίζουμε την απεικόνιση $\bar{\theta} : G_T \to (\bar{L})^*$ με $\bar{\theta}(\sigma) = \bar{c_\sigma}$. Αρχικά θα δείξουμε ότι η $\bar{\theta}$ είναι φυσική , δηλαδή ότι η $\bar{\theta}$ δεν εξαρτάται από την επιλογή του $t \in S$. Αν λοιπόν $t' \in R_L$ τέτοιο ώστε $t'R_L = Q(R_L)_Q$, τότε $t' = ut$ όπου το u είναι αντιστρέψιμο στοιχείο του $(R_L)_Q$ δηλαδή $u \in ((R_L)_Q)^* = (R_L)_Q \setminus Q(R_L)_Q$. Έστω ότι $\sigma(t') = c'_\sigma t'$, τότε $\sigma(ut) = c'_\sigma ut$ (1).
Όμως $\sigma \in G_T$ άρα $\sigma(u) \equiv u \pmod{Q(R_L)_Q}$ από το οποίο προκύπτει ότι $\sigma(u) = u + vt$ για κάποιο $v \in (R_L)_Q$. Λόγω αυτού η σχέση (1) παίρνει τη μορφή : $(u + tv)c_\sigma t = c'_\sigma ut$, τότε $uc_\sigma + vc_\sigma t = c'_\sigma u$ και θεωρώντας τις εικόνες στο $\bar{L}$, έχουμε $\bar{u}\bar{c_\sigma} = \bar{c'_\sigma}\bar{u}$ άρα $\bar{c_\sigma} = \bar{c'_\sigma}$. Δηλαδή η $\bar{\theta}$ είναι φυσική απεικόνιση.

$\bar{\theta}$ είναι ομομορφισμός ομάδων : $\bar{\theta}(\sigma\tau) = \bar{\theta}(\sigma)\bar{\theta}(\tau)$, για $\sigma, \tau \in G_T$. Πράγματι, αν $\sigma(t) = c_\sigma t$ και $\tau(t) = c_\tau t$ τότε $\sigma\tau(t) = \sigma(c_\tau t) = (c_\tau + vt)c_\sigma t = (c_\sigma c_\tau + vc_\sigma t)t$, όπου $v \in (R_L)_Q$ (διότι $\sigma(c_\tau) \equiv c_\tau \pmod{Q(R_L)_Q}$, αφού $c_\tau \in (R_L)_Q$ και $\sigma \in G_T$). Άρα $\bar{\theta}(\sigma\tau) = \overline{c_\tau c_\sigma + vc_\sigma c_\tau} = \overline{c_\tau}\overline{c_\sigma} = \bar{\theta}(\tau)\bar{\theta}(\sigma)$.

Ο πυρήνας του $\bar{\theta}$ ισούται με την G_{Δ_1}. Πράγματι, αν $\sigma \in G_{\Delta_1}$ τότε $\sigma(t) \equiv t \pmod{Q^2}$ οπότε $\sigma(t) = (1 + bt)t$ με $b \in R_L$, άρα $\bar{\theta}(\sigma) = \overline{1 + bt} = \bar{1}$. Αντίστροφα, αν $\sigma \in G_T$ τέτοιο ώστε $\bar{\theta}(\sigma) = \bar{1}$, δηλαδή $\overline{c_\sigma} = \overline{1}$, τότε $\sigma(t) - t = (c_\sigma - 1)t \in t^2(R_L)_Q$, οπότε $\sigma(t) \equiv t \pmod{Q^2(R_L)_Q}$ και από Πρόταση 4.2.2 (3), $\sigma \in G_{\Delta_1}$.

Σύμφωνα με τα παραπάνω η G_T/G_{Δ_1} είναι ισόμορφη με μια υποομάδα της $(\bar{L})^*$. Αν $p\mathbb{Z} = Q \cap \mathbb{Z}$, τότε το $\bar{L}$ είναι ένα πεπερασμένο σώμα που περιέχει το $\mathbb{Z}_p$, άρα από τη θεωρία των πεπερασμένων σωμάτων έχουμε ότι τα μη μηδενικά στοιχεία του $\bar{L}$ φτιάχνουν μια κυκλική ομάδα τάξης $|\bar{L}| - 1$, το οποίο προφανώς δεν είναι πολλαπλάσιο του p, οπότε η G_T/G_{Δ_1} είναι επίσης κυκλική της οποίας η τάξη δεν είναι πολλαπλάσιο του p.

(2) Έστω $i \geq 1$. Αν $\sigma \in G_{\Delta_i}$ τότε $\sigma(t) = t + d_\sigma t^{i+1}$ με $d_\sigma \in (R_L)_Q$. Θεωρούμε την απεικόνιση $\widetilde{\theta_i} : G_{\Delta_i} \to \bar{L}$ με $\widetilde{\theta_i}(\sigma) = \bar{d_\sigma}$ και θα δείξουμε ότι είναι

μονομορφισμός ομάδων. Πράγματι, αν $\sigma, \tau \in G_{\Delta_i}$, τότε :

$$\begin{aligned}\sigma\tau(t) &= \sigma(t + d_\tau t^{i+1}) = \sigma(t) + \sigma(d_\tau)\sigma(t)^{i+1} \\ &= t + d_\sigma t^{i+1} + (d_\tau + d' t^{i+1})(t + d_\sigma t^{i+1})^{i+1} \\ &= t + (d_\sigma + d_\tau)t^{i+1} + ct^{i+2},\end{aligned}$$

όπου $d', c \in R_L$ άρα $\widetilde{\theta}_i(\sigma\tau) = \overline{d_\sigma + d_\tau} = \widetilde{\theta}_i(\sigma) + \widetilde{\theta}_i(\tau)$.

Αν $\sigma \in G_{\Delta_{i+1}}$ τότε $\sigma(t) = t + ct^{i+2}$, οπότε $d_\sigma = ct$ και $\bar{d_\sigma} = \bar{0}$. Αντίστροφα , αν $\bar{d_\sigma} = \bar{0}$, τότε $\sigma(t) \equiv t \pmod{Q^{i+2}}$ όμως $Q^{i+2} \subseteq Q^{i+2}(R_L)_Q$ από το οποίο έπεται το ζητούμενο.

Παρατηρώντας ότι ο $\bar{L}$ είναι διανυσματικός χώρος πάνω από το $\mathbb{Z}_p$ το ίδιο ισχύει και για την $G_{\Delta_i}/G_{\Delta_{i+1}}$.

(3) Η ομάδα G_T έχει την παρακάτω αλυσίδα κανονικών υποομάδων :

$$G_T \supseteq G_{\Delta_1} \supseteq G_{\Delta_2} \supseteq ... \supseteq G_{\Delta_k} = \{\epsilon\}$$

(για κάποιο k από της Πρόταση 4.2.2 (2». Όπως αποδείξαμε παραπάνω η G_T/G_{Δ_1} είναι κυκλική ομάδα και κάθε $G_{\Delta_i}/G_{\Delta_{i+1}}$ είναι elementary abelian p-ομάδα , τότε η G_T είναι επιλύσιμη και η G_{Δ_1} είναι $p-$ομάδα.

(4) Γνωρίζουμε ότι $e = [L : K_{\Delta_1}][K_{\Delta_1} : K_T]$ (Θεώρημα 4.1.1) , όμως $[L : K_{\Delta_1}] = |G_{\Delta_1}|$ η οποία είναι $p-$ομάδα (**3**) και $[L : K_{\Delta_1}] = |G_T/G_{\Delta_1}|$ αλλά από το **(1)** αυτή η ομάδα έχει τάξη σχετικώς πρώτη με το p. □

Αφού οι G_T, G_{Δ_1} είναι κανονικές υποομάδες της G_Z, έχουμε ότι $\sigma G_T \sigma^{-1} = G_T$ και $\sigma G_{\Delta_1}\sigma^{-1} = G_{\Delta_1}$ για κάθε $\sigma \in G_Z$. Οπότε θεωρώντας τα σύμπλοκα της G_T μέσω της G_{Δ_1} προκύπτει ότι $\sigma(\tau G_{\Delta_1})\sigma^{-1} = (\sigma\tau\sigma^{-1})G_{\Delta_1}$ για κάθε $\tau \in G_T$. Άρα ο σ δρα με συζυγία στην ομάδα πηλίκο G_T/G_{Δ_1} και η δράση ορίζεται ως $\widetilde{\sigma}(\tau G_{\Delta_1}) = (\sigma\tau\sigma^{-1})G_{\Delta_1}$. Η πρόταση που ακολουθεί περιγράφει αυτήν την δράση.

Πρόταση 4.2.3. *Έστω $\sigma \in G_Z$ τέτοιο ώστε η εικόνα του μέσω του ομομορφισμού $G_Z \to G_Z/G_T \cong Gal(\overline{L}/\overline{K})$ να αντιστοιχεί στον αυτομορφισμό του Frobenius της επέκτασης $\overline{L}/\overline{K}$. Τότε*
(1) *Αν $\tau \in G_T$ τότε $\widetilde{\sigma}(\tau G_{\Delta_1}) = \tau^q G_{\Delta_1}$, όπου $q = \#(\overline{K})$.*
(2) *Αν η G_Z είναι αβελιανή τότε $\tau^{q-1} \in G_{\Delta_1}$ για κάθε $\tau \in G_T$ και η G_T/G_{Δ_1} έχει τάξη που διαιρεί το $q-1$*

Απόδειξη. **(1)** Έστω $t \in R_L$ τέτοιο ώστε $t(R_L)_Q = Q(R_L)_Q$ και θα υπολογίσουμε το $\sigma\tau\sigma^{-1}(t)$. Όπως στην απόδειξη του θεωρήματος 4.2.1 γράφουμε

$\sigma(\tau) = c_\sigma t, \sigma^{-1}(t) = c_{\sigma^{-1}} t$ με $c_\sigma, c_{\sigma^{-1}} \in (R_L)_Q$ και έχουμε ότι $\sigma(c_{\sigma^{-1}})c_\sigma = 1$. Άν λοιπόν $t \in G_T$ τότε

$$\begin{aligned}
\sigma\tau\sigma^{-1}(t) &= \sigma\tau(c_{\sigma^{-1}}t) \\
&= \sigma(\tau(c_{\sigma^{-1}})\tau(t)) \\
&= \sigma(c_{\sigma^{-1}} + vt)\sigma(c_\tau)\sigma(t) \\
&= (\sigma(c_{\sigma^{-1}}) + \sigma(v)c_\sigma t)\sigma(c_\tau)c_\sigma t \\
&\equiv \sigma(c_\tau)t \pmod{Q^2(R_L)_Q} \equiv {c_\tau}^q t \pmod{Q^2(R_L)_Q}
\end{aligned}$$

όπου $v \in (R_L)_Q$, δεδομένου ότι ο αυτομορφισμός του Frobenius $\widetilde{\sigma}$ ορίζεται ως η ύψωση στη δύναμη $q = \#(\overline{K})$.

Από την άλλη μεριά, $\tau(t) = c_\tau t, \tau^2(t) = \tau(c_\tau)\tau(t) = (c_\tau + ut)c_\tau t \equiv {c^2}_\tau t \pmod{Q^2(R_L)_Q}$ (όπου $u \in (R_L)_Q$). Ομοίως ${\tau^q}(t) \equiv {c^q}_\tau t \pmod{Q)^2(R_L)_Q}$, άρα $\sigma\tau\sigma^{-1}(t) \equiv \tau^q(t) \pmod{Q^2(R_L)_Q}$ και τότε $\tau^{-q}\sigma\tau\sigma^{-1}(t) \equiv t \pmod{Q^2(R_L)_Q}$ δηλαδή $\tau^{-q}\sigma\tau\sigma^{-1} \in G_{\Delta_1}$. Λόγω των παραπάνω συμπεραίνουμε ότι $\widetilde{\sigma}(\tau G_{\Delta_1}) = (\sigma\tau\sigma^{-1})G_{\Delta_1} = \tau^q G_{\Delta_1}$.

(2) Αν η G_Z είναι αβελιανή ομάδα , τότε $(\tau^{-q}\sigma\tau\sigma^{-1})^{-1} = \tau^{q-1} \in G_{\Delta_1}$ για κάθε $\tau \in G_T$. Όμως η G_T/G_{Δ_1} είναι κυκλική ομάδα και $\tau^{q-1}G_{\Delta_1} = G_{\Delta_1}$, άρα η τάξη της G_{Δ_1} διαιρεί το $q-1$. □

Θεώρημα 4.2.2. *Έστω L/K μια επέκταση Galois και το Q να είναι η μοναδική επέκταση του P στο L. Υποθέτουμε ότι υπάρχει $t \in R_L$ τέτοιο ώστε $Q(R_L)_Q = t(R_L)_Q$ και $(R_L)_Q = (R_K)_P[t]$ (αυτό ισχύει όταν το Q διακλαδίζεται πλήρως πάνω από το P, δηλαδή το σώμα αδρανείας $K_T(Q|P)$ ισούται με το K.) Τότε ο εκθέτης της διαφορίζουσας του Q στην L/K ισούται με*

$$s_Q(L/K) = \sum_{i=0}^{k-1} [|G_{\Delta_i}| - 1]$$

όπου $G_T = G_{\Delta_0} \supseteq G_{\Delta_1} \supseteq ... \supseteq G_{\Delta_{k-1}} \supseteq G_{\Delta_k} = \{id\}$, οι ομάδες διακλάδωσης του Q στην επέκταση L/K.

Απόδειξη. Από Λήμμα 4.2.1 και Πρόταση 2.2.2 έχουμε ότι $\Delta_P(L/K) = g'(t)(R_L)_P$, όπου $g = Irr(t, K)$. Γράφουμε $g(X) = \prod_{\sigma \in G} (X - \sigma(t))$, όπου $G := Gal(L/K)$. Τότε $g'(t) = \prod_{\sigma \neq id} (t - \sigma(t))$. Αφού το Q είναι η μοναδική επέκταση του P στο L έχουμε ότι $G_Z(Q|P) = G$. Αν $\sigma \in G_Z \setminus G_T$

τότε $\sigma(t) - t \in R_L$ όμως $\sigma(t) - t \notin Q$ και ομοίως αν $\sigma \in G_{\Delta_i} \setminus G_{\Delta_{i+1}}$ τότε $\sigma(t) - t \in Q^{i+1}$ όμως $\sigma(t) - t \notin Q^{i+2}$.

Αν τώρα $s := s_Q(L/K)$ τότε

$$Q^s(R_L)_Q = g'(t)(R_L)_Q = \prod_{\sigma \neq id} (\sigma(t) - t)(R_L)_Q$$

και γράφοντας το $(\sigma(t) - t)(R_L)_Q$ στη μορφή $(\sigma(t) - t)(R_L)_Q = Q^{s(\sigma)}(R_L)_Q$ προκύπτει ότι

$$s = s_Q(L/K) = \sum_{\sigma \neq id} s(\sigma) = \sum_{i=0}^{k-1} \sum_{\sigma \in G_{\Delta_i} \setminus G_{\Delta_{i+1}}} s(\sigma) = \sum_{i=0}^{k-1} (i+1)[|G_{\Delta_i}| - |G_{\Delta_{i+1}}|] =$$

$$= (|G_{\Delta_0}| - |G_{\Delta_1}|) + 2(|G_{\Delta_1}| - |G_{\Delta_2}|) + ... + r(|G_{\Delta_k - 1}| - |G_{\Delta_k}|)$$

$$= |G_{\Delta_0}| + |G_{\Delta_1}| + ... + |G_{\Delta_{k-1}}| - k = \sum_{i=0}^{k-1} (|G_{\Delta_i}| - 1).$$

□

Κεφάλαιο 5

Το θεώρημα Kronecker-Weber

Είμαστε πλέον σε θέση να αποδείξουμε το θεώρημα των Kronecker-Weber .

Θεώρημα Kronecker-Weber. *Αν L είναι ένα αλγεβρικό σώμα αριθμών τέτοιο ώστε η επέκταση $L/\mathbb{Q}$ να είναι αβελιανή, τότε υπάρχει ρίζα της μονάδας ζ τέτοια ώστε $L \subseteq \mathbb{Q}(\zeta)$.*

Απόδειξη. Πρώτα θα θεωρήσουμε δυο σημαντικές ειδικές περιπτώσεις και στη συνέχεια θα δείξουμε πως θα ανάγαγουμε τη γενική περίπτωση σε αυτές τις δύο ειδικές. Για να επιτευχθεί ο σκοπός μας όμως, θα χρειαστούμε κάποια λήμματα.

Περίπτωση 1. *Υποθέτουμε ότι $[L : \mathbb{Q}] = p^m$ και $\delta_L = p^k$, όπου p περιττός πρώτος, $m, k \geq 1$.*

Λήμμα 5.1. *Υπάρχει ακριβώς ένα πρώτο ιδεώδες P στο L τέτοιο ώστε $P \cap \mathbb{Z} = p\mathbb{Z}$. Επιπλέον ο p διακλαδίζεται πλήρως στην επέκταση $L/\mathbb{Q}$ και $K_T = K_{\Delta_1} = \mathbb{Q}$.*

Απόδειξη. Έστω ότι υπάρχουν $P, P' \in Spec(R_L)$ τέτοια ώστε $P \cap \mathbb{Z} = P' \cap \mathbb{Z} = p\mathbb{Z}$. Αφού η $G := Gal(L/\mathbb{Q})$ είναι αβελιανή, ισχύει $G_Z(P|p\mathbb{Z}) = G_Z(P'|p\mathbb{Z})$ και $G_T(P|p\mathbb{Z}) = G_T(P'|p\mathbb{Z})$ (βλ. Πρόταση 4.1.1). Έστω K_T να είναι το σώμα αδρανείας των P, P'. Θα δείξουμε ότι $|\delta_{K_T}| = 1$

Από Θεώρημα 4.1.1 ο p δεν διακλαδίζεται στην $K_T/\mathbb{Q}$, άρα $p \nmid \delta_{K_T}$. Αν q είναι πρώτος με $q \neq p$ και $q \mid \delta_{K_T}$ τότε από το θεώρημα του *Dedekind* έχουμε ότι ο q διακλαδίζεται στην $K_T/\mathbb{Q}$ άρα και στην επέκταση $L/\mathbb{Q}$, δηλαδή

$q \mid \delta_L = p^k$, άτοπο. Συνεπώς η δ_{K_T} δεν έχει κανένα πρώτο παράγοντα και από το του θεώρημα του $Minkowski$, έχουμε ότι $K_T = \mathbb{Q}$.

Επομένως, αν K_Z είναι το σώμα ανάλυσης του P στην επέκταση $L/\mathbb{Q}$ (το οποίο ισούται με το σώμα ανάλυσης όλων των πρώτων ιδεωδών του R_L που είναι πάνω απο το p) τότε $\mathbb{Q} \subseteq K_Z \subseteq K_T$ και $K_T = \mathbb{Q}$, οπότε $K_Z = \mathbb{Q}$. Δηλαδή το P είναι η μοναδική επέκταση του $p\mathbb{Z}$ στο L και συνεπώς $r = 1$.
Γνωρίζουμε ότι $[K_T : K_Z] = [K_T : \mathbb{Q}] = f(P|p\mathbb{Z})$ (Θεώρημα 4.1.1), οπότε $f(P|p\mathbb{Z}) = 1$. Τελικά από την σχέση $[L : \mathbb{Q}] = efr$ συμπεραίνουμε ότι $[L : \mathbb{Q}] = e$, δηλαδή το πρώτο ιδεώδες $p\mathbb{Z}$ διακλαδίζεται πλήρως στην επέκταση $L/\mathbb{Q}$.

Επίσης, επειδή $p \nmid [K_{\Delta_1} : \mathbb{Q}] = [K_{\Delta_1} : K_T]$ και $[L : \mathbb{Q}] = p^m$ έπεται ότι $K_{\Delta_1} = K_T$ (βλ. Θεώρημα 4.2.1). □

Λήμμα 5.2. *Έστω H σώμα με $\mathbb{Q} \subseteq H \subseteq L$ και $[H : \mathbb{Q}] = p$. Άν R_H είναι ο δακτύλιος των ακεραίων του H και $Q = P \cap R_H$ τότε ο εκθέτης της διαφορίζουσας του Q στην επέκταση $H/\mathbb{Q}$ ισούται με $2(p-1)$.*

Απόδειξη. Επειδή ο p διακλαδίζεται πλήρως στην $L/\mathbb{Q}$, από την μεταβατικότητα των δεικτών διακλάδωσης έπεται ότι ο p διακλαδίζεται πλήρως και στην επέκταση $H/\mathbb{Q}$.

Αν z είναι γεννήτορας του ιδεώδους $Q(R_H)_Q$, δηλαδή $Q(R_H)_Q = z(R_H)_Q$, τότε $(R_H)_Q = \mathbb{Z}_p[z]$, το σύνολο $\{1, z, ..., z^{p-1}\}$ είναι γραμμικώς ανεξάρτητο πάνω από το $\mathbb{Q}$ και ο z είναι ρίζα ενός $Eisenstein$ πολυωνύμου

$$g(X) = X^p + a_1 X^{P-1} + ... + a_p, a_i \in \mathbb{Z}, p \mid a_i, \forall i = 1, 2, ..., p$$

όμως $p^2 \nmid a_p$ (Πρόταση 4.2.1). Συνεπώς $g(X) = \prod_{\sigma \in G} (X - \sigma(z))$, όπου $G := Gal(H/\mathbb{Q})$ και $g'(z) = \prod_{\sigma \neq id} (z - \sigma(z))$. Γνωρίζουμε ότι (Πρόταση 2.2.1) $\Delta_{p\mathbb{Z}}(H/\mathbb{Q}) = g'(z)(R_H)_Q$.
Θα πρέπει λοιπόν να υπολογίσουμε τη μεγαλύτερη δύναμη του $Q(R_H)_Q$ που διαιρεί το κύριο ιδεώδες που παράγεται από το

$$g'(z) = pz^{p-1} + (p-1)a_1 z^{p-2} + ... + a_{p-1}$$

Επειδή ο p διακλαδίζεται πλήρως στην $H/\mathbb{Q}$ και $[H : \mathbb{Q}] = p$, έπεται ότι $(p\mathbb{Z})(R_H)_Q = z^p(R_H)_Q$. Από την άλλη μεριά αν q είναι ένας πρώτος διαφορετικός του p τότε $q \notin Q$, οπότε $q(R_H)_Q = (R_H)_Q = z^0(R_H)_Q$. Άρα για κάθε $a \in \mathbb{Z}$, αν $p^m \mid\mid a$ τότε $a(R_H)_Q = z^{pm}(R_H)_Q$ με $m \geq 0$.

Πιο συγκεκριμένα, $a_i(p-i)(R_H)_Q = z^{ps_i}(R_H)_Q$, άρα $s_i \geq 1 \forall i \in \{1,...,p-1\}$. Οπότε

$$[(p-i)a_i z^{p-i-1}](R_H)_Q = z^{ps_i+(p-i-1)}(R_H)_Q$$

Με το ίδιο επιχείρημα που χρησιμοποήσαμε στην απόδειξη της Πρότασης 4.2.1 αν $i,j \in \{1,...,p-1\}$ με $i \neq j$ ισχύει $ps_i+(p-i-1) \neq ps_j+(p-j-1)$ οπότε αν $g'(z)(R_H)_Q = z^s(R_H)_Q$ τότε $s = min\{ps_i+(p-i-1), 0 \leq i \leq p-1\}$. Άρα $p \leq s$, αφού $s_i \geq 1$ οπότε $p \leq ps_i+(p-i-1)$, για $i = 1...,p-1$. Επίσης

$$(pz^{p-1})(R_H)_Q = z^{p+p-1}(R_H)_Q = z^{2p-1}(R_H)_Q$$

άρα έχουμε τις ανισότητες $p \leq s \leq 2p-1$. Όμως ο εκθέτης της διαφορίζουσας ισούται με

$$s = \sum_{i=0}^{r-1}(|G'_{\Delta_i}|-1)$$

όπου G'_{Δ_i} είναι η $i-$οστή ομάδα διακλάδωσης του Q στην επέκταση $H/\mathbb{Q}$ (Θεώρημα 4.2.2).

Επειδή $[H:\mathbb{Q}] = p \Rightarrow |G'\Delta_i| = 1$ ή p, οπότε $p-1 \mid s$ και άρα

$$1 < \frac{p}{p-1} \leq \frac{s}{p-1} \leq \frac{2p-1}{p-1} = 2 + \frac{1}{p-1} < 3$$

δηλαδή $\frac{s}{p-1} = 2 \Rightarrow s = 2(p-1)$. □

Θεμελιώδες Λήμμα. *Έστω i ο μικρότερος δείκτης τέτοιος ώστε $G_{\Delta_i} \neq G = Gal(L/\mathbb{Q})(i > 1$ από Λήμμα 5.1). Τότε $[K_{\Delta_i}:\mathbb{Q}] = p$ και K_{Δ_i} είναι το μοναδικό σώμα βαθμού p πάνω από το $\mathbb{Q}$ που περιέχεται στο L.*

Απόδειξη. Έχουμε ότι $[K_{\Delta_i}:\mathbb{Q}] = [K_{\Delta_i}:K_{\Delta_{i-1}}] = |G_{\Delta_{i-1}}/G_{\Delta_i}|$. Γνωρίζουμε όμως ότι η $G_{\Delta_{i-1}}/G_{\Delta_i}$ είναι ισόμορφη με μια υποομάδα της προσθετικής ομάδας του $\overline{L}$ (Θεώρημα 4.2.1). Επειδή $f(L|\mathbb{Q}) = 1 \Rightarrow \overline{L} = \mathbb{F}_p$ και λόγω της υπόθεσης $G_{\Delta_i} \neq G_{\Delta_{i-1}}$ συμπεραίνουμε ότι $|G_{\Delta_{i-1}}/G_{\Delta i}| = p$, άρα και $[K_{\Delta i}:\mathbb{Q}] = p$.

Έστω H ένα σώμα τέτοιο ώστε $\mathbb{Q} \subseteq H \subseteq L, [H:\mathbb{Q}] = p$ και υποθέτουμε ότι $H \neq K_{\Delta_i}$. Θα υπολογίσουμε τις διαφορίζουσες $\Delta_{P_{K_{\Delta i}}}(L|K_{\Delta_i}), \Delta_{P_H}(L|H)$ χρησιμοποιώντας το Θεώρημα 4.2.2.
Αν $\mathcal{H} := Gal(L/H)$, τότε $G_{\Delta_j}(L|H) = G_{\Delta_j}(L|\mathbb{Q}) \cap \mathcal{H}$ και $G_{\Delta_j}(L|K_{\Delta_i}) =$

$G_{\Delta_j}(L|\mathbb{Q}) \cap G_{\Delta_i}(L/\mathbb{Q}) \forall j = 0, 1, ...$
Άρα $G_{\Delta_0}(L|K_{\Delta_i}) = ... = G_{\Delta_i}(L|K_{\Delta_i}) = G_{\Delta_i}$ ενώ $G_{\Delta_j}(L|K_{\Delta_i}) = G_{\Delta_j}$, για $j \geq i+1$. Ομοίως $G_{\Delta_0}(L|H) = ... = G_{\Delta i-1}(L|H) = \mathcal{H}$ (αφού $G_{\Delta_{i-1}} = G$), ενώ $G_{\Delta_i}(L|H)$ περιέχεται γνήσια στην G_{Δ_i} διότι αλλιώς αν $G_{\Delta_i}(L|H) = G_{\Delta_i}(L|\mathbb{Q}) \Rightarrow G_{\Delta_i}(L|\mathbb{Q}) \subseteq \mathcal{H}$ και $G_{\Delta_j}(L|H) \subseteq G_{\Delta_j}$ για $j \geq i+1$. Οπότε

$$s_P(L|K_{\Delta_i}) = \sum_{j=0}^{k-1} [|G_{\Delta_j}(L|K_{\Delta_i})| - 1] > \sum_{j=0}^{k-1} [|G_{\Delta_j}(L|H)| - 1] = s_P(L|H).$$

Όμως από τη μεταβατικότητα της διαφορίζουσας παίρνουμε:

$$\Delta_{p\mathbb{Z}}(L|\mathbb{Q}) = \Delta_{P_{K_{\Delta_i}}}(L|K_{\Delta_i})(\Delta_{K_{p\mathbb{Z}}}(K_{\Delta_i}|\mathbb{Q})(R_L)_P)$$

και

$$\Delta_{p\mathbb{Z}}(L|\mathbb{Q}) = \Delta_{P_H}(L|H)(\Delta_{p\mathbb{Z}}(H|\mathbb{Q})(R_L)_P).$$

Το P διακλαδίζεται πλήρως στην $L/\mathbb{Q}$ και $[H:\mathbb{Q}] = [K_{\Delta_i}:\mathbb{Q}] = p$, επομένως από Λήμμα 5.2 οι εκθέτες των διαφοριζουσών $\Delta_{P_{K_{\Delta_i}}}(L|K_{\Delta_i}), \Delta_{P_H}(L|H)$ συμπίπτουν, άτοπο. □

Λήμμα 5.3. *Έστω G μια αβελιανή ομάδα. Τότε ισχύουν τα εξης:*
(1) *Έστω $|G| = p^m, m \geq 1$, p πρώτος και H υποομάδα της G με $|H| = p^h$. Τότε για $h < h' \leq m$ υπάρχει $H' \leq G$ με $H \leq H'$ και $|H'| = p^{h'}$.*
(2) *Αν $|G| = p^m$ και η G έχει ακριβώς μια υποομάδα τάξης p^{m-1} τότε η G είναι κυκλική.*

Απόδειξη. **(1)** Αρκεί να το δείξουμε για $h' = h+1 \leq m$ και τότε επαναλαμβάνουμε το επιχείρημα.

Έστω $\overline{G} = G/H$ τάξης p^{m-h}, άρα $\exists \bar{x} \in \overline{G}$ τάξης p. Θεωρούμε $H' =< H, x >$ τότε $H \leq H'$ και $H' = H \cup xH \cup ... \cup x^{p-1}H (x^p \in H)$ άρα $|H'| = pp^h = p^{h+1}$.
(2) Έστω H η μοναδική υποομάδα τάξης p^{m-1} της G. Υποθέτουμε ότι υπάρχει $x \in G \setminus H$ με $ord(x) < m$. Από το **(1)** η κυκλική ομάδα που παράγεται από το x περιέχεται σε μια υποομάδα τάξης p^{m-1}, δηλαδή στην H, άτοπο. □

Πόρισμα 1. *$H\, G := Gal(L/\mathbb{Q})$ είναι κυκλική.*

Απόδειξη. Η G είναι αβελιανή τάξης p^m και λόγω του Θεμελιώδους Λήμματος έχει μοναδική υποομάδα τάξης $p^{m-1} \Rightarrow G$ κυκλική (βλ. Λήμμα 5.3). □

Λήμμα 5.4. *Έστω K, K' αλγεβρικά σώματα αριθμών με $K/\mathbb{Q}, K'/\mathbb{Q}$ επεκτάσεις Galois και θεωρούμε $L = KK'$ τη σύνθεση τους. Αν q πρώτος που δεν διακλαδίζεται στην $K/\mathbb{Q}$ και q δεν διακλαδίζεται στην $K'/\mathbb{Q}$ τότε ο q δεν διακλαδίζεται ούτε στην $KK'/\mathbb{Q}$.*

Απόδειξη. Η επέκταση $L/K \cap K'$ είναι *Galois* και μάλιστα

$$Gal(L/K \cap K') \cong Gal(K/K \cap K') \times Gal(K'/K \cap K')$$

Αυτός ο ισομορφισμός αντιστοιχίζει κάθε $\sigma \in Gal(L/K \cap K')$ σε ένα ζευγάρι $(\sigma_K, \sigma_{K'})$, όπου $\sigma_K = \sigma \restriction K, \sigma_{K'} = \sigma \restriction K'$. Έστω τώρα $Q \in Spec(R_L)$ τέτοιο ώστε $Q \cap \mathbb{Z} = q\mathbb{Z}$ και $G_T(Q|q\mathbb{Z})$ η ομάδα αδρανείας.

Αν $\sigma \in G_T(Q|q\mathbb{Z}) \cap Gal(L/K \cap K')$ τότε $\sigma_K \in G_T(Q \cap K), \sigma_{K'} \in G_T(Q \cap K'|Q \cap (K \cap K'))$.

Λόγω της υπόθεσης οι ομάδες αδρανείας των πρώτων ιδεωδών των K, K' που επεκτείνουν το q είναι τετριμμένες, δηλαδή $\sigma_K = \sigma_{K'} = id$ οπότε $\sigma = id$ και το Q δεν διακλαδίζεται στην $L/K \cap K'$. Όμως $Q \cap (K \cap K')$ δεν διακλαδίζεται στην $K \cap K'/\mathbb{Q}$, αφού δεν διακλαδίζεται στην $K/\mathbb{Q} \Rightarrow$ το Q δεν διακλαδίζεται στην $KK'/\mathbb{Q} \Rightarrow$ ο q δεν διακλαδίζεται στην $KK'/\mathbb{Q}$. □

Παρατήρηση. *Το παραπάνω λήμμα ισχύει και όταν οι επεκτάσεις $K/\mathbb{Q}, K'/\mathbb{Q}$ δεν είναι Galois.*

Πρόταση 1. *Στην Περίπτωση 1, $L \subseteq \mathbb{Q}(\zeta)$, όπου ζ μια ρίζα της μονάδας.*

Απόδειξη. Αν $F := \mathbb{Q}(\zeta)$, όπου ζ μια πρωταρχική p^{m+1} ρίζα της μονάδας τότε η επέκταση $F/\mathbb{Q}$ είναι Galois, κυκλική και μάλιστα $Gal(F/\mathbb{Q}) \cong (\mathbb{Z}/p^{m+1}\mathbb{Z})^*$. Δηλαδή $F/\mathbb{Q}$ είναι κυκλική επέκταση βαθμού $\varphi(p^{m+1}) = p^m(p-1)(p \neq 2)$. Γνωρίζουμε επίσης ότι δ_F είναι δύναμη του p (Πρόταση 3.1.4).

Η κυκλική ομάδα $Gal(F/\mathbb{Q})$ έχει υποομάδα τάξης $p-1$, της οποίας το σώμα των σταθερών στοιχείων θα συμβολίζουμε με F', οπότε $[F' : \mathbb{Q}] = p^m$. Επομένως $F'/\mathbb{Q}$ είναι κυκλική επέκταση και δ'_F είναι ξανά δύναμη του p. Πράγματι, αν q πρώτος με $q \mid \delta_{F'}$, τότε ο q διακλαδίζεται στην $F'/\mathbb{Q}$ άρα και στην $F/\mathbb{Q} \Rightarrow q \mid \delta_F$ δηλαδή $q = p$. Αν LF' είναι η σύνθεση των σωμάτων L, F' τότε η επέκταση $LF'/\mathbb{Q}$ είναι επίσης αβελιανή με βαθμό $[LF' : \mathbb{Q}] = [LF' : F'][F' : \mathbb{Q}] = [L : L \cap F'][F' : \mathbb{Q}]$, οπότε είναι δύναμη του p. Τώρα θα δείξουμε ότι $\delta_{LF'}$ είναι δύναμη του p. Πράγματι, αν $q \mid \delta_{LF'}$ τότε ο q διακλαδίζεται στην $LF'/\mathbb{Q}$ και σύμφωνα με το Λήμμα 5.4, είτε ο q διακλαδίζεται στην $L/\mathbb{Q}$ είτε διακλαδίζεται στην $F'/\mathbb{Q}$. Ισοδύναμα, $q \mid \delta_L$ ή $q \mid \delta_{F'}$ δηλαδή $q = p$ και $\delta_{LF'}$ είναι δύναμη p.

Στη συνέχεια εφαρμόζουμε το Πόρισμα 1 στην αβελιανή επέκταση $LF'/\mathbb{Q}$ με βαθμό και διακρίνουσα δυνάμεις του p. Έπεται ότι $LF'/\mathbb{Q}$ είναι κυκλική και από θεωρία $Galois$ έχουμε

$$Gal(LF'/L\cap F') \cong Gal(L/L\cap F')\times Gal(F'/L\cap F')$$

τότε όμως η παραπάνω ανάλυση πρέπει να είναι τετριμμένη, δηλαδή μία εκ των $Gal(L/L\cap F'), Gal(F'/L\cap F')$ πρέπει να είναι τετριμμένη. Αν $L = L\cap F' \Rightarrow L\subseteq F'$ ενώ αν $F' = L\cap F' \Rightarrow F'\subseteq L$ και αφού $[L:\mathbb{Q}] = [F':\mathbb{Q}] \Rightarrow F' = L$. □

Περίπτωση 2. *Αν* $[L:\mathbb{Q}] = 2^m, \delta_L = 2^k$ *όπου* $m,k\geq 1$.

Λήμμα 5.5. *Δεδομένου ότι* $m\geq 1$, *υπάρχει πραγματικό σώμα* K *τέτοιο ώστε* $[K:\mathbb{Q}] = 2^m, \delta_K$ *να είναι δύναμη του 2 και* $K\subseteq\mathbb{Q}(\xi)$, *όπου* ξ *μια ρίζα της μονάδας.*

Απόδειξη. Έστω ξ πρωταρχική ρίζα της μονάδας τάξης 2^{m+2} και $K' = \mathbb{Q}(\xi)$. Τότε $[K':\mathbb{Q}] = \phi(2^{m+2}) = 2^{m+1}$ οπότε $i\in K'$.

Για $K = K'\cap\mathbb{R}$, έχουμε $K' = K(i)$. Πράγματι, οι συζυγείς του ξ ανήκουν στο K' και είναι είτε πραγματικοί ή εμφανίζονται σε ζευγάρια μιγαδικών της μορφής $a+bi, a-bi$ με $a,b\in\mathbb{R}\Rightarrow 2a, 2b\in K'\cap\mathbb{R} = K$ άρα $a,b\in K$ και $K' = K(i)$. Οπότε $[K':K] = 2$ και $2^{m+1} = [K:\mathbb{Q}] = [K':K][K:\mathbb{Q}] = 2[K:\mathbb{Q}]\Rightarrow [K:\mathbb{Q}] = 2^m$.

Τώρα θα δείξουμε ότι και η διακρίνουσα δ_K του K είναι δύναμη του 2. Έστω q πρώτος τέτοιος ώστε $q\mid\delta_K$, τότε ο q διακλαδίζεται στην επέκταση $K/\mathbb{Q}$ άρα διακλαδίζεται και στην $K'/\mathbb{Q}$, δηλαδή $q\mid\delta_{K'}$. Το ζητούμενο έπεται από την Πρόταση 3.1.4. □

Λήμμα 5.6. *Αν* $m\geq 1$, *τότε υπάρχει ακριβώς ένα σώμα πραγματικών* K *τέτοιο ώστε* $K/\mathbb{Q}$ *να είναι αβελιανή επέκταση,* $[K:\mathbb{Q}] = 2^m$ *και* δ_K *να είναι δύναμη του 2.*

Απόδειξη. Για $m = 1$ και $[F:\mathbb{Q}] = 2$ με $F\subseteq\mathbb{R}\Rightarrow F = \mathbb{Q}(\sqrt{d})$ όπου $d>0$, ελεύθερος τετραγώνων. Τότε $\delta_F = d$ όταν $d\equiv 1 \pmod 4$ και $\delta_F = 4d$ όταν $d\equiv 2 \pmod 4$ ή $d\equiv 3 \pmod 4$. Οπότε αν η δ_F είναι δύναμη του 2 τότε $d = 2$ και $F = \mathbb{Q}(\sqrt{2})$.

Τώρα υποθέτουμε ότι $m\geq 2$. Η ομάδα $Gal(F/\mathbb{Q})$ είναι αβελιανή, τάξης 2^m και περιέχει μια υποομάδα τάξης 2^{m-1}. Οπότε το σώμα F περιέχει ένα υπόσωμα H με $[H:\mathbb{Q}] = 2$ και διακρίνουσας δύναμη του $2\Rightarrow H = \mathbb{Q}(\sqrt{2})$. Συνεπώς η

$Gal(F/\mathbb{Q})$ έχει μοναδική υποομάδα τάξης 2^{m-1} και επειδή είναι αβελιανή είναι και κυκλική (Λήμμα 5.3).

Αν K είναι το πραγματικό σώμα του Λήμματος 5.5 και $F \neq K$ θεωρούμε τη σύνθεση FK. Τότε $FK \subseteq \mathbb{R}$, $FK/\mathbb{Q}$ είναι αβελιανή επέκταση βαθμού και διακρίνουσας δύναμης του 2. Δηλαδή η $Gal(FK/\mathbb{Q})$ είναι κυκλική και επιπλέον ισχύει ο ισομορφισμός

$$Gal(FK/K \cap F) \cong Gal(F/F \cap K) \times Gal(K/F \cap K).$$

Όπως στην απόδειξη της Περίπτωσης 1 συμπεραίνουμε ότι είτε $F \subseteq K$ είτε $K \subseteq F$ και λόγω του ότι τα F, K έχουν τον ίδιο βαθμό υπεράνω του $\mathbb{Q}$, $K = F$. □

Πρόταση 2. *Στην Περίπτωση 2, ισχύει και πάλι $L \subseteq \mathbb{Q}(\zeta)$, για κάποια ρίζα της μονάδας ζ.*

Απόδειξη. Αφού τα $\mathbb{Q}(i)$ και L είναι αβελιανές επεκτάσεις του $\mathbb{Q}$ τότε και η σύνθεση $L(i)$ θα είναι. Επίσης παρατηρούμε ότι η επέκταση $L(i)/\mathbb{Q}$ έχει βαθμό και διακρίνουσα δυνάμεις του 2.

Έστω $K = L(i) \cap \mathbb{R}$, τότε η $K/\mathbb{Q}$ είναι πραγματική επέκταση βαθμού και διακρίνουσας δύναμης του 2. Από τα δύο προηγούμενα λήμματα προκύπτει ότι υπάρχει ρίζα της μονάδας ξ με $K \subseteq \mathbb{Q}(\xi)$. Έστω $L(i) = K(a + bi)$, όπου $a, b \in \mathbb{R}$. Ο $a - bi$, ο οποίος είναι συζυγής του $a + bi$ πάνω από το $\mathbb{Q}$ ανήκει στο $L(i)$ οπότε $a \in L(i) \cap \mathbb{R} = K$ και $bi \in L(i) \Rightarrow b^2 \in L(i) \cap \mathbb{R} = K \Rightarrow a + bi$ είναι ρίζα του πολυωνύμου $X^2 - 2aX + (a^2 + b^2) \in K[X]$ οπότε $[L(i) : K] = 2$, αφού $i \notin K \Rightarrow L \subseteq L(i) = K(i) \subseteq \mathbb{Q}(\xi, i) \subseteq \mathbb{Q}(\zeta)$, με ζ πρωταρχική ρίζα της μονάδας τάξης ίσης με το ελάχιστο κοινό πολλαπλάσιο των τάξεων των ξ και i. □

Αναγωγή στις περιπτώσεις 1 και 2

Αν το θεώρημα ισχύει για αβελιανές επεκτάσεις με βαθμό δύναμη πρώτου τότε ισχύει για κάθε πεπερασμένη αβελιανή επέκταση του $\mathbb{Q}$.

Πράγματι, αν L είναι ένα αλγεβρικό σώμα αριθμών το οποίο είναι αβελιανή επέκταση βαθμού n πάνω από το $\mathbb{Q}$ τότε

$$Gal(L/\mathbb{Q}) \cong \prod_{i=1}^{s} \mathcal{H}_i$$

όπου $\mathcal{H}_i$ πεπερασμένες αβελιανές ομάδες με $\#(\mathcal{H}_i) = {p_i}^{h_i}$, p_i πρώτοι αριθμοί και $p_i \neq p_j$ όταν $i \neq j$. Δηλαδή $[L : \mathbb{Q}] = n = \prod_{i=1}^{s} {p_i}^{h_i}$. Θεωρούμε

$\mathcal{L}_i = \prod_{i \neq j} \mathcal{H}_j, \forall i = 1, 2, ..., s$ και L_i να συμβολίζει το σώμα των σταθερών στοιχείων της $\mathcal{L}_i$. Τότε $[L_i : \mathbb{Q}] = {p_i}^{h_i}$. Επιπλέον αν $L_1 L_2 ... L_s$ είναι η σύνθεση των σωμάτων $L_1, ..., L_s$ τότε $Gal(L/L_1 L_2 ... L_s) \subseteq \cap_{i=1}^{s} \mathcal{L}_i = \{id\}$. Άρα $L = L_1 L_2 ... L_s$, δηλαδή $L_i \subseteq \mathbb{Q}(\xi_i)$, όπου ξ_i κάποια ρίζα της μονάδας. Συνεπώς $L = L_1 L_2 ... L_s \subseteq \mathbb{Q}(\xi_1, ..., \xi_s) \subseteq \mathbb{Q}(\zeta)$, με ζ να είναι πρωταρχική ρίζα της μονάδας τάξης ίσης με το ελάχιστο κοινό πολλαπλάσιο των τάξεων των ξ_i για $i = 1, ..., s$

Επομένως αρκεί να δείξουμε τώρα ότι αν L αλγεβρικό σώμα αριθμών με δ_L να είναι δύναμη κάποιου πρώτου p και $[L : \mathbb{Q}] =$ δύναμη του ίδιου πρώτου p, τότε το θεώρημα ισχύει για όλες τις αβελιανές επεκτάσεις του $\mathbb{Q}$ βαθμού δύναμης του p.

Πρόταση 3. *Έστω $L/\mathbb{Q}$ αβελιανή επέκταση βαθμού n. Για κάθε πρώτο αριθμό q, με $q|\delta_L$ και $q \nmid n$, υπάρχει αβελιανή επέκταση $L'/\mathbb{Q}$ τέτοια ώστε $[L' : \mathbb{Q}] \mid n, L \subseteq L'(\xi)$, όπου ξ είναι μια $q-$ ρίζα της μονάδας , $q \nmid \delta_{L'}$. Επίσης αν q' είναι πρώτος που διαιρεί την $\delta_{L'}$, τότε $q' \mid \delta_L$.*

Υποθέτοντας την Πρόταση 3 μπορούμε να συνεχίσουμε ως εξής: Αν $L/\mathbb{Q}$ είναι μια αβελιανή επέκταση βαθμού p^m και δ_L είναι επίσης δύναμη του p, τότε είμαστε ήδη στην Περίπτωση 1 ή στην Περίπτωση 2 και το θεώρημα ισχύει.

Αν υπάρχει πρώτος q, διαφορετικός από τον p , τέτοιος ώστε ο q να διαιρεί την δ_L, από την Πρόταση 3 υπάρχει αβελιανή επέκταση $L_1/\mathbb{Q}$ και μια $q-$ρίζα της μονάδας ξ_1 τέτοια ώστε $L \subseteq L_1(\xi_1), [L_1 : \mathbb{Q}]$ να είναι δύναμη του p και $q \nmid \delta_{L_1}$. Επίσης αν q' είναι οποιοσδήποτε πρώτος με $q' \mid \delta_{L_1} \Rightarrow q' \mid \delta_L$. Άρα η δ_{L_1} έχει λιγότερους πρώτους παράγοντες από την δ_L.

Αν $\delta_{L_1} \neq p^k, \forall k \in \mathbb{N}$ επαναλαμβάνουμε το ίδιο επιχείρημα οπότε υπάρχει αβελιανή επέκταση $L_2/\mathbb{Q}$ και μια ρίζα της μονάδας ξ_2 τέτοια ώστε $L_1 \subseteq L_2(\xi_2), [L_2 : \mathbb{Q}]$ να είναι δύναμη του p και η δ_{L_2} να έχει λιγότερους πρώτους παράγοντες από την δ_{L_1}.

Μετά από πεπερασμένο πλήθος βημάτων φτάνουμε σε μια αβελιανή επέκταση $L_r/\mathbb{Q}$ βαθμού δύναμης του p, $L_{r-1} \subseteq L_r(\xi_r)$ όπου ξ_r είναι μια ρίζα της μονάδας και τελικά δ_{L_r} να είναι δύναμη του p (ίσως να ισούται με $1 \Rightarrow L_r = \mathbb{Q}$). Οπότε από την Περίπτωση 1 ή την Περίπτωση 2 $L_r \subseteq \mathbb{Q}(\xi_{r+1})$, όπου ξ_{r+1} είναι ρίζα της μονάδας.

Τότε $L \subseteq L_1(\xi_1), L_1 \subseteq L_2(\xi_2), ..., L_{r-1} \subseteq L_r(\xi_r), L_r \subseteq \mathbb{Q}(\xi_{r+1})$ και άρα $L \subseteq \mathbb{Q}(\xi_1, \xi_2, ..., \xi_{r+1}) \subseteq \mathbb{Q}(\zeta)$, με ζ είναι μια πρωταρχική ρίζα της μονάδας τάξης ίσης με το ελάχιστο πολλαπλάσιο των τάξεων των $\xi_1, ..., \xi_{r+1}$. Αυτό αποδεικνύει το θεώρημα. Απομένει να αποδείξουμε την Πρόταση 3 :

Απόδειξη Πρότασης 3

Ειδική Περίπτωση Αν το L περιέχει μια πρωταρχική $q-$ ρίζα της μονάδας, έστω ξ.

Τότε $\mathbb{Q} \subseteq \mathbb{Q}(\xi) \subseteq L$ και θεωρούμε $Q \in Spec(R_L)$ τέτοιο ώστε $\mathbb{Q} \cap \mathbb{Z} = q\mathbb{Z}$. Αφού $q \nmid n = [L : \mathbb{Q}] \Rightarrow q \nmid e(Q|q\mathbb{Z})$. Γνωρίζουμε ότι η $G_{\Delta_1}(Q|q\mathbb{Z})$ είναι $q-$ομάδα οπότε $q \mid [L : K_{\Delta_1}] \mid n$ και $L = K_{\Delta_1}$. Ισχύει ότι $e(Q|q\mathbb{Z}) = |G_T/G_{\Delta_1}| = |G_T|$ διαιρεί το $q-1$. (βλ. Πρόταση 4.2.3) Από την άλλη μεριά, $e(Q|q\mathbb{Z}) = e(Q|Q')e(Q'|q\mathbb{Z})$, όπου $Q' = Q \cap R_{\mathbb{Q}(\xi)}$. Όμως $e(Q'|q\mathbb{Z}) = q-1$ (βλ. Πρόταση 3.1.3) άρα $(q-1) \mid e$, δηλαδή $q-1 = e$ και συνεπώς $e(Q|Q') = 1$.

Θεωρούμε $L' := K_T$ και θα δείξουμε ότι ικανοποιεί τις ζητούμενες συνθήκες. Η επέκταση $K_T/\mathbb{Q}$ είναι προφανώς αβελιανή και $[K_T : \mathbb{Q}] \mid n$. Η ομάδα αδρανείας $G_T(Q|Q')$ ισούται με $G_T(Q|Q') = G_T(Q|q\mathbb{Z}) \cap Gal(L/\mathbb{Q}(\xi))$, οπότε $K_T(Q|Q') = K_{\Delta_1}\mathbb{Q}(\xi) = K_{\Delta_1} = L$. Άρα $[L : K_T(\xi)] = e(Q|Q') = 1 \Rightarrow L = K_T(\xi) = L'(\xi)$. Παρατηρούμε ότι $q \nmid \delta_{K_T}$ καθώς ο q δεν διακλαδίζεται στην επέκταση $K_T/\mathbb{Q}$ (Θεώρημα 4.1.1).

Αν q' είναι πρώτος με $q \neq q'$ και $q' \mid \delta_{K_T}$ τότε ο q' διακλαδίζεται στην $K_T/\mathbb{Q}$ οπότε διακλαδίζεται και στην $L/\mathbb{Q}$ και $q' \mid \delta_L$.

Γενική Περίπτωση

Αν ξ είναι μια πρωταρχική $q-$ ρίζα της μονάδας θεωρούμε τη σύνθεση $L(\xi) = L\mathbb{Q}(\xi)$ και έχουμε ότι η $L(\xi)/\mathbb{Q}$ είναι αβελιανή. Έστω $F = L \cap \mathbb{Q}(\xi)$, τότε

$$Gal(L(\xi)/F) \cong Gal(L/F) \times Gal(\mathbb{Q}(\xi)/F)$$

Τότε $[L(\xi) : \mathbb{Q}] = [L(\xi) : F][F : \mathbb{Q}] = [L : F][\mathbb{Q}(\xi) : F][F : \mathbb{Q}] = [L : \mathbb{Q}][\mathbb{Q}(\xi) : F] \mid n(q-1)$.

Τώρα εφαρμόζουμε την ειδική περίπτωση στην αβελιανή επέκταση $L(\xi)/\mathbb{Q}$. Έστω q πρώτος τέτοιος ώστε $q \mid \delta_L$ και $q \nmid n$ τότε ο q διακλαδίζεται στην $L/\mathbb{Q}$ συνεπώς και στην $L(\xi)/\mathbb{Q}$ (ξ πρωταρχική $q-$ ρίζα της μονάδας) δηλαδή $q \mid \delta_{L(\xi)}$. Επίσης $q \nmid [L(\xi) : \mathbb{Q}]$ διότι $[L(\xi) : \mathbb{Q}] \mid n(q-1)$ και $q \nmid n$. Από την ειδική περίπτωση αν $Q \in Spec(R_{L(\xi)})$ τέτοιο ώστε $Q \cap \mathbb{Z} = q\mathbb{Z}$ και K_T είναι το σώμα αδρανείας του Q στην $L(\xi)/\mathbb{Q}$ τότε $K_T(\xi) = L(\xi)$ και

$$[L(\xi) : K_T] = e(Q|q\mathbb{Z}) = q-1$$

και

$$[L(\xi) : \mathbb{Q}] = [L(\xi) : K_T][K_T : \mathbb{Q}] = (q-1)[K_T : \mathbb{Q}]$$

οπότε $[K_T : \mathbb{Q}] \mid n$.

Αφού ο q δεν διακλαδίζεται στην $K_T/\mathbb{Q}$ έπεται ότι $q \nmid \delta_{K_T}$. Τώρα αν q' είναι ένας πρώτος διαφορετικός από τον q με $q' \mid \delta_{K_T}$, δηλαδή ο q' διακλαδίζεται στην $K_T/\mathbb{Q}$ τότε διακλαδίζεται και στην $L(\xi)/\mathbb{Q}$. Δηλαδή διακλαδίζεται στην $L/\mathbb{Q}$ ή στην $\mathbb{Q}(\xi)/\mathbb{Q}$, ισοδύναμα, είτε $q' \mid \delta_L$ είτε $q' \mid \delta_{\mathbb{Q}(\xi)}$. Επειδή όμως ο q' δεν διακλαδίζεται στην $\mathbb{Q}(\xi)/\mathbb{Q}$ έπεται ότι $q' \mid \delta_L$. Επομένως αρκεί να πάρουμε $L' = K_T$. □

Κεφάλαιο 6

Το τοπικό Kronecker-Weber θεώρημα

Θεώρημα 1 (Τοπικό) **.** *Έστω $p \in \mathbb{P}, \mathbb{Q}_p$ το $p-$αδικό σώμα και $K/\mathbb{Q}_p$ μια πεπερασμένη αβελιανή επέκταση. Τότε υπάρχει $n_p \in \mathbb{N}$ τέτοιο ώστε $K \subseteq \mathbb{Q}_p(\zeta_{n_p})$.*

Θεώρημα 2 (global) **.** *Έστω $K/\mathbb{Q}$ πεπερασμένη αβελιανή επέκταση . Υπάρχει $m \in \mathbb{N}$ τέτοιο ώστε $K \subseteq \mathbb{Q}(\zeta_m)$.*

Πρόταση. *Θεώρημα 1, $\forall p \in \mathbb{P} \Rightarrow$ Θεώρημα 2.*

Απόδειξη. Έστω $K/\mathbb{Q}$ μια πεπερασμένη αβελιανή επέκταση και p κάποιος πρώτος, ο οποίος διακλαδίζεται στην $K/\mathbb{Q}$. Αν Q είναι κάποιο πρώτο ιδεώδες του R_K με $Q \mid p\mathbb{Z}$ τότε θεωρούμε την πλήρωση του σώματος K ως πρός το Q, έστω K_Q. Συνεπώς έχουμε την επέκταση τοπικών σωμάτων

$$K_Q/\mathbb{Q}_p.$$

Η επέκταση $K_Q/\mathbb{Q}_p$ είναι Galois. Πράγματι, έστω L/K μια πεπερασμένη επέκταση Galois , $P \in Spec(R_K), Q \in Spec(R_L)$ έτσι ώστε $Q \cap R_K = P$ τότε υπάρχει $\vartheta \in L$ τέτοιο ώστε $L = K(\theta)$ ([2], θεώρημα 2.1, σελίδα 128). Αν $f(X) = Irr(\theta, K)$ εφόσον η L/K είναι Galois όλες οι ρίζες του f θα ανήκουν στο L. Θεωρούμε την πλήρωση του K ως προς το P, έστω K_P. Αν $f(X) = p_1(X)p_2(X)...p_n(X)$ είναι η ανάλυση του f σε γινόμενο αναγώγων πολυωνύμων πάνω από το K_P τότε δίχως βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $p_1(\theta) = 0$ και $L_Q = K_P(\theta)$. Οι συζυγείς του θ πάνω από το

K_P είναι οι ρίζες του $p_1(X)$. Όλες αυτές οι ρίζες ανήκουν στο L και συνεπώς και στο L_Q. Άρα η επέκταση L_Q/K_P είναι επέκταση Galois.

Πρόταση. ***(1)*** $Gal(K_Q/\mathbb{Q}_p) \cong G_Z(Q|p\mathbb{Z})$.
(2) *Η ομάδα αδρανείας μπορεί να υπολογιστεί τοπικά. Δηλαδή*

$$G_T(Q|p\mathbb{Z}) = G_T(L_Q|\mathbb{Q}_p).$$

(χωρίς απόδειξη) [6], Πρόταση 5-4-2, σελίδα 83

Σύμφωνα με το **(1)** της παραπάνω Πρότασης $Gal(K_Q/\mathbb{Q}_p) \leq Gal(K/\mathbb{Q})$ και αφού η $Gal(K/\mathbb{Q})$ είναι αβελιανή τότε και η $Gal(K_Q/\mathbb{Q}_p)$ είναι αβελιανή. Από το Θεώρημα 1, έπεται ότι υπάρχει $n_p \in \mathbb{N}$ τέτοιο ώστε

$$K_Q \subseteq \mathbb{Q}_p(\zeta_{n_p}). \tag{6.1}$$

Έστω $p^{l_p} \mid\mid n_p$ και

$$n := \prod_{p \text{ διακλαδίζεται στο K}} p^{l_p}.$$

Θα αποδείξουμε ότι $K \subseteq \mathbb{Q}(\zeta_n)$.

Έστω $L = K\mathbb{Q}(\zeta_n) = K(\zeta_n)$. Τότε η $L/\mathbb{Q}$ είναι αβελιανή επέκταση Galois. Στην επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ διακλαδίζονται ακριβώς οι πρώτοι διαιρέτες του n (Πρόταση 3.1.6). Όμως το n είναι ένα γινόμενο πρώτων, οι οποίοι είναι ακριβώς αυτοί που διακλαδίζονται στο K. Άρα αν p διακλαδίζεται στην $L/\mathbb{Q}$ τότε θα διακλαδίζεται και στην $K/\mathbb{Q}$ (βλ. Λήμμα 5.4).

Έστω τώρα L_T η πλήρωση του σώματος L, ως προς κάποιο πρώτο ιδεώδες T του L που βρίσκεται πάνω από τον p και $T \mid Q$ (όπου p πρώτος αριθμός διακλαδιζόμενος στο L, άρα και στο K). Ισχύει ότι

$$L_T = K_Q(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{n_p}, \zeta_n) = \mathbb{Q}(\zeta_m)$$

όπου $m :=$εκπ$(n_p, n) \Rightarrow p^l \mid\mid m$, συνεπώς $m = p^l n', n' \nmid p$.

Λήμμα 1. *Για κυκλοτομικές επεκτάσεις του $\mathbb{Q}_p$ ισχύει :*
Η ομάδα αδρανείας της $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ είναι ισόμορφη προς την $(\mathbb{Z}/p^l\mathbb{Z})^*$, όπου $p^l \mid\mid n$.

Απόδειξη. Αν $n = p^l m$, όπου $p \nmid m$ τότε $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p^l m}) = \mathbb{Q}(\zeta_{p^l})\mathbb{Q}(\zeta_m)$. Επομένως

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong Gal(\mathbb{Q}(\zeta_{p^l})/\mathbb{Q}) \times Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/p^l\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \cong H_1 \times H_2.$$

Παρατηρούμε ότι $Fix(H_2) = \mathbb{Q}(\zeta_{p^{l_p}})$. Στην επέκταση $\mathbb{Q}(\zeta_{p^{l_p}})/\mathbb{Q}$ ο p διακλαδίζεται πλήρως (Πρόταση 3.1.3). Δηλαδή $e = \varphi(p^{l_p}), r = 1$ και $f = 1$. Συνεπώς $G_T(P|p\mathbb{Z}) = (\mathbb{Z}/p^{l_p}\mathbb{Z})^*$. Επίσης $p \nmid m$, άρα ο p δεν διακλαδίζεται στην επέκταση $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Τελικά η ομάδα αδρανείας του $p\mathbb{Z}$ στην επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ταυτίζεται με αυτήν της $\mathbb{Q}(\zeta_{p^{l_p}})/\mathbb{Q}$ δηλαδή είναι ισόμορφη με την $(\mathbb{Z}/p^{l_p}\mathbb{Z})^*$. □

Επειδή $p^{l_p} \mid\mid n$ και $p^{l_p} \mid\mid m$ έπεται ότι οι ομάδες αδρανείας των $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ και $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ είναι ισόμορφες προς την $(\mathbb{Z}/p^{l_p}\mathbb{Z})^*$. Από την σχέση $\mathbb{Q}_p(\zeta_n) \leq L_T \leq \mathbb{Q}_p(\zeta_m)$ και την παραπάνω παρατήρηση, έπεται ότι η ομάδα αδρανείας του L_T είναι ισόμορφη με την $(\mathbb{Z}/p^{l_p}\mathbb{Z})^*$, όποτε η τάξη της ισούται με $\varphi(p^{l_p})$.

Έστω G' να είναι η ομάδα που παράγεται από τις ομάδες αδρανείας όλων των πρώτων ιδεωδών του L που βρίσκονται πάνω από το $p\mathbb{Z}$, όταν ο p διακλαδίζεται στο L. Αν $F := Fix(G')$, τότε στην επέκταση $F/\mathbb{Q}$ κανένας πρώτος δεν διακλαδίζεται. Επομένως από το θεώρημα του Minkowski , έπεται ότι $F = \mathbb{Q}$. Δηλαδή $Gal(L/\mathbb{Q}) = G' \Rightarrow [L : \mathbb{Q}] = |G'|$. Από τον ορισμό της G' και το γεγονός ότι η G' είναι αβελιανή

$$|G'| \leq \prod_{p \text{ διακλαδίζεται στο } L} |G_T(L|p\mathbb{Z})| = \prod_{p \text{ διακλαδίζεται στο } K} \varphi(p^{l_p}) = \varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Επειδή όμως $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n) \subseteq L = K(\zeta_n)$ και $[L : \mathbb{Q}] \leq \varphi(n), [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ προκύπτει ότι $K\mathbb{Q}(\zeta_n) = K(\zeta_n) = L = \mathbb{Q}(\zeta_n) \Rightarrow$ και άρα $K \subseteq \mathbb{Q}(\zeta_n)$. □

Κεφάλαιο 7

Νεώτερα σχετικά αποτελέσματα

7.1 Kronecker- Weber μέσω Stickelberger

Το πιο σημαντικό, ίσως, βήμα κατά την απόδειξη του θεωρήματος των Kronecker-Weber είναι η ακόλουθη Πρόταση :

Πρόταση. *Αν $p \in \mathbb{P} \setminus 2$ τότε υπάρχει μοναδική επέκταση $K/\mathbb{Q}$ βαθμού p, με διακρίνουσα δύναμη του p. Αυτή είναι η κυκλική επέκταση $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ και το $\mathbb{Q}(\zeta_p)$ είναι το μοναδικό υπόσωμα του $\mathbb{Q}(\zeta_{p^2})$ βαθμού p πάνω από το $\mathbb{Q}$.*

Ο συγγραφέας δίνει μια διαφορετική απόδειξη για την πρόταση αυτή. Όλο το υπόλοιπο μέρος της απόδειξης του θεωρήματος των Kronecker-Weber παραμένει το ίδιο. Η απόδειξη χρησιμοποιεί το θεώρημα του Stickelberger , ότι η δράση του στοιχείου του Stickelberger

$$\theta := \sum_{\alpha=1}^{p-1} {\sigma_\alpha}^{-1} \in \mathbb{Z}[Gal(F/\mathbb{Q})](\sigma_\alpha : \zeta_p \to {\zeta_p}^\alpha)$$

όπου $\sigma_\alpha : \zeta_p \to {\zeta_p}^\alpha, F = \mathbb{Q}_p$, σε κάθε ιδεώδες του F (ακέραιο ή κλασματικό) μας δίνει κάποιο κύριο ιδεώδες αυτού.

Στα Μαθηματικά και ιδαίτερα στη Θεωρία Αριθμών *γενικά σώματα* λέγονται τα αλγεβρικά σώματα αριθμών (πεπερασμένες επεκτάσεις του $\mathbb{Q}$, υποσώματα του $\mathbb{C}$ καθώς και πεπερασμένες επεκτάσεις του σώματος $\mathbb{F}_q(T)$ των ρητών συναρτήσεων, $q := p^n$, μιας μεταβλητής με συντελεστές από ένα πεπερασμένο

σώμα με $q-$ στοιχεία.) Ο λόγος της κοινής ονομασίας είναι ότι υπάρχουν αρκετές ομοιότητες στην αριθμητική τους. Φυσικά θα πρέπει αμέσως να τονίσουμε ότι υπάρχουν και διαφορές. Είναι λοιπόν φυσικό να εξεταστεί η ισχύς ενός ανάλογου θεωρήματος , αυτού των Kronecker-Weber και στην περίπτωση της θετικής χαρακτηριστικής. Μια ισοδύναμη έκφραση του θεωρήματος των Kronecker-Weber είναι η ακόλουθη :

Το σώμα $\mathbb{Q}^{ab}$, η maximal αβελιανή επέκταση του $\mathbb{Q}$ είναι η ένωση όλων των κυκλοτομικών σωμάτων.

Η πρόταση της προηγούμενης παραγράφου δεν ισχύει πλέον. Υπάρχουν άπειρες κυκλικές επεκτάσεις του $\mathbb{F}_q(T)$ βαθμού p στις οποίες μόνο ένας (fixed) πρώτος διαιρέτης διακλαδίζεται.
Ο D.Hayes [8] κατασκεύασε κυκλοτομικά σώματα συναρτήσεων. Μόνο που στη συγκεκριμένη περίπτωση η ένωση όλων αυτών των κυκλοτομικών σωμάτων δεν ταυτίζεται με την maximal abelian επέκταση του $\mathbb{F}_q(T)$. Ο Hayes αποδεικνύει ότι η maximal αβελιανή επέκταση του K συμπίπτει με τη σύνθεση τριών κατηγοριών σωμάτων.
Την ένωση όλων των κυκλοτομικών σωμάτων, την ένωση όλων των σταθερών επεκτάσεων του $\mathbb{F}_q(X)$ καθώς και την ένωση όλων των υποσωμάτων των αντίστοιχων κυκοτομικών σωμάτων συναρτήσεων για τους οποίους ο **άπειρος** πρώτος διακλαδίζεται πλήρως άγρια (totally widly ramified). Για την απόδειξη ο συγγραφέας χρησιμοποιεί το νόμο αντιστροφής του Artin. Τέλος, στο [3] δημοσιεύεται μια συνδιαστική απόδειξη του θεωρήματος αυτού. Χρησιμοποιείται η αριθμητική των διανυσμάτων του Witt.

Βιβλιογραφία

[1] J.W.S. Cassels, Local Fields, CUP 1986, 151-159 και 235-237

[2] George Bachman, Introduction to p-adic Numbers and Valuation Theory, Academic Press New York, 1964.

[3] J. Cesar Salas-Torres, Martha Rzedowski-Calderon και Gabriel Villa Salvador, A combinatorial proof of the Kronecker-Weber Theorem in positive characteristic, [arXiv : 1367v] [math NT], 12 July 2013.

[4] Gabriel Daniel, Villa Salvador, Topics in the Theory of algebraic function fields, Birkhauser 2006.

[5] B. Delaunay, Zur Bestimmung algebraischer Zahlkorper durch Kongruenzen ; eine Anwendung auf die Abelschen Gleichungen, Crelle, **152** (1923), 122-123.

[6] Larry J. Goldstein, Analytic Number Theory, Prentice Hall

[7] M.J Greenberg, An elementary proof of the Kronecker-Weber Theorem, American Mathematical Monthly **81** (1974), 601-607 και διόρθωση **82** (1975), 803.

[8] D.R Hayes, Explicit class filed theory for rational function fields, Trans. Am. Math. Soc. **189** (1974), 77-91.

[9] D. Hilbert Neuer Beweis des Kronecker'schen Fundamentalsatz uber Abelsche Zahlkorper, Nachrichten Ges. Wiss. Gottingen (1896), 29-39 και Bericht : Die Theorie der algebraischen Zalhkorper, Jahresbericht der Deutschen Mathematiker Vereinigung **4**, 175-546

[10] L. Kronecker, Uber die algebraisch auflosbaren Gleichungen, Sitzungsbericht der Preussen Akademie der Wissenschaften, Berlin 1853, 365-374.

[11] F.Lemmermeyer, Kronecker-Weber via Stickelberger, J. de th. des Nombres de Bordeaux **17** (2005), 555-558.

[12] Yu. I. Manin, A. A. Panchiskin, Introduction to Modern Number Theory, Second Edition, Springer 2008

[13] Wladyslaw Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, PWN-Polish Scientific Publishers
1η έκδοση 1974, 263-269
2η έκδοση 1990, 289-295.

[14] Jurgen Neukirch, Algebraische Zahlentheorie, Springer 1992, 340-341.

[15] Olaf Neumann, Two proofs of the Kronecker-Weber theorem "according to Kronecker and Weber", Crelle **323** (1981), 105-126.

[16] P. Ribenboim, Classical Theory of Algebraic Numbers, Springer, New York 2001.

[17] I. Shaferevich, "A new proof of the Kronecker-Weber Theorem", Collected Mathematical papers, Springer 1989, 54-58.

[18] Rodney Y. Sharp,Steps in Commutative Algebra (London Mathematical Society Student Texts **51**),Cambridge University Press 2000 , 2nd edition.

[19] A. Speiser, Die Zerlegungsgruppe, Crelle **149**, (1919), 174-188.

[20] L.C. Washington, Introduction to Cyclotomic Fields, Springer 1982.

[21] H. Weber, Theorie der Abelschen Zahlkorper I, II, Acta Mathematica (1886) , 8, 193-263, (1887), **9**, 105-130.

[22] H. Weber, Zur Theorie der zyklischen Zahlkorper, Mathematische Annalen **67** (1909), 32-60 και **70** (1911), 459-470.