Εθνικο και Καποδιστριακο Πανεπιστημιο
Αθηνων

Εισαγωγή στη θεωρία κλάσεων σωμάτων

Συγγραφέας:
Γιώργος Κατσιμπρακης

Εισηγητής:
Αριστείδης Κοντογεωργης

5 Μαΐου 2019

Επιτροπή:

Α.Κοντογιώργης, Μ.Μαλιάκας, Ι.Ντόκας

Στους γονείς μου

Περιεχόμενα

Εισαγωγή

Η θεωρία κλάσεων σωμάτων είναι μια θεωρία η οποία στοχεύει στην μελέτη αβελιανών επεκτάσεων σωμάτων. Οι ιστορικές της ρίζες μπορεί να αναζητηθούν στην γενίκευση του νόμου τετραγωνικής αντιστροφής του Gauss. Πράγματι αν $f(x) \in \mathbb{Q}[x]$ είναι ένα ανάγωγο τετραγωνικό πολυώνυμο η διάσπαση του modulo πρώτους p με την βοήθεια του νόμου ανάλυσης (θεώρημα 1.1.9) μπορεί να ταυτιστεί με διάσπαση του ιδεώδους $p\mathscr{O}_K$, στην τετραγωνική επέκταση K που ορίζεται ως το σώμα ριζών του πολυωνύμου f. Αν το $f(x) = x^2 - q$, όπου $q \neq 2$ πρώτος, τότε το σύνολο των πρώτων που διασπώνται στην επέκταση $K/\mathbb{Q}$ δίνονται από το σύνολο

$$\mathrm{Spl}(f(x)) = \{p \in \mathbb{P} : \left(\frac{q}{p}\right) = 1\}.$$

Ο υπολογισμός του παραπάνω συνόλου απαιτεί να υπολογίσουμε άπειρα σύμβολα του Legendre, ενώ ο τετραγωνικός νόμος αντιστροφής του Gauss ανάγει τον υπολογισμό σε πεπερασμένα τέτοια σύμβολα, αφού το q είναι σταθερό και αρκεί να αναλύσουμε την συμπεριφορά του p modulo q για όλους τους πρώτους p.

Ο τετραγωνικός νόμος αντιστροφής μπορεί να επεκταθεί στον νόμος ανάλυσης των κυκλοτομικών πολυωνύμων [5] ο οποίος χαρακτηρίζει τους πρώτους για τους οποίους η αναγωγή του κυκλοτομικού πολυώνυμου διασπάται πλήρως:

$$\mathrm{Spl}(\Phi_n(x)) = \{p \in \mathbb{P} : p \equiv 1 \mod n\},$$

τον οποίο και θα ονομάζουμε και κυκλοτομικό νόμο αντιστροφής.

Το θεώρημα των Kronecker-Weber αναφέρει ότι κάθε αβελιανή επέκταση K του $\mathbb{Q}$ περιέχεται μέσα σε μία κυκλοτομική επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ και συνεπώς χαρακτηρίζεται από μια υποομάδα $H_{K,n} < \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Για κάθε πρώτο p, $p \nmid n$ η παρακάτω ακολουθία είναι είναι ακριβής:

$$1 \to H_{K,n} \hookrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \xrightarrow{\left(\frac{K/\mathbb{Q}}{p\mathbb{Z}}\right)} \mathrm{Gal}(K/\mathbb{Q}) \to 1$$

Δηλαδή το σύμβολο του Αρτιν επάγει ένα ισομορφισμό

$$\frac{(\mathbb{Z}/n\mathbb{Z})^*}{H_{K,n}} \cong \mathrm{Gal}(K/\mathbb{Q}).$$

Έστω ότι η $H_{K,n}$ περιέχει τις κλάσεις

$$H_{K,n} = \{\bar{a}_1, \ldots, \bar{a}_s\}, \quad a_i \in \mathbb{Z}, \bar{a}_i \equiv a_i \mod f_L, (a_i, f_L) = 1.$$

Το σύμβολο του Αρτιν για a_i είναι

$$\left(\frac{K/\mathbb{Q}}{a_i\mathbb{Z}}\right) : \zeta_n \mapsto \zeta_n^{a_i}.$$

Επομένως

$$(p \nmid n \text{ και } \bar{p} \in H) \Leftrightarrow (\bar{p} = \bar{a}_i \text{για κάποιο } i).$$

Ώστε

$$(p \in \mathrm{Spl}(K/\mathbb{Q})) \Leftrightarrow (p \equiv a_i \mod n \text{ για κάποια} a_i),$$

δηλαδή και το σύνολο $\mathrm{Spl}(K/\mathbb{Q})$ χαρακτηρίζεται μέσω ισοδυναμιών, ακριβώς όπως και στον νόμο της τετραγωνικής αντιστροφής.

Ο στόχος της θεωρίας κλάσεων σωμάτων είναι να γενικεύσουμε την παραπάνω κατασκευή στην περίπτωση της μελέτης αβελιανών επεκτάσεων ενός σώματος αριθμών $K \neq \mathbb{Q}$. Δυστυχώς σε αυτή την περίπτωση δεν υπάρχει γενίκευση του θεωρήματος Kronecker-Weber. Απάντηση σε όλα τα προηγούμενα προβλήματα όταν η L/K είναι αβελιανή επέκταση, έδωσε η Θεωρία κλάσεων σωμάτων. Γενικά K είναι λένα σώμα αριθμών ή ένα σώμα συναρτήσεων μιας μεταβλητής (καθολικά σώματα) ή ένα τοπικό σώμα. Η θεωρία κλάσεων σωμάτων έχει πολλές διαφορετικές διατυπώσεις σε πολλές διαφορετικές γλώσσες. Γενικά τα βασικά θεωρήματα αυτής δίνουν μια ισοδυναμία $\psi : \mathrm{Ab}_K \to \mathrm{Sub}_X$ ανάμεσα στην κατηγορία των αβελιανών επεκτάσεων του K και την κατηγορία Sub_X των ανοικτών υποομάδων μιας τοπικά συμπαγούς αβελιανής ομάδας $X = X(K)$ η οποία ορίζεται αποκλειστικά σε όρους του σώματος K. Η ομάδα $X(K)$ στην περίπτωση των καθολικών σωμάτων είναι η idele class group ή η πολλαπλασιαστική ομάδα K^* στην περίπτωση που το K είναι τοπικό σώμα. Ο ορισμός της αντί-ισοδυναμίας απεικονίζει μια αλγεβρική επέκταση L/K στην εικόνα της $N_{L/K}X(L) \subset X(K)$. Το θεώρημα ύπαρξης εξασφαλίζει ότι κάθε ανοικτή υποομάδα $H \subset X(K)$ είναι της μορφής $N_{L/K}X(L)$ για κάποια L/K αβελιανή επέκταση, το λεγόμενο σώμα κλάσεων της H.

Ακολουθούμε το βιβλίο της Childress [2] και αρχίζουμε στο πρώτο κεφάλαιο περιγράφοντας βασικά θεωρήματα από την αλγεβρική θεωρία αριθμών που θα μας χρησιμέψουν στην συνέχεια. Στο δεύτερο κεφάλαιο αφού ορίσουμε τους χαρακτήρες Dirichlet αναφερόμαστε στην συνάρτηση L, αποδεικνύουμε το γινόμενο Euler και παρουσιάζουμε το θεώρημα Dirichlet για πρώτους σε αριθμητικές προόδους. Επιπλέον ορίζουμε την πυκνότητα Dirichlet που θα μας χρησιμέψει για να ορίσουμε στο επόμενο κεφάλαιο το σώμα κλάσεων (class field). Στο τρίτο κεφάλαιο αναφέρουμε το θεώρημα προσέγγισης, ορίζουμε τα ray class groups και το γεγονός ότι η αυστηρή ray class group είναι πεπερασμένη και αποδεικνύουμε την γενίκευση του θεωρήματος Dirichlet. Τέλος αναφέρουμε τα κυριότερα θεωρήματα της θεωρίας κλάσεων σωμάτων.

Γιώργος Κατσιμπράκης
Αθήνα 2019

Κεφάλαιο 1

Στοιχεία Σωμάτων Αριθμών

1.1 Σώματα αριθμών

Ορισμός 1.1.1. *Ένα σώμα αριθμών είναι μια πεπερασμένη επέκταση του* $\mathbb{Q}$.

Ορισμός 1.1.2. *Εάν F σώμα τότε ένα κλασματικό ιδεώδες του F είναι κάθε μη μηδενικό πεπερασμένα παραγόμενο $\mathscr{O}_F$ - submodule του F όπου $\mathscr{O}_F$ είναι ο δακτύλιος των αλγεβρικών ακέραιων του F.*

Παρατήρηση 1.1.3. *Αποδεικνύεται ότι ο $\mathscr{O}_F$ είναι δακτύλιος Dedekind.*

Με I_F συμβολίζουμε την ομάδα των κλασματικών ιδεωδών του F που έχει ως πράξη τον πολλαπλασιασμό ιδεωδών, μονάδα τον δακτύλιο $\mathscr{O}_F$ και που για κάθε $\alpha \in I_F$ ορίζεται ως αντίστροφο στοιχείο το κλασματικό ιδεώδες:

$$\alpha^{-1} = \{x \in F : x\alpha \subset \mathscr{O}_F\}.$$

Με P_F συμβολίζουμε την ομάδα των κύριων κλασματικών ιδεωδών του F, που είναι κανονική υποομάδα της I_F.

Ορισμός 1.1.4. *Ορίζεται έτσι η ομάδα πηλίκο $C_F = I_F/P_F$ που λέγεται ideal class group. Έχει αποδειχθεί ότι για κάθε σώμα αριθμών η ideal class group C_F έχει πεπερασμένη τάξη που την συμβολίζουμε με h_F και που λέγεται class number.*

Ισχύει το εξής θεώρημα που είναι σχετικό με την ανάλυση ενός πρώτου ιδεώδους του δακτυλίου $\mathscr{O}_F$ σε γινόμενο πρώτων ιδεωδών του δακτυλίου $\mathscr{O}_K$, όπου K/F πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών:

Θεώρημα 1.1.5. *Έστω K/F πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{p}$ μη μηδενικό και πρώτο ιδεώδες του δακτυλίου $\mathscr{O}_F$. Τότε ισχύει:*

$$\mathfrak{p}\mathscr{O}_F = \mathfrak{B}_1^{e_1}\mathfrak{B}_2^{e_2}\cdots\mathfrak{B}_g^{e_g}$$

όπου B_i πρώτα ιδεώδη του $\mathscr{O}_K$ διαφορετικά μεταξύ τους και $e_i, g = g(\mathfrak{p})$ θετικοί ακέραιοι.

Επειδή ο δακτύλιος $\mathscr{O}_K$ είναι Dedekind η παράσταση αυτή είναι μοναδική. Ο αριθμός e_i λέγεται δείκτης διακλάδωσης του $\mathfrak{B}_i$ υπέρ του $\mathfrak{p}$ και τον συμβολίζουμε $e_i = e_i\ (\mathfrak{B}_i/\mathfrak{p})$. Επειδή οι δακτύλιοι $\mathscr{O}_K$ και $\mathscr{O}_F$ είναι Dedekind, κάθε πρώτο ιδεώδες είναι μέγιστο. Συνεπώς οι δακτύλιοι $\mathscr{O}_K/\mathfrak{B}_i$ και $\mathscr{O}_F/\mathfrak{p}$ είναι σώματα. Το σώμα $\mathscr{O}_F/\mathfrak{p}$ μπορεί να θεωρηθεί υπόσωμα του $\mathscr{O}_K/\mathfrak{B}_i$. Επιπλέον αν ισχύει η ιδιότητα της πεπερασμένης νόρμας, τα παραπάνω σώματα είναι πεπερασμένα σώματα χαρακτηριστικής p όπου: $p = \mathbb{Z} \cap \mathfrak{p}$. Ορίζεται συνεπώς ο θετικός ακέραιος $f_i = f_i(\mathfrak{B}_i/\mathfrak{p})$ να είναι ο δείκτης $[\mathscr{O}_K/\mathfrak{B}_i : \mathscr{O}_F/\mathfrak{p}]$ που ονομάζεται βαθμός αδράνειας του B_i υπέρ του $\mathfrak{p}$. Τότε ισχύει:

$$[K : F] = \sum_{n=1}^{g} f_i e_i$$

Εάν επιπλέον η επέκταση K/F είναι Galois τότε η ομάδα Galois $G = G(K/F)$ δρα μεταβατικά στο σύνολο $\{\mathfrak{B}_1, \mathfrak{B}_2, \dots, \mathfrak{B}_g\}$, δηλαδή για κάθε ζεύγος $\mathfrak{B}_i, \mathfrak{B}_j$ υπάρχει $\sigma \in G$ έτσι ώστε $\sigma(\mathfrak{B}_i) = (\mathfrak{B}_j)$. Επειδή κάθε ιδεώδες του $\mathscr{O}_K$ γράφεται μονοσήμαντα σε γινόμενο πρώτων ιδεωδών αφού ο $\mathscr{O}_K$ είναι δακτύλιος Dedekind άρα

$$\mathfrak{p}\mathscr{O}_F = (\mathfrak{B}_1 \mathfrak{B}_2 \dots \mathfrak{B}_g)^e$$

όπου $e = e_1 = e_2 = \cdots = e_g$. Τότε ισχύει:

$$[K : F] = efg,$$

όπου $f = f_1 = f_2 = \cdots = f_g$.

Στην συνέχεια θα ορίσουμε τα εξής:

Ορισμός 1.1.6. *Εαν K/F πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathscr{O}_F$ με:*

$$\mathfrak{p}\mathscr{O}_F = \mathfrak{B}_1^{e_1} \mathfrak{B}_2^{e_2} \dots \mathfrak{B}_g^{e_g},$$

όπου B_i πρώτα ιδεώδη του $\mathscr{O}_K$ διαφορετικά μεταξύ τους και $e_i, g = g(\mathfrak{p})$ θετικοί ακέραιοι. Θα λέμε ότι

- *το $\mathfrak{p}$ διακλαδίζεται πλήρως στην K/F αν $g = 1$,*
- *το $\mathfrak{p}$ δεν διακλαδίζεται στην K/F αν $e_i = e_i\ (\mathfrak{B}_i/\mathfrak{p}) = 1$ για κάθε i,*
- *το $\mathfrak{p}$ παραμένει αδρανές στην K/F αν το $\mathfrak{p}\mathscr{O}_K$ είναι πρώτο ιδεώδες του $\mathscr{O}_K$*
- *$\mathfrak{p}$ διασπάται πλήρως στην K/F αν $g = [K : F]$.*

Στην συνέχεια θα ορίσουμε τον οδηγό, με την βοήθεια του οποίου θα διατυπώσουμε το θεώρημα Dedekind - Kummer. Με τη βοήθεια του θεωρήματος αυτού μπορούμε να βγάλουμε συμπεράσματα γύρω από την φύση της ανάλυσης του $\mathfrak{p}$ στον δακτύλιο $\mathscr{O}_K$ παρότι το θεώρημα δεν είναι πλήρες. Και αυτό γιατί ένας πεπερασμένος αριθμός από ιδεώδη αποκλείονται και μόνο τα πρώτα ιδεώδη που είναι σχετικά πρώτα με τον οδηγό λογαριάζονται.

Ορισμός 1.1.7. *Έστω L/K διαχωρίσιμη επέκταση με $\theta \in \mathscr{O}_L$ πρωταρχικό στοιχείο. Ονομάζουμε οδηγό $\mathscr{F}$ του δακτυλίου $\mathscr{O}_K[\theta]$ το μεγαλύτερο ιδεώδες του $\mathscr{O}_L$ που περιέχεται στο $\mathscr{O}_K[\theta]$. Ισχύει δηλαδή:*

$$\mathscr{F} = \{x \in \mathscr{O}_L / x\mathscr{O}_L \in \mathscr{O}_K[\theta]\}$$

Παρατήρηση 1.1.8. *Επειδή αποδεικνύεται ότι ο δακτύλιος $\mathscr{O}_L$ είναι $\mathscr{O}_K$ − module έχουμε ότι $\mathscr{F} \neq 0$.*

Θεώρημα 1.1.9. *Dedekind - Kummer Έστω L/K πεπερασμένη επέκταση αλγεβρικών σωμάτων αριθμών με $\mathscr{O}_L = \mathscr{O}_K[\theta]$ και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathscr{O}_K$ σχετικά πρώτο με τον οδηγό $\mathscr{F}$ του δακτυλίου $\mathscr{O}_K[\theta]$. Εάν:*

$$\overline{g(X)} = \overline{g_1(X)}^{e_1} \dots \overline{g_k(X)}^{e_k}$$

η παραγοντοποίηση του $\overline{g(X)} = g(X) \mathrm{mod} \mathfrak{p}$ σε διακεκριμένα μονικά ανάγωγα πολυώνυμα $\overline{g_i(X)} = g_i(X) \mathrm{mod} \mathfrak{p}$ υπέρ του σώματος κλάσεων υπολοίπων $\mathscr{O}_K/\mathfrak{p}$ με $g_i(X) \in \mathscr{O}_K[X]$ μονικά πολυώνυμα τότε τα:

$$B_i = \mathfrak{p}\mathscr{O}_L + g_i(\theta)\mathscr{O}_L$$

για $i = 1, 2, \dots, k$ είναι όλα διακεκριμένα πρώτα ιδεώδη του $\mathscr{O}_L$ πάνω από το $\mathfrak{p}$ και ισχύουν:

$$f_i = f_i(B_i/\mathfrak{p}) = \deg \overline{g_i(x)}$$
$$\mathfrak{p}\mathscr{O}_L = B_1^{e_1} \dots B_k^{e_k}$$

.

Χρήσιμη είναι και έννοια της διακρίνουσας. Έχουμε τον ορισμό:

Ορισμός 1.1.10. *Έστω K/F μια πεπερασμένη επέκταση σωμάτων αριθμών και $\{u_1, \dots, u_n\}$ μια F - βάση του K.Ορίζουμε ως διακρίνουσα αυτής της βάσης και συμβολίζουμε με $d_{K/F} = d_{K/F}(u_1, \dots u_n)$ να είναι το στοιχείο:*

$$d_{K/F} = \det(\sigma_i(\alpha_j)))^2$$

όπου $\sigma_1, \dots, \sigma_n : K \hookrightarrow F^{\mathrm{alg}}$ οι F - μονομορφισμοί του K.

Παρατήρηση 1.1.11. *Ισχύει και η σχέση: $d = d[\mathrm{Tr}_{K/F}(u_i u_j)]$*

Αποδεικνύεται ότι $d_{K/F} \in F$. Επιπλέον αν $u_i \in \mathscr{O}_L$ ισχύει ότι $d_{K/F} \in \mathscr{O}_F$.

Εάν έχουμε δύο F - βάσεις του K τις $\{u_1, \dots, u_n\}$ και $\{\omega_1, \dots, \omega_n\}$ τότε η σχέση που έχουν οι διακρίνουσες αυτών των βάσεων μεταξύ τους μπορεί να περιγραφεί με την βοήθεια του πίνακα αλλαγής βάσης: Εάν $(\omega_1, \dots, \omega_n)^t = A(u_1, \dots u_n)^t$ τότε ισχύει:

$$d(\omega_1, \dots, \omega_n) = (\det A)^2 d(u_1, \dots u_n)$$

Στην ειδική περίπτωση που η επέκταση K/F είναι απλή με πρωταρχικό στοιχείο το α και $[K : F] = n$ τότε ο πίνακας $[\sigma_i(\alpha^{j-1})]$ είναι Vandermonde συνεπώς η διακρίνουσα δίνεται από την σχέση:

$$d(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\alpha) - \sigma_j(\alpha))$$

Ορισμός 1.1.12. *Εάν L/K επέκταση αλγεβρικών σωμάτων αριθμών και θ πρωταρχικό στοιχείο με:*

$$\alpha\theta^i = \sum_{j=0}^{n-1} \alpha_{j,i}\theta^j$$

όπου $\alpha \in L$ και $\{1, \theta, \ldots, \theta^{n-1}\}$ βάση της επέκτασης, τότε ο πίνακας $A(\alpha) = (\alpha_{ji})$ λέγεται πίνακας παράστασης του α. Η ορίζουσα του πίνακα αυτού λέγεται norm του α και την συμβολίζουμε $N_{L/K}(\alpha)$.

Παρατήρηση 1.1.13. *Αποδεικνύεται ότι η απεικόνιση της νόρμας*

$$N_{L/K} : L^* \to K^*$$

είναι μορφισμός ομάδων.

Ειδικά αν $\mathscr{O}_K = \mathscr{O}_F[\alpha]$ και το πολυώνυμο $f(X)$ είναι το ανάγωγο πολυώνυμο του α υπέρ F τότε συνδέεται η ορίζουσα με την διακρίνουσα ως εξής:

$$N_{K/F}(f'(\alpha)) = (-1)^{\frac{n(n-1)}{2}} d(1, \alpha, \ldots, \alpha^{n-1}).$$

Η έννοια της νόρμας επεκτείνεται και σε ιδεώδη σύμφωνα με τα παρακάτω:

Ορισμός 1.1.14. *Έστω K/F πεπερασμένη επέκταση σωμάτων αριθμών $\mathfrak{p}$ ένα μη μηδενικό πρώτο ιδεώδες του $\mathscr{O}_F$ και $\mathscr{B}$ πρώτο ιδεώδες του $\mathscr{O}_K$ πάνω από το $\mathfrak{p}$. Η norm του $\mathscr{B}$ ορίζεται ως:*

$$N_{K/F}(\mathscr{B}) = \mathfrak{p}^{f(\mathscr{B}/\mathfrak{p})}.$$

Η norm επεκείνεται πολλαπλασιαστικά για κάθε κλασματικό ιδεώδες του K:

$$N_{K/F}(\mathscr{B}^{\alpha_1}, \ldots, \mathscr{B}^{\alpha_t}) = N_{K/F}(\mathscr{B})^{\alpha_1} \ldots N_{K/F}(\mathscr{B})^{\alpha_t}.$$

Συνεπώς η norm ενός κλασματικού ιδεώδους του K είναι κλασματικό ιδεώδες του F. Ειδικά αν η επέκταση K/F είναι Galois τότε ισχύει:

$$N_{K/F}(\mathscr{U})\mathscr{O}_K = \prod_{\sigma \in G(K/F)} \sigma(\mathscr{U})$$

Η norm στοιχείου και η norm ιδεώδους συνδέονται. Πράγματι αν $\alpha \in K$ τότε:

$$N_{K/F}(\alpha\mathscr{O}_K) = N_{K/F}(\alpha)\mathscr{O}_F.$$

Επιπλέον αν $F \subset E \subset K$ σώματα αριθμών ισχύει:

$$N_{K/F} = N_{E/F} \circ N_{K/E}.$$

Ορισμός 1.1.15. *Έστω η Galois επέκταση K/F σωμάτων αριθμών με ομάδα Galois την G. Έστω επίσης ένα μη μηδενικό πρώτο ιδεώδες $\mathfrak{p}$ του $\mathscr{O}_F$ και ένα πρώτο ιδεώδες $\mathscr{B}$ του $\mathscr{O}_K$ πάνω από το $\mathfrak{p}$. Η ομάδα αναλύσεως του $\mathscr{B}$ υπέρ το $\mathfrak{p}$ ορίζεται ως:*

$$Z(\mathscr{B}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathscr{B}) = \mathscr{B}\}.$$

Η ομάδα αναλύσεως αλλιώς συμβολίζεται με $G_z = G_z(\mathscr{B}/\mathfrak{p})$.

Παρατήρηση 1.1.16. *Η $Z(\mathscr{B}/\mathfrak{p})$ δρα στο πεπερασμένο σώμα $\mathscr{F}_B = \mathscr{O}_K/\mathscr{B}$ αφήνοντας σταθερό το υπόσωμα $\mathscr{F}_\mathfrak{p} = \mathscr{O}_F/\mathfrak{p}$ και ορίζεται έτσι ένας φυσικός ομομορφισμός ομάδων:*

$$Z(\mathscr{B}/\mathfrak{p}) \to G(\mathscr{F}_B/\mathscr{F}_\mathfrak{p}).$$

Θεώρημα 1.1.17. *Έστω K/F επέκταση Galois σωμάτων αριθμών με ομάδα Galois την G. Έστω επίσης $\mathfrak{p}$ ένα μη μηδενικό πρώτο ιδεώδες του $\mathscr{O}_F$. Ισχύουν τα ακόλουθα:*

i Η ομάδα G δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών $\mathscr{B}$ του $\mathscr{O}_K$ που βρίσκονται πάνω από το $\mathfrak{p}$ και ισχύει: $[G : Z(\mathscr{B}/\mathfrak{p})] = \#\{$ πρώτοι $\mathscr{B}$ του $\mathscr{O}_K : \mathscr{B}|\mathfrak{p}\mathscr{O}_K\} = g$. Επίσης αν $\mathscr{B}, \mathscr{B}'$ είναι πρώτα ιδεώδη του $\mathscr{O}_K$ πάνω από το $\mathfrak{p}$ τότε οι $Z(\mathscr{B}/\mathfrak{p})$ και $Z(\mathscr{B}'/\mathfrak{p})$ είναι G - συζυγείς.

ii Ισχύουν ότι: $N\mathfrak{p} = \#\mathscr{F}_\mathfrak{p}$, $N\mathscr{B} = \#\mathscr{F}_\mathscr{B}$ και η ομάδα Galois $G(\mathscr{F}_\mathscr{B}/\mathscr{F}_\mathfrak{p})$ είναι κυκλική και παράγεται από τον αυτομορφισμό του Frobenius $\phi_\mathfrak{p} : x \mapsto x^{N_\mathfrak{p}}$

iii Ο ομομορφισμός

$$Z(\mathscr{B}/\mathfrak{p}) \to G(\mathscr{F}_\mathscr{B}/\mathscr{F}_\mathfrak{p})$$

είναι επί, ο πυρήνας του λέγεται ομάδα αδρανείας που συμβολίζεται με $T(\mathscr{B}/\mathfrak{p})$. Είναι $[Z(\mathscr{B}/\mathfrak{p}) : T(\mathscr{B}/\mathfrak{p})] = f$ και η ομάδα $T(\mathscr{B}/\mathfrak{p})$ έχει τάξη e.

Εάν K/F επέκταση Galois από το θεμελιώδες θεώρημα της θεωρίας Galois ξέρουμε ότι οι ομάδες αναλύσεως και αδρανείας αντιστοιχίζονται στα σταθερά υποσώματα τους που είναι ενδιάμεσα σώματα και λέγονται σώμα αναλύσεως K_Z και αδρανείας K_T αντίστοιχα.

Για αβελιανές επεκτάσεις η παραγοντοποίηση των ιδεωδών που παράγονται από το $\mathfrak{p}$ στα παραπάνω ενδιάμεσα σώματα περιγράφεται από το παρακάτω θεώρημα:

Θεώρημα 1.1.18. *Έστω K/F αβελιανή επέκταση σωμάτων αριθμών και $\mathfrak{p}$ ενα πρώτο ιδεώδες του $\mathscr{O}_F$. Τότε το $\mathfrak{p}$ διασπάται πλήρως στην K_Z/F. Ακόμη οι πρώτοι πάνω από το $\mathfrak{p}$ παραμένουν αδρανείς στην K_T/K_Z και διακλαδίζονται πλήρως στην K/K_T.*

Αν $e = e(\mathscr{B}/\mathfrak{p}) = 1$ τότε από τον φυσικό ομομορφισμό

$$Z(\mathscr{B}/\mathfrak{p}) \to G(\mathscr{F}_\mathscr{B}/\mathscr{F}_\mathfrak{p})$$

έχουμε ότι οι ομάδες $Z(\mathscr{B}/\mathfrak{p})$ και $G(\mathscr{F}_\mathscr{B}/\mathscr{F}_\mathfrak{p})$ είναι ισόμορφες κυκλικές ομάδες τάξεως f. Η ομάδα Galois για τα σώματα υπολοίπων παράγεται από τον αυτομορφισμό του Frobenius ϕ_P και υπάρχει μοναδικό στοιχείο $\sigma \in Z(\mathscr{B}/\mathfrak{p})$ που αντιστοιχεί στον $\phi_\mathfrak{p}$ μέσω του φυσικού ισομορφισμού. Έχουμε ότι: $Z(\mathscr{B}/\mathfrak{p}) = \langle\sigma\rangle$. Το στοιχείο σ λέγεται το στοιχείο του Frobenius στο $\mathscr{B}$. Το συμβολίζουμε με $\sigma = (\frac{\mathscr{B}}{K/F}) = (\mathscr{B}, K/F)$. Για το στοιχείο του Frobenius έχουμε την παρακάτω πρόταση:

Πρόταση 1.1.19. *Έστω K/F επέκταση Galois σωμάτων αριθμών, $\mathfrak{p}$ ενα πρώτο ιδεώδες του $\mathscr{O}_F$ που δεν διακλαδίζεται στην K/F και $\mathscr{B}$ ένα πρώτο ιδεώδες του*

$\mathscr{O}_K$ με $\mathscr{B}|\mathfrak{p}\mathscr{O}_K$. Τότε το στοιχείο του Frobenius στο $\mathscr{B}$ είναι το μοναδικό στοιχείο $\sigma \in G(K/F)$ που ικανοποιεί τη σχέση:

$$\sigma(\alpha) \equiv \alpha^{N_{\mathfrak{p}}} \operatorname{mod}\mathscr{B}$$

για κάθε $\alpha \in \mathscr{O}_K$.

Ορισμός 1.1.20. *Αν υποθέσουμε επιπλέον ότι η G είναι αβελιανή τότε από το πρώτο σκέλος του θεωρήματος 1.1.17 έπεται ότι η $Z(\mathscr{B}/\mathfrak{p})$ εξαρτάται μόνο από το $\mathfrak{p}$ και γι αυτό μπορούμε να γράψουμε $Z(\mathfrak{p})$. Επίσης αν το $\mathfrak{p}$ δεν διακλαδίζεται στην K/F θα αποδείξουμε στην πρόταση 1.1.21 που ακολουθεί ότι το στοιχείο του Frobenius στο $\mathscr{B}$ εξαρτάται μόνο από το $\mathfrak{p}$. Σε αυτή την περίπτωση το ονομάζουμε ο αυτομορφισμός του Artin για το $\mathfrak{p}$ και συμβολίζουμε $(\frac{\mathfrak{p}}{K/F}) = (\mathfrak{p}, K/F)$.*

Ορίζεται και η απεικόνιση:
{ πρώτοι του $\mathscr{O}_K$ που δεν διακλαδίζονται στην $/F$ } $\to G$ με:

$$\mathfrak{p} \mapsto \sigma_{\mathfrak{p}} = \left(\frac{\mathfrak{p}}{K/F}\right).$$

Πρόταση 1.1.21. *Έστω K/F αβελιανή επέκταση σωμάτων αριθμών, $\mathfrak{p}$ ενα πρώτο ιδεώδες του $\mathscr{O}_F$ που δεν διακλαδίζεται στην K/F και $\mathscr{B}$ ένα πρώτο ιδεώδες του O_K με $\mathscr{B}|\mathfrak{p}O_K$. Τότε το $\sigma = (\frac{\mathfrak{p}}{K/F})$ δεν εξαρτάται από την επιλογή του πρώτου $\mathscr{B}$ που είναι πάνω από το $\mathfrak{p}$.*

Πρόταση 1.1.22. *Έστω K/F αβελιανή επέκταση σωμάτων αριθμών με ομάδα Galois την G και $F \subset L \subset K$. (Άρα L/F, K/L επίσης αβελιανές). Έστω επίσης $\mathfrak{p}$ πρώτο ιδεώδες στον $\mathscr{O}_F$ που δεν διακλαδίζεται στην K/F. Τότε ορίζονται τα $(\frac{\mathfrak{p}}{L/F})$ και $(\frac{\mathfrak{p}}{K/F})$ και ισχύει: $(\frac{\mathfrak{p}}{L/F}) = (\frac{\mathfrak{p}}{K/F})|_L$.*

Θεώρημα 1.1.23. *Έστω $K \subset \mathbb{Q}(\zeta_m)$ τότε ταυτίζουμε $G(\mathbb{Q}_m/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ και έστω $H < (\mathbb{Z}/m\mathbb{Z})^\times$ η υποομάδα που αντιστοιχεί στην $G(\mathbb{Q}(\zeta_m)/K)$. Τότε οι πρώτοι $p|m$ που αναλύονται πλήρως στην $K/\mathbb{Q}$ είναι ακριβώς αυτοί οι p για τους οποίους ισχύει $p \operatorname{mod} m \in H$.*

Ας συμβολίσουμε τώρα με r_1 το πλήθος των εμφυτεύσεων $F \hookrightarrow \mathbb{R}$ και με r_2 το πλήθος των συζυγών εμφυτεύσεων $F \hookrightarrow \mathbb{C}$. Τότε $[F : \mathbb{Q}] = r_1 + 2r_2$. Η ομάδα $\mathscr{O}_F^\times$ περιγράφεται από το επόμενο θεώρημα:

Θεώρημα 1.1.24 (Το θεώρημα μονάδων του Dirichlet)**.** *Έστω F σώμα αριθμών και ας συμβολίσουμε με r_1 και r_2 το πλήθος των πραγματικών εμφυτεύσεων και συζυγών ζευγών από φανταστικές εμφυτεύσεις του F αντίστοιχα. Τότε υπάρχουν μονάδες $\epsilon_1, \dots, \epsilon_{r_1+r_2-1} \in \mathscr{O}_F^\times$ τέτοιες ώστε:*

$$\mathscr{O}_F^\times \cong W_F \times \langle\epsilon_1\rangle \times \cdots \times \langle\epsilon_{r_1+r_2-1}\rangle \cong W_F \times \mathbb{Z}^{r_1+r_2-1}$$

όπου W_F είναι η ομάδα των ριζών της μονάδας στο F. Τα στοιχεία ϵ_j λέγονται θεμελιώδες σύστημα μονάδων για το F.

Ειδικά για τις κυκλοτομικές επεκτάσεις αξίζει να αναφέρουμε τα εξής:

Θεώρημα 1.1.25. *Έστω θ μια q-οστη πρωταρχική ρίζα της μονάδας όπου $q = p^\alpha$ με α θετικό ακέραιο και R ο δακτύλιος των αλγεβρικών ακέραιων στο $\mathbb{Q}(\theta)$.*

(i) $[\mathbb{Q}(\theta) : \mathbb{Q}] = \phi(q) = p^{\alpha-1}(p-1)$.

(ii) *Το πολυώνυμο:*

$$\Phi_q(X) = \frac{X^{p^\alpha} - 1}{X^{p^{\alpha-1}} - 1} = t^{p-1} + t^{p-2} + \ldots + 1,$$

όπου $t = X^{p^{\alpha-1}}$

(iii) *Το στοιχείο* $\alpha = 1 - \theta$ *παράγει ένα πρώτο ιδεώδες* αR *στο* R *και* $pR = (\alpha R)^{\phi(q)}$. *Ο σχετικός βαθμός του* αR *υπέρ* $\mathbb{Z}$ *είναι 1.*

(iv) *Εάν* $q > 2$ *τότε ο* p *εχει δείκτη διακλάδωσης* $e = \phi(q) > 1$ *και το ιδεώδες* (p) *είναι το μοναδικό πρώτο ιδεώδες του* $\mathbb{Z}$ *που διακλαδίζεται στον* R.

(v) $R = \mathbb{Z}[\theta]$.

(vi) $\Delta(1, \theta, \ldots, \theta^{\phi(q)-1})) = \pm p^{p^{\alpha-1}}(\alpha p - \alpha - 1)$ *όπου το πρόσημο* $+$ *εμφανίζεται αν και μόνο αν* $p \equiv 1 \text{mod} 4$ *ή αν* $q = 2^\alpha$ *με* $\alpha > 2$.

Πρόταση 1.1.26. *Εάν p πρώτος αριθμός που δεν διαιρεί τον θετικό ακέραιο m τότε ο p έχει δείκτη διακλάδωσης $e = 1$ στο $\mathbb{Q}(\theta m)$.*

Θεώρημα 1.1.27. *Η ομάδα Galois του $\mathbb{Q}(\theta_m)$ υπερ το $\mathbb{Q}$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα των κλάσεων υπολοίπων $(\mathbb{Z}/m)^*$ των ακεραίων πρώτων με τον m modulo m.*

Θεώρημα 1.1.28. *Ο δακτύλιος των αλγεβρικών ακεραίων στο $\mathbb{Q}(\theta_m)$ είναι $\mathbb{Z}[\theta_m]$ όπου θ_m είναι μια m-οστη πρωταρχική ρίζα της μονάδας.*

1.2 Πληρώσεις σωμάτων αριθμών

Οι πληρώσεις ενός σώματος αριθμών στην θεωρία κλάσεων σωμάτων έχουν σημαντικό ρόλο. Θα αναφέρουμε μερικά βασικά στοιχεία σχετικά με αυτές.

Ορισμός 1.2.1. *Έστω ένα αλγεβρικό σώμα αριθμών F. Μια απόλυτη τιμή στο F είναι μια απεικόνιση $F \to [0, \infty)$ που την εικόνα κάθε στοιχείου $x \in F$ την συμβολίζουμε με $|x|$ που ικανοποιεί τις ιδιότητες:*

(i) $|x| = 0$ *αν και μόνο αν* $x = 0$

(ii) $|x \cdot y| = |x| \cdot |y|$ *για κάθε* $x, y \in F$

(iii) $|x + y| \leq |x| + |y|$ *για κάθε* $x, y \in F$

Μια μη Αρχιμήδεια απόλυτη τιμή είναι μια απόλυτη τιμή που ικανοποιεί την ισχυρότερη συνθήκη:

(iv) $|x + y| \leq max\{|x|, |y|\}$ *για κάθε* $x, y \in F$

Εάν $|\cdot|$ είναι μια απόλυτη τιμή στο F τότε ορίζεται μια μετρική d στο F από τη σχέση: $d(x,y)=|x-y|$. Δύο απόλυτες τιμές στο F είναι ισοδύναμες αν ορίζουν την ίδια τοπολογία από τις μετρικές τους.

Ορισμός 1.2.2. *Για να ορίσουμε μια μη Αρχιμήδεια απόλυτη τιμή στο σώμα αριθμών F θεωρούμε $\mathfrak{p}$ ενα μη μηδενικό πρώτο ιδεώδες του δακτυλίου $\mathcal{O}_F$. Εάν $x\in F^{\times}$ τότε το ιδεώδες $x\mathcal{O}_F$ αναλύεται σε γινόμενο πρώτων ιδεωδών του $\mathcal{O}_F$:*

$$x\mathcal{O}_F = \mathfrak{p}^{\alpha}{\mathfrak{p}_1}^{\alpha_1}\dots{\mathfrak{p}_t}^{\alpha_t}$$

όπου τα πρώτα ιδεώδη $\mathfrak{p},\mathfrak{p}_1,\dots,\mathfrak{p}_t$ είναι όλα διακεκριμένα μεταξύ τους και οι αριθμοί $\alpha,\alpha_1,\dots,\alpha_t$ είναι ακέραιοι. Επειδή ο δακτύλιος $\mathcal{O}_F$ είναι Dedekind η ανάλυση αυτή είναι μοναδική συνεπώς μπορούμε να ορίσουμε την απεικόνιση $\operatorname{ord}: F^{\times}\to\mathbb{Z}$ με $\operatorname{ord}_{\mathfrak{p}}(x)=\alpha$ η οποία λέγεται διακριτή εκτίμηση στο σώμα F.

Παρατήρηση 1.2.3. *Η συνάρτηση αυτή είναι κανονικοποιημένη δηλαδή ισχύει:* $\operatorname{ord}(F^{\times})=\mathbb{Z}$.

Ορισμός 1.2.4. *Χρησιμοποιώντας την $\operatorname{ord}(x)$ ορίζουμε την p - αδική απόλυτη τιμή στο F ως εξής:*

$$|x| = \begin{cases} 0 & x=0 \\ c^{\operatorname{ord}_p(x)} & x\neq 0 \end{cases}$$

όπου $0<c<1$.

Διαφορετικές επιλογές πραγματικών αριθμών c παράγουν ισοδύναμες απόλυτες τιμές. Εύκολα βλέπουμε ότι η $|\cdot|_p$ είναι μια μη Αρχιμήδεια απόλυτη τιμή στο F. Επίσης αν $p\neq q$ οι $|\cdot|_p$ και $|\cdot|_q$ δεν είναι ισοδύναμες. Τυπικές επιλογές για τον πραγματικό αριθμό c είναι $1/p$ όπου $p\mathbb{Z}=\mathfrak{p}\cap\mathbb{Z}$ ή $1/N_{\mathfrak{p}}$ όπου $N_{\mathfrak{p}}$ είναι ο θετικός γεννήτωρας του $N_{F/\mathbb{Q}}(\mathfrak{p})$.

Παρατήρηση 1.2.5. *Εύκολα μπορεί κανείς να αποδείξει ότι αν ένα σώμα είναι εφοδιασμένο με μια μετρική που είναι ορισμένη από μια μη Αρχιμήδεια απόλυτη τιμή τότε όλα τα τρίγωνα σε αυτό το χώρο είναι ισοσκελή.*

Μπορεί κάποιος να ορίσει μια Αρχιμήδεια απόλυτη τιμή στο σώμα F μέσω μιας εμφύτευσης $\sigma: F\hookrightarrow\mathbb{C}$ θέτοντας:

$$|x|_{\sigma} = |\sigma(x)|$$

όπου $|\cdot|$ είναι η συνήθης απόλυτη τιμή στο $\mathbb{C}$. Έστω $\sigma_1,\dots,\sigma_{r_1}$ όλες οι διακεκριμένες πραγματικές και $\sigma_{r_1+1},\dots,\sigma_{r_1+r_2}$ όλες οι διακεκριμένες φανταστικές εμφυτεύσεις στο F έτσι ώστε κάθε ζεύγος συζυγών φανταστικών εμφυτεύσεων να εμφανίζεται ακριβώς μία φορά. Τότε αποδεικνύεται ότι οι απόλυτες τιμές $|\cdot|_{\sigma_1},\dots,|\cdot|_{\sigma_{r_1+r2}}$ είναι ανά δύο μη ισοδύναμες στο F, ενώ οι απόλυτες τιμές $|\cdot|_{\sigma}$ και $|\cdot|_{\overline{\sigma}}$ είναι ισοδύναμες.

Σχετικό με την ισοδυναμία απόλυτων τιμών είναι το θεώρημα του Ostrofski που αναφέρουμε αμέσως:

Θεώρημα 1.2.6 (Ostrofski). *Κάθε μη τεριμμένη απόλυτη τιμή στο $\mathbb{Q}$ είναι ισοδύναμη με μία από τις απόλυτες τιμές $|\cdot|_p$ όπου p πρώτος ή $p = \infty$.*

Ορισμός 1.2.7. *Η πλήρωση ενός αλγεβρικού σώματος αριθμών F ως προς την απόλυτη τιμή$|\cdot|$ είναι το σώμα: $\{$ακολουθίες Cauchy στο $F/$ μηδενικές ακολουθίες στο $F\}$.*

Μέσω των σταθερών ακολουθιών θα θεωρούμε το F ως υπόσωμα κάθε πλήρωσης του. Εάν το F είναι εφοδιασμένο με απόλυτη τιμή $|\cdot|_{\mathfrak{p}}$ όπου $\mathfrak{p}$ ένα μη μηδενικό πρώτο ιδεώδες του $\mathscr{O}_F$ τότε συμβολίζουμε την πλήρωση του F με $F_{\mathfrak{p}}$. Εάν$|\cdot| =|\cdot|_\sigma$ για κάποια μιγαδική εμφύτευση σ του F, τότε η πλήρωση του F είναι ισόμορφη με το $\mathbb{R}$ ή με το $\mathbb{C}$.

Εξετάζοντας την p -δική πλήρωση του F με μεγαλύτερη λεπτομέρεια ορίζουμε τον δακτύλιο των p -δικων ακεραίων ως εξής:

Ορισμός 1.2.8. *Έστω F σώμα με πλήρωση $F_{\mathfrak{p}}$. Ο δακτύλιος:*

$$\mathscr{O}_{\mathfrak{p}} = \{x \in F_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$$

λέγεται ο δακτύλιος των p- δικων ακεραίων.

Παρατήρηση 1.2.9. *Ο δακτύλιος αυτός είναι τοπικός δακτύλιος (στην πραγματικότητα διακριτός δακτύλιος εκτίμησης) με μοναδικό μέγιστο ιδεώδες: $\mathscr{P}_{\mathfrak{p}} = \{x \in F_{\mathfrak{p}} : |x|_{\mathfrak{p}} < 1\}$. Οι μονάδες του $\mathscr{O}_{\mathfrak{p}}$ είναι ακριβώς τα στοιχεία που έχουν απόλυτη τιμή 1. Ισχύει ότι ο δακτύλιος $\mathscr{O}_F$ είναι υποδακτύλιος του $\mathscr{O}_{\mathfrak{p}}$ και είναι πυκνός στον $\mathscr{O}_{\mathfrak{p}}$. Επιπλέον έχουμε: $\mathscr{P}_{\mathfrak{p}} = \mathfrak{p}\mathscr{O}_{\mathfrak{p}}$ και:*

$$O_{\mathfrak{p}}/\mathscr{P}_{\mathfrak{p}} \cong \mathscr{O}_F/\mathfrak{p}.$$

Ως εκ τούτου το $F_{\mathfrak{p}}$ είναι local field δηλαδή είναι πλήρες ως προς την διακριτή εκτίμηση και έχει πεπερασμένο σώμα υπολοίπων.

Ορισμός 1.2.10. *Ορισμός 1.2.10*

Ας διαλέξουμε τώρα ένα στοιχείο $\pi \in \mathfrak{p} - \mathfrak{p}^2$ και ας το δούμε ως στοιχείο του $F_{\mathfrak{p}}$. Παρατηρούμε ότι $\mathscr{P}_{\mathfrak{p}} = \langle \pi \rangle$. Το π λέγεται uniformizer στο $F_{\mathfrak{p}}$.

Κάθε στοιχείο $x \in F_{\mathfrak{p}}$ μπορεί να γραφτεί στην μορφή:$x = \epsilon\pi_{\mathrm{t}}$ όπου t ακέραιος και $\epsilon \in {O_{\mathfrak{p}}}^{\times}$.Αυτό οδηγεί στην p-δικη επέκταση του x:

$$x = \sum_{j=t}^{\infty} \alpha_j \pi^j$$

όπου τα α_j επιλέγονται από ένα πεπερασμένο σύνολο διακεκριμένων αντιπροσώπων του $O_{\mathfrak{p}}/\mathscr{P}_{\mathfrak{p}}$.

Συγκεκριμένα αν $F = \mathbb{Q}$ τότε $\mathfrak{p} = p\mathbb{Z}$ για κάποιο πρώτο αριθμό p. Αν συμβολίσουμε την πλήρωση με $\mathbb{Q}_p$ και τον δακτύλιο των p-δικων ακεραίων με $\mathbb{Z}_p$ μπορούμε να επιλέξουμε τα α_j από το σύνολο $\{0, 1, \ldots, p-1\}$.

Έστω πάλι F σώμα αριθμών και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathscr{O}_F$.Το παρακάτω θεώρημα μας επιτρέπει να ανυψώσουμε μια παραγοντοποίηση ενός πολυωνύμου υπέρ ενός σώματος υπολοίπων $\mathscr{O}_F/\mathfrak{p}$ σε μία παραγοντοποίηση υπέρ μιας πλήρωσης $F_{\mathfrak{p}}$.

Θεώρημα 1.2.11 (Λήμμα του Hensel). *Έστω σώμα αριθμών και $\mathfrak{p}$ πρώτο ιδεώδες του $\mathscr{O}_F$. Αν $f(X) \in \mathscr{O}_\mathfrak{p}[X]$ βαθμού n, έστω $\overline{f(X)}$ η κανονική εικόνα του $f(X)$ στον δακτύλιο $\mathscr{O}_\mathfrak{p}/\mathscr{P}_\mathfrak{p}[X]$ (γίνονται τότε οι συντελεστές modulo $\mathscr{P}_\mathfrak{p}$) και ισχύει:*

$$\overline{f(x)} = \overline{g(X)}\ \overline{h(X)},$$

όπου $\deg(\overline{g}) = t$ και $\overline{g}$, $\overline{h}$ μονικά και πρώτα μεταξύ τους στον $O_\mathfrak{p}/\mathscr{P}_\mathfrak{p}[X]$ τότε υπάρχει παραγοντοποίηση $f(X) = g(X)h(X)$ στον $\mathscr{O}_\mathfrak{p}[X]$ όπου $\deg g = t$ και g, h είναι μονικά πολυώνυμα μετατρέπονται modulo $\mathscr{P}_\mathfrak{p}$ σε $\overline{g}, \overline{h}$ αντίστοιχα.

Παρατήρηση 1.2.12. *Η πλήρωση $\mathbb{Q}_\mathfrak{p}$ δεν είναι αλγεβρικά κλειστή αλλά σε αντίθεση με την περίπτωση της Αρχιμήδειας απόλυτης τιμής στον $\mathbb{Q}$ όταν κάποιος παίρνει την αλγεβρική κλειστότητα $\mathbb{Q}_\mathfrak{p}^{\mathrm{alg}}$ του $\mathbb{Q}_\mathfrak{p}$ δεν είναι πλήρης. Ευτυχώς η πλήρωση της αλγεβρικής κλειστότητας του $\mathbb{Q}_\mathfrak{p}$ είναι συγχρόνως αλγεβρικά κλειστή και πλήρης. Έτσι έχουμε ένα σώμα το οποίο είναι ανάλογο με το $\mathbb{C}$ που το συμβολίζουμε με $\mathbb{C}_\mathfrak{p}$. Υπάρχει μια μοναδική απόλυτη τιμή στο $\mathbb{C}_\mathfrak{p}$ που επεκτείνει την p-δικη απόλυτη τιμή του $\mathbb{Q}_\mathfrak{p}$ που θα συμβολίζουμε επίσης με $|\cdot|_\mathfrak{p}$.*

Έστω F σώμα αριθμών και p πρώτος αριθμός ή $p = \infty$. Εάν $\sigma : F \hookrightarrow \mathbb{Q}_p^{alg}$ είναι μια εμφύτευση (όπου $\mathbb{Q}_\infty^{alg} = \mathbb{C}$) ορίζουμε για κάθε $x \in F$: $|x|_\sigma = |\sigma(x)|_p$. Εύκολα μπορούμε να διαπιστώσουμε ότι η $|\cdot|_\sigma$ είναι μια απόλυτη τιμή στο F που επεκτείνει την $|\cdot|_p$. Επιπλέον κάθε επέκταση της $|\cdot|_p$ στο F είναι τοπολογικά ισοδύναμη με μια $|\cdot|_p$.

Πότε δύο εμφυτεύσεις σ_1, σ_2 του F δίνουν ισοδύναμες απόλυτες τιμές στο F; Ακριβώς όταν είναι συζυγείς εμφυτεύσεις δηλαδή όταν υπάρχει αυτομορφισμός ϕ του $\mathbb{Q}_p^{\mathrm{alg}}$ ώστε $\phi \circ \sigma_1 = \sigma_2$. Έτσι υπάρχει μια ένα προς ένα αντιστοιχία:

$$\left\{ \begin{matrix} \text{τοπολογικά διακεκριμένες} \\ \text{επεκτάσεις του} |\cdot|p \text{ στο } F \end{matrix} \right\} \leftrightarrow \left\{ \begin{matrix} \text{συζυγείς κλάσεις εμφυτεύσεων} \\ \sigma{:}F \hookrightarrow \mathbb{Q}_p^{\mathrm{alg}} \end{matrix} \right\}.$$

Αν το σώμα αριθμών F είναι μια απλή επέκταση του $\mathbb{Q}$ και το στοιχείο α είναι πρωταρχικό, τότε το μονικό ανάγωγο πολυώνυμο $f(X)$ του α μας είναι χρήσιμο για να μάθουμε περισσότερα για τις επεκτάσεις του $|\cdot|_p$. Στον $\mathbb{Q}_p[X]$ αν η παραγοντοποίηση του $f(X)$ σε γινόμενο διακεκριμένων ανάγωγων πολυωνύμων είναι:

$$f(X) = h_1(X) \cdots h_g(X)$$

τότε δύο εμφυτεύσεις σ_1, σ_2 είναι συζυγείς αν και μόνο αν στέλνουν το α σε ρίζες του ίδιου πολυωνύμου $\phi_j[X]$. Συνεπώς υπάρχουν g διακεκριμένες επεκτάσεις της $|\cdot|_p$ στο F. Επιπλέον αν $\sigma(\alpha)$ είναι μια ρίζα του $\phi_j[X]$ τότε για την πλήρωση F_σ του F ως προς την $|\cdot|_\sigma$ ισχύει $\deg h_j = [F_\sigma : \mathbb{Q}_p]$.

Έστω K/F επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{p}$ ένα μη μηδενικό πρώτο ιδεώδες του $\mathscr{O}_F$. Αν:

$$\mathfrak{p}\mathscr{O}_K = \mathscr{B}^{e_1} \dots \mathscr{B}^{e_g}$$

η παραγοντοποίηση του ιδεώδους $\mathfrak{p}\mathscr{O}_K$ σε γινόμενο διακεκριμένων πρώτων ιδεωδών $\mathscr{B}_1, \dots, \mathscr{B}_g$ του $\mathscr{O}_K$ με e_j θετικοί ακέραιοι τότε οι απόλυτες τιμές $|\cdot|_{\mathscr{B}_1}, \dots, |\cdot|_{\mathscr{B}_g}$

είναι ανά δύο μη ισοδύναμες στο K αλλά οι περιορισμοί τους στο υπόσωμα F παράγουν την ίδια τοπολογία με την απόλυτη τιμή $|\cdot|_{\mathfrak{p}}$. Επιπλέον οι απόλυτες τιμές $|\cdot|_{\mathscr{B}_1}, \ldots, |\cdot|_{\mathscr{B}_g}$ είναι όλες οι μη ισοδύναμες επεκτάσεις της $|\cdot|_{\mathfrak{p}}$ στο K. Κάθε πλήρωση $K_{\mathscr{B}j}$ είναι μια πεπερασμένη επέκταση του $F_{\mathfrak{p}}$.

Αντίστροφα αν k είναι μια πεπερασμένη επέκταση τότε υπάρχει πεπερασμένη επέκταση K του F και ένα πρώτο ιδεώδες $\mathscr{B}$ του $\mathscr{O}_K$ τέτοιο ώστε $k = K_{\mathscr{B}}$.Έτσι όλες οι πεπερασμένες επεκτάσεις του $F_{\mathfrak{p}}$ προκύπτουν από πρώτα ιδεώδη σε πεπερασμένες επεκτάσεις του F.

Ανάλογα με την περίπτωση των σωμάτων αριθμών, η έννοια του κλασματικού ιδεώδους εφαρμόζεται στις πληρώσεις $F_{\mathfrak{p}}$. Όπως στα σώματα αριθμών έχουμε μια μοναδική παραγοντοποίηση κλασματικών ιδεωδών αφού ο δακτύλιος $\mathscr{O}_{\mathfrak{p}}$ είναι περιοχή κύριων ιδεωδών. Οι παραγοντοποιήσεις είναι πολύ απλές σε αυτήν την περίπτωση αφού υπάρχει μόνο ένα πρώτο ιδεώδες. Για την επέκταση $K_{\mathscr{B}/F_{\mathfrak{p}}}$ μπορούμε να παραγοντοποιήσουμε το ιδεώδες $\mathscr{P}_{\mathfrak{p}}\mathscr{O}_{\mathscr{B}}$ ως $\mathscr{P}_{\mathscr{B}}^e$ για κάποιον θετικό ακέραιο $e = e(\mathscr{P}_{\mathscr{B}}/\mathscr{P}_{\mathfrak{p}})$ που λέγεται τοπικός δείκτης διακλάδωσης. Ορίζουμε επίσης ως:

$$f = f(\mathscr{P}_{\mathscr{B}}/\mathscr{P}_{\mathfrak{p}}) = [\mathscr{O}_{\mathscr{B}}/\mathscr{P}_{\mathscr{B}} : \mathscr{O}_{\mathfrak{p}}/\mathscr{P}_{\mathfrak{p}}]$$

τον τοπικό βαθμό σωμάτων υπολοίπων.

Ισχύει: $ef = [K_{\mathscr{B}} : F_{\mathfrak{p}}]$ αφού οι $\mathscr{O}_{\mathfrak{p}}$ και $\mathscr{O}_{\mathscr{B}}$ είναι τοπικοί δακτύλιοι δεν έχουμε ανάλυση στη επέκταση $K_{\mathscr{B}}/F_{\mathfrak{p}}$. Χρησιμοποιούμε την ορολογία και εδώ πλήρως διακλαδιζόμενη αν $f = 1$, διακλαδιζόμενη αν $e > 1$ και δεν διακλαδίζεται αν $e = 1$ αλλά μπορούμε να εφαρμόσουμε αυτές τις περιγραφές για ολόκληρη την επέκταση αφού σε κάθε σώμα υπάρχει μόνο ένα πρώτο ιδεώδες.

Γενικά εάν K/F είναι μια επέκταση σωμάτων αριθμών και $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες του $\mathscr{O}_F$ με $\mathfrak{p}\mathscr{O}_K = \mathscr{B}_1^{e_1} \ldots \mathscr{B}_g^{e_g}$ τότε ισχύουν: $e(\mathscr{P}_{\mathscr{B}_j}/\mathscr{P}_{\mathfrak{p}}) = e(\mathscr{B}_j/\mathscr{P}_{\mathfrak{p}})$ και $f(\mathscr{P}_{\mathscr{B}_j}/\mathscr{P}_{\mathfrak{p}}) = f(\mathscr{B}_j/\mathscr{P}_{\mathfrak{p}})$ δηλαδή δείκτες διακλάδωσης και βαθμοί σωμάτων υπολοίπων για τα σώματα αριθμών και τις πληρώσεις τους συμπίπτουν.

Επιπλέον αν η επέκταση K/F είναι Galois το ίδιο συμβαίνει και για την $K_{\mathscr{B}_j}/F_{\mathfrak{p}}$ και επιπλέον ισχύει:

$$\mathrm{Gal}(K_{\mathscr{B}_j}/F_{\mathfrak{p}}) \cong \{\sigma \in G(K/F) : \big|\sigma(x)\big|_{\mathscr{B}_j} \forall x \in K_{\mathscr{B}_j}\} \cong Z(\mathscr{B}_j/\mathfrak{p})$$

Το επόμενο θεώρημα είναι σχετικό με διακλαδώσεις σε επεκτάσεις της πλήρωσης $F_{\mathfrak{p}}$.

Θεώρημα 1.2.13. *Με $F_{\mathfrak{p}}$ συμβολίζουμε την πλήρωση ενός σώματος αριθμών F σε ένα μη μηδενικό πρώτο ιδεώδες $\mathfrak{p}$ του $\mathscr{O}_F$.*

(i) Κάθε πεπερασμένη και πλήρως διακλαδιζόμενη επέκταση του $F_{\mathfrak{p}}$ εχει τη μορφή $F_{\mathfrak{p}}(\pi)$ όπου π είναι ρίζα ενός πολυωνύμου του Eisenstein στο $\mathscr{O}_{\mathfrak{p}}[T]$

(ii) Εάν $\pi \in F_{\mathfrak{p}}^{\mathrm{alg}}$ είναι ρίζα ενός πολυωνύμου του Eisenstein στο $\mathscr{O}_{\mathfrak{p}}[T]$ τότε η επέκταση $F_{\mathfrak{p}}(\pi)/F_{\mathfrak{p}}$ είναι πλήρως διακλαδιζόμενη.

(iii) Εάν f θετικός ακέραιος τότε υπάρχει μία μοναδική μη διακλαδιζόμενη επέκταση του $F_{\mathfrak{p}}$ βαθμού f (μοναδική μέσα σε μια σταθερή αλγεβρική κλειστότητα).

Είναι επέκταση Galois με κυκλική ομάδα Galois και δημιουργείται αν επισυνάψουμε στο $F_{\mathfrak{p}}$ μία ανύψωση κάθε πρωταρχικού στοιχείου για τον βαθμό f επέκταση του πεπερασμένου σώματος $\mathscr{O}_{\mathfrak{p}}/\mathscr{P}_{\mathfrak{p}}$.

Κεφάλαιο 2

Αναλυτικές Μέθοδοι

2.1 Το θεώρημα του Dirichlet

Όπως είναι γνωστό πρώτος ο Ευκλείδης απέδειξε ότι υπάρχουν άπειροι πρώτοι. Αιώνες μετά ο Euler ανακάλυψε μια άλλη απόδειξη χρησιμοποιώντας την συνάρτηση ζήτα του Riemann.

Η απόδειξη του Dirichlet για την ύπαρξη άπειρων πρώτων σε αριθμητικές προόδους είναι μια γενίκευση της ιδέας του Euler μόνο που αντικαθιστά την συνάρτηση ζήτα από την συνάρτηση L ενός χαρακτήρα Dirichlet. Ο Dirichlet έδωσε την απόδειξη για τον prime modulus το 1837 ολοκληρώνοντας την γενική περίπτωση το 1840.

Για $m = 1$ έχουμε το θεώρημα του Ευκλείδη. Το θεώρημα για αριθμητικές προόδους ήταν βασικό στοιχείο για την απόπειρα του Legendre να αποδείξει την τετραγωνική αντιστροφή. Δυστυχώς ο Legendre δεν κατάφερε να την αποδείξει. Η πρώτη πλήρης απόδειξη οφείλεται στον Gauss εφαρμόζοντας μια διαφορετική προσέγγιση και έγινε αργότερα αν και προηγείται χρονικά του θεωρήματος του Dirichlet.

Σε αυτό το κεφάλαιο θα αναφερθούμε τους χαρακτήρες Dirichlet και τις L συναρτήσεις τους και θα αποδείξουμε το θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές προόδους.

2.1.1 Χαρακτήρες σε πεπερασμένες αβελιανές ομάδες

Ορισμός 2.1.1. *Έστω G μια πεπερασμένη αβελιανή ομάδα. Ένας χαρακτήρας της G είναι ένας πολλαπλασιαστικός ομομορφισμός $G \to \mathbb{C}^\times$. Συμβολίζουμε με $\widehat{G}$ το σύνολο όλων των χαρακτήρων της G.*

Ορισμός 2.1.2. *Εάν $\chi, \psi \in \widehat{G}$ ορίζουμε ως το γινόμενο αυτών των δύο χαρακτήρων να είναι η συνάρτηση $\chi\psi : G \to \mathbb{C}^\times$. Τότε ικανοποιείται η σχέση: $\chi\psi(g) = \chi(g)\psi(g)$ για κάθε $g \in G$. Συνεπώς η $\widehat{G}$ είναι πολλαπλασιαστική ομάδα που λέγεται η ομάδα χαρακτήρων της G.*

Ο ομομορφισμός $\chi_0 : G \to \mathbb{C}^\times$ $\chi_0 : g \mapsto 1$ *λέγεται ο τετριμμένος χαρακτήρας της* G *και είναι η μονάδα της* $\widehat{G}$.

Ορισμός 2.1.3. *Εάν* $g \in G$ *ορίζουμε την απεικόνιση* $\widehat{g} : \widehat{G} \to \mathbb{C}^\times$ *με* $\widehat{g}(\chi) \mapsto \chi(g)$.

Πρόταση 2.1.4. *Εάν η* G *είναι πεπερασμένη αβελιανή ομάδα τότε* $\widehat{G} \cong G$ *όπου η απεικόνιση* $g \mapsto \widehat{g}$ *είναι ισομορφισμός* $G \to \widehat{\widehat{G}}$.

Πρόταση 2.1.5. *Έστω η* G *είναι πεπερασμένη αβελιανή ομάδα. Εάν* $H < G$ *θεωρούμε το σύνολο:*

$$H^\perp = \{\chi \in \widehat{G} : \chi(h) = 1 \forall h \in H\}$$

(i) Εάν $H < G$ *τότε* $H^\perp \cong \widehat{G/H}$

(ii) Εάν $H < G$ *τότε* $\widehat{H} \cong \widehat{G}/\widehat{H^\perp}$

(iii) Ισχύει: $\widehat{\widehat{H}} = H$ *αν κάνουμε την ταύτιση* $\widehat{\widehat{G}} = G$

Πρόταση 2.1.6 (Σχέσεις ορθογωνιότητας)**.** *(i) Θεωρούμε ένα χαρακτήρα* χ *μιας πεπερασμένης αβελιανής ομάδας* G. *Τότε:*

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \chi \neq \chi_0 \\ \#G & \chi = \chi_0 \end{cases}$$

(ii) Θεωρούμε ένα στοιχείο g *μιας πεπερασμένης ομάδας* G.*Τότε:*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} 0 & g \neq 1 \\ \#G & g = 1 \end{cases}$$

2.1.2 Χαρακτήρες Dirichlet

Ορισμός 2.1.7. *Έστω* n *ενας θετικός ακέραιος.Ένας χαρακτήρας Dirichlet* χ *modulo* n *είναι ένας χαρακτήρας της αβελιανής ομάδας* $(\mathbb{Z}/n\mathbb{Z})^\times$ *δηλαδή είναι ένας πολλαπλασιαστικός ομομορφισμός:*

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$$

Ο θετικός ακέραιος n *λέγεται modulus του* χ.

Παρατήρηση 2.1.8. *Εάν* χ *χαρακτήρας Dirichlet modulus* n *και* $n|m$ *τότε χρησιμοποιώντας τον φυσικό ομομορφισμό* $\phi : (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ *ορίζουμε:* $\chi' = \chi \circ \phi$.*Τότε ο* x' *είναι επίσης χαρακτήρας Dirichlet αλλά modulus* m. *Σε αυτή την περίπτωση λέμε ότι ο* χ *επάγει τον* χ'.

Ορισμός 2.1.9. *Έστω f_χ ο ελάχιστος δυνατός modulus για έναν Dirichlet χαρακτήρα χ δηλαδή ο χ δεν επάγεται από κανένα χαρακτήρα Dirichlet με modulus μικρότερο από f_χ. Τότε ο f_χ καλείται οδηγός του χ. Ένας χαρακτήρας Dirichlet που είναι ορισμένος με modulus τον οδηγό του f_χ λέγεται primitive.*

Παρατήρηση 2.1.10. *Ένας χαρακτήρας Dirichlet χ μπορεί να θεωρηθεί και ως μια συνάρτηση: $\chi : \mathbb{Z} \to \mathbb{C}$ με:*

$$x(\alpha) = \begin{cases} x(\alpha \mathrm{mod} f_\chi) & (\alpha, f_\chi) = 1 \\ 0 & (\alpha, f_\chi) \neq 1 \end{cases}$$

Έστω χ_0 ο τεριμμένος χαρακτήρας με οδηγό 1. Εάν χ, ψ primitive Dirichlet χαρακτήρες με οδηγούς f_χ, f_ψ αντίστοιχα θέτουμε $n =$ΕΚΠ(f_χ, f_ψ). Η συνάρτηση $\eta : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ που ορίζεται ως εξής: $\eta : \alpha \mapsto \chi(\alpha)\psi(\alpha)$ είναι εύκολο να δούμε ότι είναι ένας (πιθανών όχι primitive) χαρακτήρας. Ορίζουμε το γινόμενο $\chi\psi$ να είναι ο primitive Dirichlet χαρακτήρας που επάγει τον η.Με αυτό τον τρόπο ορίζουμε έναν πολλαπλασιασμό σε primitive Dirichlet χαρακτήρες που είναι κλειστός. Εύκολα μπορούμε να διαπιστώσουμε ότι μονάδα είναι ο χ_0.

Παρατήρηση 2.1.11. *Ο οδηγός του $\chi\psi$ είναι ένας διαιρέτης του γινομένου των οδηγών των χ, ψ.*

Εάν $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ είναι ένας χαρακτήρας Dirichlet τότε αυτόν μπορούμε να τον συσχετίσουμε με την απεικόνιση $\overline{\chi} : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ που ορίζεται από την σχέση:

$$\overline{\chi}(\alpha) = (\chi(\alpha))^{-1} = \overline{\chi(\alpha)}$$

ο μιγαδικός συζυγής. Είναι εύκολο να αποδείξουμε ότι ο $\overline{\chi}$ είναι χαρακτήρας Dirichlet, έχει τον ίδιο οδηγό με τον χ και ότι $\overline{\chi}\chi = \chi_0$. Έτσι οι primitive χαρακτήρες Dirichlet σχηματίζουν μια πολλαπλασιαστική ομάδα. Η τάξη ενός χαρακτήρα Dirichlet είναι η τάξη του σαν στοιχείο αυτής της ομάδας. Επειδή η εικόνα ενός χαρακτήρα Dirichlet είναι μια πεπερασμένη ομάδα ριζών της μονάδας στον $\mathbb{C}_\times$ η τάξη του θα είναι πάντα πεπερασμένη. Επιπλέον αν ο χ έχει οδηγό n τότε η τάξη του χ πρέπει να είναι διαιρέτης του $\phi(n)$.

Ορισμός 2.1.12. *Ένας χαρακτήρας Dirichlet τάξης 2 λέγεται quadratic.*

Ορισμός 2.1.13. *Για κάθε χαρακτήρα Dirichlet ισχύει: $\chi(-1) = 1$ ή $\chi(-1) = -1$.*

(i) Αν $\chi(1) = 1$ ο χ λέγεται άρτιος.

(ii) Αν $\chi(1) = -1$ ο χ λέγεται περιττός.

Εάν n θετικός ακέραιος τότε οι χαρακτήρες Dirichlet που έχουν οδηγούς που διαιρούν τον n σχηματίζουν μια πεπερασμένη ομάδα. Αν ζ_n είναι μια πρωταρχική n-στη ρίζα της μονάδας τότε μπορούμε να κάνουμε την ταύτιση:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n))/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

όπου κάθε χαρακτήρας που ανήκει στην ομάδα των χαρακτήρων Dirichlet modulo n μπορεί να θεωρηθεί ως χαρακτήρας της ομάδας Galois G.

Ορισμός 2.1.14. *Έστω χ χαρακτήρας της ομάδας $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n))/\mathbb{Q})$ και K το σταθερό σώμα του πυρήνα του χ. Το σώμα K ονομάζεται ώς το σώμα που είναι συσχετισμένο με τον χαρακτήρα χ.*

Ορισμός 2.1.15. *Έστω X πεπερασμένη ομάδα χαρακτήρων Dirichlet και n το ελάχιστο κοινό πολλαπλάσιο όλων των οδηγών αυτών των χαρακτήρων. Μπορούμε να δούμε το X σαν υποομάδα της $\widehat{G}$ όπου $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n))/\mathbb{Q})$. Έστω $H = \cap \ker\chi$ όπου η τομή εκτείνεται σε όλα τα $\chi \in X$. Η H είναι υποομάδα της G και αν K το σταθερό σώμα της H τότε το K λέγεται ως το σώμα που συσχετίζεται με την ομάδα X.*

Παρατήρηση 2.1.16. *Εάν $\chi \in X$ τότε $H < \ker\chi$ και άρα το σώμα το συσχετιζόμενο με τον χαρακτήρα χ είναι υπόσωμα του σώματος που είναι συσχετιζόμενο με την ομάδα των χαρακτήρων X. Επιπλέον αν η X είναι κυκλική παραγόμενη από τον χαρακτήρα χ τότε το σώμα που είναι συσχετιζόμενο με την X είναι το ίδιο με το σώμα που είναι συσχετιζόμενο με τον χαρακτήρα χ.*

Υπάρχει σχέση μεταξύ του οδηγού ενός χαρακτήρα Dirichlet και της διακρίνουσας του συσχετιζόμενου σώματος. Σχετικά με αυτό είναι το επόμενο θεώρημα το οποίο παρουσιάζουμε χωρίς απόδειξη:

Θεώρημα 2.1.17 (Τύπος οδηγού-διακρίνουσας)**.** *Έστω X μια πεπερασμένη ομάδα χαρακτήρων Dirichlet και K το συσχετιζόμενο αβελιανό σώμα αριθμών. Τότε:*

$$d_{K/\mathbb{Q}} = (-1)^{r_2} \prod_{\chi \in X} f_\chi$$

όπου r_2 είναι ο αριθμός των ζευγών των φανταστικών εμφυτεύσεων του K.

Έστω $\mathbb{Q} \subset L \subset K$ όπου $K/\mathbb{Q}$ πεπερασμένη αβελιανή επέκταση. Με X_K συμβολίζουμε την ομάδα των χαρακτήρων της ομάδας $\mathrm{Gal}(K/\mathbb{Q})$. Τότε:

$$\begin{aligned}\{\chi \in X_K : \chi(g) = 1 \forall g \in \mathrm{Gal}(K/L)\} = \mathrm{Gal}(K/L)^\perp &= G(K/\widehat{\mathbb{Q})/\mathrm{Gal}}(K/L) \\ &= \widehat{\mathrm{Gal}(L/\mathbb{Q})} = X_L\end{aligned}$$

όπου με X_L συμβολίζουμε την ομάδα χαρακτήρων που συσχετίζεται με το σώμα L.

Αντίστροφα αν έχουμε μια αβελιανή επέκταση $K/\mathbb{Q}$ που έχει ως ομάδα χαρακτήρων την X_K και L το σταθερό σώμα της $Y^\perp$ τότε:

$$Y^\perp = \{g \in \mathrm{Gal}(K/\mathbb{Q}) : x(g) = 1 \forall x \in Y\} = \mathrm{Gal}(K/L)$$

και

$$Y = (Y^\perp)^\perp = \mathrm{Gal}(K/L)^\perp = \widehat{\mathrm{Gal}(L/\mathbb{Q})} = X_L$$

Δείξαμε ότι υπάρχει μια αντιστοιχία ένα προς ένα:

{ υποομάδες της X_K} $\leftrightarrow$ { υποσώματα του K}

που δίνεται από:

$Y \leftrightarrow$σταθερό σώμα της $Y^\perp$ ή από $X_L = \mathrm{Gal}(K/L)^\perp \leftrightarrow L$

Για αβελιανές επεκτάσεις του $\mathbb{Q}$ μπορούμε να υπολογίσουμε δείκτες διακλάδωσης σε όρους χαρακτήρων Dirichlet. Για να περιγράψουμε πως χρειαζόμαστε κάποιες παρατηρήσεις. Εάν n θετικός ακέραιος με $n = \prod_{j=1}^{m} p_j^{\alpha_j}$ όπου p_j είναι διακεκριμένοι πρώτοι και $\alpha_j > 0$. Τότε:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{j=1}^{m} (\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^\times$$

Συνεπώς ένας χαρακτήρας Dirichlet ορισμένος modulo n γράφεται στην μορφή:

$$\chi = \prod_{j=1}^{m} \chi_{p_j}$$

όπου χ_{p_j} είναι χαρακτήρας Dirichlet modulo $p_j^{\alpha_j}$.

Έστω X μια ομάδα από χαρακτήρες Dirichlet modulo $n = \prod_{j=1}^{m} p_j^{\alpha j}$. Ορίζουμε:

$$X_{p_j} = \{\chi_{p_j} : \chi \in X\}$$

Θεώρημα 2.1.18. *Έστω X μια ομάδα από χαρακτήρες Dirichlet με συσχετιζόμενο σώμα το K. Εάν ο $p \in \mathbb{Z}$ είναι πρώτος τότε ο δείκτης διακλάδωσης του p στην επέκταση $K/\mathbb{Q}$ είναι $e = \#(X_p)$.*

Απόδειξη. Έστω n το ελάχιστο κοινό πολλαπλάσιο των f_x με $\chi \in X$ και $n = p^\alpha m$ όπου ο p δεν διαιρεί τον m. Ισχύει $K \subset \mathbb{Q}(\zeta_n)$ και επιπλέον ότι:

$$\mathbb{Q}(\zeta_m) \subset L = K(\zeta_m) \subset \mathbb{Q}(\zeta_n).$$

Επειδή η ομάδα $\widehat{\mathrm{Gal}(L/\mathbb{Q})}$ παράγεται από τις $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$ και $G(\widehat{\mathbb{Q}(\zeta_m)}/\mathbb{Q})$, παράγεται από την X και τους χαρακτήρες modulo m. Επειδή $(p, m) = 1$ η ομάδα $\widehat{\mathrm{Gal}(L/\mathbb{Q})}$ είναι το ευθύ γινόμενο του X_p και των χαρακτήρων του $\mathbb{Q}(\zeta_m)$. Ισχύει: $L = E\mathbb{Q}(\zeta_m)$ όπου E είναι το υπόσωμα του $\mathbb{Q}(\zeta_{p^\alpha})$ που αντιστοιχεί στο X_p.

Μια και ο p δεν διακλαδίζεται στην $\mathbb{Q}(\zeta_m/\mathbb{Q})$ ο δείκτης διακλάδωσης για τον p στην $L/\mathbb{Q}$ είναι e. Αλλά ο p δεν διακλαδίζεται στην L/E άρα ο δείκτης διακλάδωσης για τον p στην $E/\mathbb{Q}$ είναι e. Αλλά ο p διακλάδίζεται πλήρως στην $\mathbb{Q}(\zeta_{p^\alpha})/\mathbb{Q}$ επομένως και στη $E/\mathbb{Q}$. Άρα $e = [E : \mathbb{Q}] = \#(X_p)$. □

Πόρισμα 2.1.19. *Έστω X μια ομάδα από χαρακτήρες Dirichlet και K το συσχετιζόμενο σώμα. Ένας πρώτος p δεν διακλαδίζεται στην επέκταση $K/\mathbb{Q}$ αν και μόνο αν $\chi(p) \neq 0$ $\forall \chi \in X$.*

Απόδειξη. Έστω ότι ο p διακλαδίζεται στην $K/\mathbb{Q}$. Τότε έχουμε $e = \#X_p \neq 1$ συνεπώς η X_p περιέχει κάποιο μη τεριμμένο στοιχείο χ. Έτσι υπάρχει ένας μη τεριμμένος χαρακτήρας χ στην X με τον οδηγό του να διαιρείται από τον p δηλαδή $\chi(p) = 0$.

Αντίστροφα αν $\chi(p) = 0$ για κάποιο στοιχείο χ στην X τότε ο οδηγός του χ πρέπει να διαιρείται από τον p. Έτσι η X_p δεν μπορεί να είναι η τετριμμένη. Αυτό όμως σημαίνει ότι $e = \#X_p > 1$ άρα ο p διακλαδίζεται. □

Θεώρημα 2.1.20. *Έστω X ομάδα από χαρακτήρες Dirichlet με συσχετιζόμενο σώμα K. Έστω επίσης p πρώτος. Ορίζουμε τις υποομάδες:*

$$Y = \{\chi \in X : \chi(p) \neq 0\}$$

$$Y_1 = \{\chi \in X : \chi(p) = 1\}$$

Τότε:

(i) η X/Y είναι ισόμορφη με την ομάδα αδρανείας για τον p

(ii) η X/Y_1 είναι ισόμορφη με την ομάδα αναλύσεως για τον p

(iii) η Y/Y_1 είναι κυκλική τάξης f

Απόδειξη. Λόγω του πορίσματος 2.1.19 το υπόσωμα L του K που είναι συσχετισμένο με την Y πρέπει να είναι το μεγαλύτερο υπόσωμα του K στο οποίο ο p να μην διακλαδίζεται. Συνεπώςτο $L = K(T)$ είναι το σταθερό σώμα της ομάδας αδρανείας T_p και $T_p = \mathrm{Gal}(K/L)$.

Από την ένα προς ένα αντιστοιχία μεταξύ υποομάδων της X και υποσωμάτων του K έχουμε:

$$Y = \mathrm{Gal}(K/L)^{\perp}$$

Άρα:

$$\begin{aligned} X/Y &= \widehat{\mathrm{Gal}(K/\mathbb{Q})}/\mathrm{Gal}(K/L)^{\perp} \\ &= \widehat{\mathrm{Gal}(K/L)} \\ &\cong \mathrm{Gal}(K/L) = T_p. \end{aligned}$$

Συνεπώς $e = \#(T_p) = [X : Y]$.

Για την επέκταση τώρα $L/\mathbb{Q}$ εχουμε ότι δεν διακλαδίζεται στο p και η ομάδα χαρακτήρων της είναι η Y. Εάν ο n είναι το ελάχιστο κοινό πολλαπλάσιο των f_x με $\chi \in X$ τότε $L \subset \mathbb{Q}(\zeta_n)$. Επίσης ο p δεν διαιρεί τον n μια και ο p δεν διακλαδίζεται στην $L/\mathbb{Q}$. Γνωρίζουμε ότι ο αυτομορφισμός του Frobenius για τον p στην $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n/\mathbb{Q})$ είναι: $\sigma_p : \zeta_n \mapsto \zeta_n^p$ και είναι μοναδικός μια και ο p δεν διακλαδίζεται. Ισχύει:

$$\mathrm{Gal}(L/\mathbb{Q}) \cong G/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$$

άρα ο αυτομορφισμός του Frobenius για τον p στην $\mathrm{Gal}(L/\mathbb{Q})$ είναι το σύμπλοκο του σ_p στο πηλίκο που το συμβολίζουμε με $\overline{\sigma}_p$. Αλλά αν $\chi \in Y$ τότε ο $\chi(\sigma)$ είναι τετριμμένος στην $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$ και άρα $\chi(\overline{\sigma}_p) = \chi(\sigma_p) = \chi(p)$. Έτσι:

$$Y_1 = \{\chi \in X : \chi(\overline{\sigma}_p) = 1\} = \langle \overline{\sigma}_p \rangle^{\perp}$$

και $Y/Y_1 \cong \widehat{\langle \overline{\sigma}_p \rangle} \cong \langle \overline{\sigma}_p \rangle$ που είναι μια κυκλική ομάδα τάξης f. Έχουμε $[Y : Y_1] = f$ και $[Y_1 : 1] = g$.

Γνωρίζουμε επίσης ότι η $\langle \overline{\sigma_p} \rangle$ είναι ισόμορφη με το πηλίκο της ομάδας αναλύσεως προς την ομάδα αδρανείας. Αλλά ο p δεν διακλαδίζεται στην $L/\mathbb{Q}$ συνεπώς η

$\langle \overline{\sigma}_p \rangle$ είναι ισόμορφη στην ομάδα αναλύσεως για τον p στην $L/\mathbb{Q}$. Η ομάδα χαρακτήρων της F είναι η Y_1 (F είναι το σταθερό σώμα του $\overline{\sigma}_p$ άρα $\chi \in \widehat{\mathrm{Gal}(F/\mathbb{Q})}$ αν και μόνο αν $\chi(\overline{\sigma}_p) = 1$ αν και μόνο αν $\chi \in Y_1$). Συνεπώς $Y_1 \cong \mathrm{Gal}(F/\mathbb{Q})$

Για την επέκταση $K/\mathbb{Q}$: Ο p αναλύεται πλήρως στην $F/\mathbb{Q}$, οι πρώτοι πάνω από τον p παραμένουν αδρανείς στην L/F και διακλαδίζονται στην K/L. Η ομάδα αναλύσεως για τον p στην $K/\mathbb{Q}$ είναι ισόμορφη με την $\mathrm{Gal}(K/F)$ μια και η μόνη ανάλυση στην $K/\mathbb{Q}$ συμβαίνει στην $F/\mathbb{Q}$ και ο p αναλύεται πλήρως εκεί. Συμπεραίνουμε ότι: $Y_1 = \mathrm{Gal}(K/F)^{\perp}$ από την ένα προς ένα αντιστοιχία και:

$$\begin{aligned} X/Y_1 = \widehat{\mathrm{Gal}(K/\mathbb{Q})}/\mathrm{Gal}(K/F)^{\perp} &= \widehat{\mathrm{Gal}(K/F)} \\ &\cong \mathrm{Gal}(K/F) \end{aligned}$$

που είναι ισόμορφη με την ομάδα αναλύσεως για το p στην $K/\mathbb{Q}$. □

2.1.3 Σειρές Dirichlet

Η συνάρτηση ζήτα του Riemann και η L-συνάρτηση του Dirichlet είναι παραδείγματα σειρών Dirichlet. Σε αυτήν την ενότητα θα αναφερθούμε σε γενικές ιδιότητες των σειρών Dirichlet τις οποίες θα χρειαστούμε αργότερα.

Ορισμός 2.1.21. *Μια σειρά Dirichlet είναι μια σειρά της μορφής:*

$$f(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$$

όπου $\alpha_n \in \mathbb{C}$ για κάθε n και s είναι μια μιγαδική μεταβλητή.

Λήμμα 2.1.22. *Εάν η $f(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$ συγκλίνει για $s = s_0$ τότε συγκλίνει ομοιόμορφα σε κάθε περιοχή της μορφής:*

$$\{s : \mathrm{Re}(s - s_0) \geq 0, \left|\mathrm{Arg}(s - s_0)\right| \leq \theta\}$$

με $\theta < \frac{\pi}{2}$.

Λήμμα 2.1.23. *Εάν η $f(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$ συγκλίνει για $s = s_0$ τότε αυτή συγκλίνει (αν και όχι απαραίτητα απολύτως) για $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ σε μία συνάρτηση που είναι ολόμορφη εκεί.*

Πόρισμα 2.1.24. *Έστω $f(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$ σειρά Dirichlet.*

(i) Εάν η ακολουθία $(\alpha_n)_{n\in\mathbb{N}}$ είναι φραγμένη τότε η $f(s)$ συγκλίνει απόλυτα για $\mathrm{Re}(s) > 1$

(ii) Εάν η ακολουθία των μερικών αθροισμάτων $(A_n)_{n\in\mathbb{N}}$ της $(\alpha_n)_{n\in\mathbb{N}}$ είναι φραγμένη τότε η $f(s)$ συγκλίνει (όχι απαραιτήτως απόλυτα) για $\mathrm{Re}(s) > 0$.

(iii) Εάν η $f(s) = \sum_{n=1}^{\infty} \frac{\alpha_n}{n^s}$ συγκλίνει στο $s = s_0$ τότε συγκλίνει απόλυτα για $\mathrm{Re}(s) > \mathrm{Re}(s_0) + 1$.

Ορισμός 2.1.25. *Έστω $x : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ ένας χαρακτήρας Dirichlet.*

1. *Η L-συνάρτηση του Dirichlet ορίζεται ως εξής:*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

2. *Η συνάρτηση ζήτα του Riemann ορίζεται ως εξής:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Παρατήρηση 2.1.26. *Παρατήρηση 2.3.6*
Έστω $\chi \neq \chi_0$. Ας ορίσουμε $A_n = \chi(1) + \cdots + \chi(n)$ με $n = mk + r$, $0 \le r \le m-1$. Τότε:

$$A_n = [\chi(1)+\ldots+\chi(m)]+[\chi(m+1)+\ldots+\chi(2m)]+\ldots+[\chi(km+1)+\ldots+\chi(km+r)]$$

$$= \chi(km+1) + \ldots + \chi(km+r)$$

Συνεπώς: $|A_n| \le r < m$ και λόγω του πορίσματος 2.3.4 (ii) εάν $\chi \neq \chi_0$ η $L(s,\chi)$ είναι αναλυτική για $\mathrm{Re}(s) > 0$. Για κάθε χ (και για $\chi = \chi_0$) η $L(s,\chi)$ συγκλίνει απόλυτα για $\mathrm{Re}(s) > 1$ λόγω του (iii).

Πρόταση 2.1.27. *Η L-συνάρτηση του Dirichlet έχει το λεγόμενο γινόμενο του Euler δηλαδή ισχύει:*

$$L(s,\chi) = \prod_{p\ prime} \left(1 - \chi(p)p^{-s}\right)^{-1}$$

για $\mathrm{Re}(s) > 1$.

Απόδειξη. Έστω s σταθερός με $\mathrm{Re}(s) > 1$. Θέλουμε να δείξουμε:

$$\lim_{N\to\infty} \prod_{p\le N} \left(1 - \frac{\chi(p)}{p^s}^{-1}\right)^{-1} = L(s,\chi).$$

Έστω $p_1, \ldots, p_k$ πρώτοι μικρότεροι από N. Τότε:

$$\prod_{i=1}^{k} \left(1 - \frac{\chi(p_i)}{{p_i}^s}\right)^{-1} = \prod_{i=1}^{k} \left(1 + \frac{\chi(p_i)}{p_i^s} + \ldots + \frac{\chi(p_i^m)}{p_i^{ms}} + \ldots\right)$$

$$= \sum_{m_1,\ldots,m_k \ge 0} \frac{\chi(p_1^{m_1}\cdots p_k^{m_k})}{(p_1^{m_1}\cdots p_k^{m_k})^s}$$

$$= \sum_{n\in\vartheta_N} \frac{\chi(n)}{n^s}$$

όπου $\vartheta_N = \{n \in \mathbb{Z} : n > 0, p \nmid n$ για κάθε p πρώτο με $p > N\}$.

Ισχύει:

$$L(s,\chi) - \prod_{p \leq N} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{n \in (\mathbb{Z}_+ \setminus \vartheta_N)} \frac{\chi(n)}{n^s}$$

Παίρνουμε απόλυτες τιμές και εφαρμόζουμε την τριγωνική ανισότητα και έχουμε:

$$\left| \sum_{n \in \mathbb{Z}_+ \setminus \vartheta_N} \frac{\chi(n)}{n^s} \right| \leq \sum_{n \in \mathbb{Z}_+ \setminus \vartheta_N} \frac{1}{n^\sigma}$$

όπου $\sigma = \mathrm{Re}(s)$

$$\leq \sum_{n \geq N} \frac{1}{n^\sigma} \to 0$$

καθώς $N \to \infty$ μια και η $\sum_{n>N} \frac{1}{n^\sigma}$ συγκλίνει για $\sigma > 1$. Το αποτέλεσμα ακολουθεί. □

Παρατήρηση 2.1.28. *Ισχύει: $L(s,\chi) \neq 0$ για $\mathrm{Re}(s) > 1$. Τότε λογαριθμώντας την σχέση από την πρόταση 2.3.7 παίρνουμε:*

$$\log L(s,\chi) = -\sum_p \log(1 - \chi(p)p^{-s})$$

όπου $\log$ *δηλώνει το τμήμα του λογαρίθμου ώστε* $\log L(s,\chi) \to 0$ *καθώς* $s \to \infty$. *Από την γραφή του* $\log(1+T)$ *σαν σειρά έχουμε:*

$$\log L(s,\chi) = \sum_p -\log(1 - \chi(p)p^{-s})$$

$$= \sum_p \sum_{n \geq 1} \frac{\chi(p)^n p^{-ns}}{n}$$

$$= \sum_p \sum_{n \geq 1} \frac{\chi(p)^n}{np^{ns}}$$

Επειδή: $\left|\frac{\chi(p)^n}{np^{ns}}\right| \leq \left|\frac{1}{p^{ns}}\right| = \frac{1}{p^{n\sigma}}$ *όπου* $\sigma = \mathrm{Re}(s)$ *άρα*

$$\sum_{p,n \geq 1} \left|\frac{\chi(p)^n}{np^{ns}}\right| \leq \sum_p \sum_{n \geq 1} \frac{1}{p^{n\sigma}} \leq \sum_{m \geq 1} \frac{1}{m^\sigma}$$

που συγκλίνει για $\sigma > 1$.

Ως εκ τούτου η παραπάνω έκφραση για τον $\log L(s,\chi)$ *συγκλίνει απολύτως για* $\mathrm{Re}(s) > 1$. *Αυτό μας επιτρέπει να αναδιατάξουμε του όρους και να πάρουμε:*

$$\log L(s,\chi) = \sum_p \sum_{n \geq 1} \frac{\chi(p)^n}{np^{ns}}$$

$$= \sum_p \frac{\chi(p)}{p^s} + \sum_p \sum_{n\geq 2} \frac{\chi(p)^n}{np^{ns}}$$

Θέτουμε:

$$\beta(s,\chi) = \sum_p \sum_{n\geq 2} \frac{x(p)^n}{np^{ns}}$$

Η σειρά $\beta(s,\chi)$ συγκλίνει απολύτως για $\mathrm{Re}(s) > \frac{1}{2}$ (και άρα η $\beta(1,\chi)$ παίρνει μια πεπερασμένη τιμή).

2.2 Το θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους

Σε αυτή την ενότητα θα αποδείξουμε το θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους. Η απόδειξη αυτή του Dirichlet είναι μια γενίκευση της τεχνικής του Euler που χρησιμοποίησε τη συνάρτηση ζήτα του Riemann για να αποδείξει ότι υπάρχουν άπειροι πρώτοι (στην περίπτωση όπου $m = 1$).

Θα περιγράψουμε παρακάτω την απόδειξη του Euler.

Η συνάρτηση ζήτα του Riemann είναι: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Αποδεικνύεται ότι:

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

Ας υποθέσουμε ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι $p_1, \ldots, p_n$ στο $\mathbb{Z}$. Τότε:

$$\zeta(s) = \prod_{j=1}^{n} \left(1 - p_j^{-s}\right)^{-1} = \prod_{j=1}^{n} \left(\frac{1}{1 - \frac{1}{p_j^s}}\right)$$

Παίρνοντας όρια έχουμε:

$$\lim_{s\to 1} \zeta(s) = \prod_{j=1}^{n} \left(\frac{1}{1 - \frac{1}{p_j}}\right)$$

που είναι ρητός αριθμός. Αλλά ξέρουμε ότι (από την σειρά για τον $\zeta(s)$) ότι $\lim_{s\to 1} \zeta(s) = \infty$ και έχουμε άτοπο.

Στην απόδειξη του θεωρήματος του Dirichlet για πρώτους σε αριθμητικές προόδους η συνάρτηση ζήτα αντικαθίσταται από την συνάρτηση L του Dirichlet.

Θεώρημα 2.2.1 (του Dirichlet για πρώτους σε αριθμητικές προόδους)**.** *Εάν m θετικός ακέραιος και α ένας ακέραιος για τον οποίο $(\alpha, m) = 1$ τότε υπάρχουν άπειροι πρώτοι p που ικανοποιούν την σχέση $p \equiv \alpha(\mathrm{mod} m)$.*

Απόδειξη. Έστω $(\alpha, m) = 1$ και ας θεωρήσουμε όλους τους χαρακτήρες Dirichlet που ορίζονται *modulo* m. Τότε:

$$\sum_{\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})}^{\times}} \chi(\alpha)^{-1} \log L(s,\chi) = \sum_{\chi} \chi(\alpha)^{-1} (\sum_p \frac{x(p)}{p^s} + \beta(s,\chi))$$

$$= \sum_p \frac{1}{p^s} \sum_\chi \chi(\alpha)^{-1}\chi(p) + \sum_\chi \chi(\alpha)^{-1}\beta(s,\chi)$$

$$= \sum_p \frac{1}{p^s} \sum_\chi \chi(p\alpha^{-1}) + \sum_\chi \chi(\alpha)^{-1}\beta(s,\chi)$$

Από τις σχέσεις ορθογωνιότητας έχουμε ότι:

$$\sum_\chi \chi(p\alpha^{-1}) = \begin{cases} \phi(m) & p \equiv \alpha (mod m) \\ 0 & \text{αλλιώς} \end{cases}$$

Συνεπώς:

$$\sum_\chi \chi(\alpha)^{-1} \log L(s,\chi) =$$

$$\phi(m) \sum_{p\equiv\alpha(mod m)} p^{-s} + (\text{Κάτι που συγκλίνει απολύτως για } \mathrm{Re}(s) > \frac{1}{2}) \qquad (2.1)$$

Παίρνουμε όρια καθώς $s \to 1$. Από το δεξί μέλος της 2.1 παίρνουμε:

$$\lim_{s\to 1} \phi(m) \sum_{p\equiv\alpha(\mathrm{mod} m)} p^{-s} + (\text{πεπερασμένη σταθερά})$$

Η τελευταία έκφραση είναι πεπερασμένος αριθμός αν υπάρχουν πεπερασμένοι το πλήθος πρώτοι p με $p \equiv \alpha(\mathrm{mod} m)$. Η απόδειξη θα ολοκληρωθεί αν αποδείξουμε ότι για το αριστερό μέλος της 2.1 ισχύει:

$$\lim_{s\to 1} \sum_\chi \chi(\alpha)^{-1} \log L(s,\chi) = \infty.$$

Για την περίπτωση όπου $\chi = \chi_0$ (με modulus m) ισχύει:

$$L(s,\chi_0) = \prod_p \left(1 - \chi_0(p)p^{-s}\right)^{-1} = \zeta(s) \prod_{p|m} (1 - p^{-s}) \to \infty$$

καθώς $s \to 1$. Συνεπώς $\log L(s,\chi_0) \to \infty$ καθώς $s \to 1$.

Για την περίπτωση που $\chi \neq \chi_0$ έχουμε δει από το πόρισμα 2.3.3 (ii) ότι η $L(s,\chi)$ είναι αναλυτική για $\mathrm{Re}(s) > 0$. Μια και η $L(1,\chi)$ είναι ορισμένη για $\chi \neq \chi_0$, ο $\log L(1,\chi)$ θα είναι πεπερασμένος αριθμός αν δείξουμε ότι $L(1,\chi) \neq 0$ για κάθε $\chi \neq \chi_0$. Αν το αποδείξουμε αυτό τότε θα έχουμε: $\sum_\chi \chi(\alpha)^{-1} \log L(s,\chi) \to \infty$ καθώς $s \to 1^+$ και η απόδειξη θα είναι πλήρης.

□

Μένει συνεπώς να αποδείξουμε ότι $L(1,\chi) \neq 0$ όταν $\chi \neq \chi_0$. Ο Dirichlet το 1840 το απέδειξε αυτό. Το 1850 ο Kummer εδωσε μια αριθμητική απόδειξη την οποία θα παρουσιάσουμε. Θα χρειαστούμε πρώτα όμως να ορίσουμε την συνάρτηση ζήτα του Dedekind για ένα σώμα αριθμών.

Ορισμός 2.2.2. *Έστω K αλγεβρικό σώμα αριθμών και το $\mathfrak{a}$ διατρέχει όλα τα μη μηδενικά ακέραια ιδεώδη του δακτυλίου $\mathscr{O}_K$ των αλγεβρικών ακέραιων του K.(κατά τέτοιο τρόπο ώστε ο $N\mathfrak{a}$ να είναι θετικός ακέραιος). Η συνάρτηση ζήτα του Dedekind είναι:*

$$\zeta_K = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}$$

.

Παρατήρηση 2.2.3. *Με επιχείρημα παρόμοιο με αυτό για τις L-συναρτήσεις έχουμε ότι ισχύει:*

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

όπου το $\mathfrak{p}$ διατρέχει όλα τα πρώτα ιδεώδη του O_K. Εύκολα βλέπει κανείς ότι ισχύει:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\gamma_n}{n^s}$$

όπου $\gamma_n = \#\{\mathfrak{a} : N\mathfrak{a} = n\}$

Το επόμενο θεώρημα είναι από το έργο του Dedekind και θα το παρουσιάσουμε παραλείποντας την απόδειξη.

Θεώρημα 2.2.4. *Η $\zeta_K(s)$ συνεχίζεται αναλυτικά στο $\mathbb{C} - \{1\}$ με μοναδικό πόλο στο $s = 1$ δηλαδή:*

$$\zeta_K(s) = \frac{\rho(K)}{s-1} + \text{ακέραια συνάρτηση}$$

Επιπλέον:

$$\rho(K) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{\omega_K \sqrt{\left|d_{K/\mathbb{Q}}\right|}}$$

όπου:

$r_1 = \#$*πραγματικές εμφυτεύσεις του* K
$r_2 = \#$*Ζεύγη φανταστικών εμφυτεύσεων του* K
$h_K = \#\mathscr{C}_K =$*class number του* K
$R_K =$ *regulator του* K
$\omega_K = \#$ *ριζών της μονάδας στο* K
$d_{K/\mathbb{Q}} =$ *η διακρίνουσα.*

Θα χρησιμοποιήσουμε την συνάρτηση ζήτα του Dedekind για να αποδείξουμε ότι $L(1, \chi) \neq 0$ για $\chi \neq \chi_0$ ολοκληρώνοντας έτσι την απόδειξη στο θεώρημα του Dirichlet για τους πρώτους σε αριθμητικές σειρές.

Έστω $K = \mathbb{Q}(\zeta_m)$ όπου m είναι το modulus στο θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους επομένως είναι και το modulus για τους χαρακτήρες χ. Έχουμε:

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

$$= \prod_{\mathfrak{p}} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1})$$

$$= \prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1}) (\prod_{p\nmid m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1})$$

Επίσης $N\mathfrak{p} = p^f$ όπου f ο βαθμός του σώματος υπολοίπων και επειδή η $K/\mathbb{Q}$ είναι επέκταση Galois έχουμε: $efg = \phi(m)$. Εάν $p \nmid m$ τότε $\epsilon = 1$, $f = \#Z(p) = \mathrm{ord}_m(p)$, $g = \phi(m)/f$.

Λήμμα 2.2.5. *Εάν $p \nmid m$ τότε* $(1 - T^f)^{\phi(m)/f} = \prod_{xmodm} (1 - \chi(p)T)$.

Θέτουμε τώρα $T = p^{-s}$ στο λήμμα 2.4.5 και παίρνουμε:

$$(1 - p^{-sf})^{-\phi(m)/f} = \prod_{\chi} (1 - \chi(p)p^{-s})^{-1}.$$

Παίρνουμε το γινόμενο όλων των $p \nmid m$ και έχουμε:

$$\prod_{p\nmid m} (1 - p^{-sf})^{-\phi(m)/f} = \prod_{\chi} \prod_{p\nmid m} (1 - \chi(p)p^{-s})^{-1}$$

Εάν $p|m$ τότε $x(p) = 0$ συνεπώς:

$$\prod_{p\nmid m} (1 - p^{-sf})^{-\phi(m)/f} = \prod_{p} (1 - p^{-sf})^{-\phi(m)/f} = \prod_{\chi} L(s, \chi)$$

Από τη άλλη μεριά:

$$\prod_{p\nmid m} (1 - p^{-sf})^{-\phi(m)/f} = \prod_{p\nmid m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})^{-1}$$

$$= \zeta_K(s) \prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s})$$

Κατά συνέπεια:

$$\zeta_K(s) \prod_{p|m} \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-s}) = \prod_{\chi} (L(s, \chi))$$

$$= L(s, \chi_0) \prod_{\chi \neq \chi_0} (L(s, \chi))$$

$$= \zeta(s) \prod_{p|m} (1 - p^s) \prod_{\chi \neq \chi_0} L(s.\chi)$$

Τελικά έχουμε:

$$\frac{\prod_{p\nmid m}\prod_{\mathfrak{p}|p}(1-N\mathfrak{p}^{-s})\zeta_K(s)}{(\prod_{p|m}(1-p^{-s}))\zeta(s)} = \prod_{\chi\neq\chi_0} L(s,\chi)$$

Οι εκφράσεις:

$$\prod_{p|m}\prod_{\mathfrak{p}|p}(1-N\mathfrak{p}^{-s})$$

και

$$\prod_{p|m}(1-p^{-s})$$

είναι μη μηδενικές σταθερές ενώ οι $\zeta_K(s)$ και $\zeta(s)$ εχουν έναν απλό πόλο για $s=1$. Παίρνοντας το όριο για $s\to 1$ το δεξί μέλος γίνεται σταθερά αφού η $\prod_{\chi\neq x_0} L(s,\chi)$ γίνεται σταθερά. Αυτό δείχνει ότι $L(s,\chi)\neq 0$ για κάθε $\chi\neq\chi_0$ και η απόδειξη του θεωρήματος Dirichlet είναι πλήρης.

2.3 Η πυκνότητα του Dirichlet

Ορισμός 2.3.1. *Έστω οι συναρτήσεις $f(s)$, $g(s)$ που ορίζονται για κάθε $s\in\mathbb{R}$ με $s>1$.Συμβολίζουμε $f(s)\sim g(s)$ αν ισχύει: η συνάρτηση $f(s)-g(s)$ είναι φραγμένη καθώς $s\to 1^+$.*

Θα χρησιμοποιήσουμε αυτό τον συμβολισμό για να αποδείξουμε πάλι το θεώρημα του Dirichlet:

Ισχύει για κάθε x:

$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \{$ σειρά Dirichlet που συγκλίνει για $\mathrm{Re}(s) > \frac{1}{2}\}$

Επομένως:

$$\log L(s,\chi)\sim\sum_p\frac{\chi(p)}{p^s}$$

Έτσι υποθέτοντας ότι $L(s,\chi)\neq 0$ όταν $\chi\neq\chi_0$ ισχύει:

$$\sum_\chi \chi(\alpha)^{-1}\log L(s,\chi)\sim\sum_{p\equiv\alpha(\mathrm{mod} m)}\frac{\phi(m)}{p^s}$$

$$\sim\log L(s,\chi_0)$$

Επειδή

$$L(s,\chi_0)=\prod_p(1-\frac{\chi_0(p)}{p^s})^{-1}=\prod_{p|m}(1-p^{-s})\zeta(s)$$

έχουμε:

$$\log L(s,\chi_0)\sim\log\zeta(s)$$

και παίρνουμε:

$$\sum_{p\equiv\alpha(\mathrm{mod} m)}\frac{1}{p^s}\sim\frac{1}{\phi(m)}\log\zeta(s)$$

Παίρνοντας τα όρια καθώς $s \to 1^+$ διαπιστώνουμε ότι η σειρά $\sum_{p\equiv\alpha(\bmod m)} \frac{1}{p^s}$ αποκλίνει και έτσι αποδεικνύεται πάλι το θεώρημα του Dirichlet και με αυτό το συμβολισμό.

Αποδεικνύεται ότι:

$$\lim_{s\to 1^+} \frac{\sum_{p\equiv\alpha(\bmod m)} p^{-s}}{\log(\frac{1}{s-1})} = \frac{1}{\phi(m)}$$

Αυτό οδηγεί στον επόμενο ορισμό:

Ορισμός 2.3.2. *Έστω $\mathscr{S}$ ενα σύνολο πρώτων αριθμών. Εάν το όριο:*

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathscr{S}} p^{-s}}{\log(\frac{1}{s-1})} = \delta$$

υπάρχει τότε λέμε ότι το σύνολο $\mathscr{S}$ έχει πυκνότητα Dirichlet $\delta = \delta(\mathscr{S})$.

Παρατήρηση 2.3.3. *Αποδεικνύονται τα εξής:*

(i) Εάν $\mathscr{S}$ ενα πεπερασμένο σύνολο πρώτων τότε $\delta(\mathscr{S}) = 0$.

(ii) Εάν $\mathscr{S}$ το σύνολο όλων των πρώτων στο $\mathbb{Z}$ τότε $\delta(\mathscr{S}) = 1$.

(iii) Εάν $\mathscr{S}$, $\mathscr{T}$ ξένα σύνολα πρώτων αριθμών τότε ισχύει: Αν δύο από τους τρείς αριθμούς $\delta(\mathscr{S})$, $\delta(\mathscr{T})$, $\delta(\mathscr{S}\cup\mathscr{T})$ είναι πεπερασμένοι τότε είναι και ο τρίτος και ισχύει ότι:

$$\delta(\mathscr{S}\cup\mathscr{T}) = \delta(\mathscr{S}) + \delta(\mathscr{T}).$$

Θεώρημα 2.3.4. *Έστω η επέκταση Galois $K/\mathbb{Q}$.Θεωρούμε το σύνολο:*
$\mathscr{S}_K = \{p \in \mathbb{Z} : p$ αναλύεται πλήρως στην $K/\mathbb{Q}\}$. Τότε:

$$\delta(\mathscr{S}_K) = \frac{1}{[K:\mathbb{Q}]}.$$

Η πυκνότητα του Dirichlet γενικεύεται και για σύνολα πρώτων μέσα σε ένα σώμα αριθμών F:

Ορισμός 2.3.5. *Έστω F σώμα αριθμών και $\mathscr{S}$ ενα σύνολο πρώτων αριθμών του $\mathscr{O}_F$. Εάν το όριο:*

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\,\in\mathscr{S}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})} = \delta$$

υπάρχει τότε λέμε ότι το σύνολο $\mathscr{S}$ έχει πυκνότητα Dirichlet $\delta = \delta_F(\mathscr{S})$.

Πόρισμα 2.3.6. *Έστω K/f επέκταση Galois. Θεωρούμε το σύνολο:*
$\mathscr{S}_{K/F} = \{\mathfrak{p} \in \mathscr{O}_F : \mathfrak{p}$ αναλύεται πλήρως στην $K/F\}$ Τότε:

$$\delta_F(\mathscr{S}_{K/F}) = \frac{1}{[K:F]}.$$

Ορισμός 2.3.7. *Έστω $\mathscr{S}$, $\mathscr{T}$ σύνολα πρώτων στον δακτύλιο $\mathscr{O}_F$ όπου F σώμα αριθμών. Τότε:*

(i) $\mathscr{S} \prec \mathscr{T}$ *αν* $\delta_F(\mathscr{S} \setminus \mathscr{T}) = 0$

(ii) $\mathscr{S} \approx \mathscr{T}$ *αν* $\mathscr{S} \prec \mathscr{T} \prec \mathscr{S}$

Θεώρημα 2.3.8. *Έστω E,K σώματα αριθμών καθένα από τα οποία είναι επέκταση Galois του $\mathbb{Q}$. Τότε: $\mathscr{S}_K \prec \mathscr{S}_E$ αν και μόνο αν $E \subset K$.*

Απόδειξη. Το αντίστροφο είναι προφανές. Για το ευθύ: Έστω $\mathscr{S}_K \prec \mathscr{S}_E$. Τότε επειδή $\mathscr{S}_{KE} = \mathscr{S}_K \cap \mathscr{S}_K$ έχουμε λόγω της προηγούμενης παρατήρησης (iii) ότι:

$$\delta(\mathscr{S}_{KE}) = \delta(\mathscr{S}_E \cap \mathscr{S}_K) = \delta(\mathscr{S}_K \setminus \mathscr{S}_E) + \delta(\mathscr{S}_E \cap \mathscr{S}_K) = \delta(\mathscr{S}_K)$$

το θεώρημα 2.3.4 δίνει $[KE : \mathbb{Q}] = [K : \mathbb{Q}]$. Από το τελευταίο συνεπάγεται $KE = K$ και συνεπώς $E \subset K$. $\square$

Κεφάλαιο 3

3.1 Οι ομάδες Ray class

Όπως έχουμε δει στην προηγούμενη ενότητα υπάρχουν άπειροι πρώτοι στο $\mathbb{Z}$ σε μια αριθμητική προόδο $\{\alpha + jm : j \in \mathbb{N}\}$ όταν $(\alpha, m) = 1$. Αυτό γενικεύεται σε πρώτα ιδεώδη του $\mathscr{O}_F$ όπου F αλγεβρικό σώμα αριθμών.

Υπάρχουν άπειροι πρώτοι $\mathfrak{p}$ του $\mathscr{O}_F$ σε μια αριθμητική προόδο; Τι εννοούμε όταν λέμε αριθμητική προόδο; Ίσως αυτό θα μπορούσε να μεταφραστεί ως μια ερώτηση γύρω από κλάσεις ιδεωδών. Εάν δοθεί μια κλάση ιδεωδών $c \in \mathscr{C}_F$ όπου $\mathscr{C}_F$ η ομάδα κλάσεων ιδεωδών του F υπάρχουν άπειρα πρώτα του $\mathscr{O}_F$ στην c; Αλλά πως εισάγεται η έννοια του modulus σε αυτό;

Αν ακολουθήσουμε σε αυτό τον Dirichlet θα πρέπει να αντικαταστήσουμε τον m από ένα ιδεώδες $\mathfrak{m}$ του $\mathscr{O}_F$ και θα πρέπει να σκεφτόμαστε για congruences modulo $\mathfrak{m}$. Αυτό οδηγεί με φυσικό τρόπο στην ιδέα της γενικευμένης ideal class group που ορίζεται για κάθε τέτοιο $\mathfrak{m}$ και που λέγεται ray class group. Επιπλέον χρειάζεται να επεκτείνουμε τις έννοιες του χαρακτήρα Dirichlet και της συνάρτησης L για ένα ανάλογο επιχείρημα με του Dirichlet.

Σε αυτό το κεφάλαιο θα ακολουθήσουμε ανάλογα επιχειρήματα με τον Dirichlet όπως έκανε και ο Weber. Αυτό θα μας οδηγήσει στην έννοια της κλάσης σώματων και στη απόδειξη της Universal norm index inequality. Πρώτα όμως θα μιλήσουμε συνοπτικά για απόλυτες τιμές και το θεώρημα προσέγγισης.

3.1.1 Το θεώρημα προσέγγισης και άπειροι πρώτοι

Θεώρημα 3.1.1 (Το θεώρημα προσέγγισης). *Έστω $|\cdot|_1, \ldots, |\cdot|_n$ μη τεριμμένες και ανά δύο μη ισοδύναμες απόλυτες τιμές σε ένα σώμα αριθμών F. Εάν $\beta_1, \ldots, \beta_n$ μη μηδενικά στοιχεία του F τότε για κάθε $\epsilon > 0$ υπάρχει ένα στοιχείο $\alpha \in F$ τέτοιο ώστε $\left|\alpha - \beta_j\right|_j < \epsilon$ για κάθε $j = 1, 2, \ldots, n$.*

Παρατήρηση 3.1.2. *Εάν το $\mathfrak{p}$ είναι ένα πρώτο ιδεώδες του $\mathscr{O}_F$ και $c = |\pi|_\mathfrak{p}$ για $\pi \in \mathfrak{p} - \mathfrak{p}^2$ τότε αν $\alpha\beta \neq 0$ και $|\alpha - \beta|_\mathfrak{p} < \epsilon$ δίνει ότι $\mathrm{ord}_\mathfrak{p}(\frac{\alpha}{\beta} - 1) > n$ όπου n δίνεται από $\frac{\epsilon}{|\beta|_\mathfrak{p}} < \epsilon^n$. Εάν α και β είναι p-δικες μονάδες τότε αυτό σημαίνει $\alpha \equiv \beta (mod \mathfrak{p}^n)$. Συγκεκριμένα αν κάθε μια από τις απόλυτες τιμές στο θεώρημα προσέγγισης είναι p-δικη για κάποιο $\mathfrak{p}$ τότε έχουμε το Κινέζικο θεώρημα υπολοίπων.*

3.2 Οι ομάδες Ray class

Ορισμός 3.2.1. *Εάν $\alpha \in F$ τότε λέμε ότι ο α είναι πλήρως θετικός και συμβολίζουμε με $\alpha \gg 0$ αν για κάθε πραγματική εμφύτευση σ ισχύει: $\sigma(\alpha) > 0$.*

Ορισμός 3.2.2. *Εάν $\mathfrak{m}$ ενα μη μηδενικό ακέραιο ιδεώδες του $\mathscr{O}_F$ τότε ορίζουμε με $\mathscr{P}^+_{F,\mathfrak{m}}$ την υποομάδα της $\mathscr{P}_F$ που παράγεται από:*

$$\{\langle\alpha\rangle : \alpha \in \mathscr{O}_F, \alpha \equiv 1(mod\mathfrak{m}) \text{ και } \alpha \gg 0\}.$$

Επίσης θα συμβλίζουμε με $a \overset{*}{\equiv} 1\mathrm{mod}\mathfrak{m}$ αν $a \equiv 1 \mod \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{m})}$ στην πλήρωση $F_\mathfrak{p}$ για κάθε $\mathfrak{p}|\mathfrak{m}$.

Παρατήρηση 3.2.3. *Αποδεικνύεται ότι:*

$$\mathscr{P}^+_{F,\mathfrak{m}} = \{\langle\alpha\rangle : \alpha \in F, \alpha \gg 0, \alpha \equiv^\times 1(mod\mathfrak{m})\}$$

$$= \{< \tfrac{\alpha}{\beta} >: \tfrac{\alpha}{\beta} \gg 0, \alpha, \beta \in \mathscr{O}_F \text{ πρώτοι στο } \mathfrak{m}, \alpha \equiv \beta(mod\mathfrak{m})\}$$

Ορισμός 3.2.4. *Έστω $\mathscr{I}_F(\mathfrak{m})$ η ομάδα των κλασματικών ιδεωδών του F που οι παραγοντοποιήσεις τους δεν περιέχουν μία μη τετριμμένη δύναμη ενός πρώτου ιδεώδους που διαιρεί το $\mathfrak{m}$:*

$$\mathscr{I}_F(\mathfrak{m}) = \{\alpha \in \mathscr{I}_F : \mathrm{ord}_\mathfrak{p}(\alpha) = 0 \forall \mathfrak{p}|\mathfrak{m}\}.$$

Η αυστηρή (στενή) ray class ομάδα ή γενικευμένη ideal class ομάδα του F για το $\mathfrak{m}$ είναι:

$$\mathscr{R}^+_{F,\mathfrak{m}} = \mathscr{I}_F(\mathfrak{m})/\mathscr{P}^+_{F,\mathfrak{m}}.$$

Έστω $F = \mathbb{Q}$ και $\mathfrak{m} = m\mathbb{Z}$ όπου $m \geq 1$. Αν $< r > \in \mathscr{I}(\mathfrak{m})$ τότε μπορούμε να υποθέσουμε ότι $r > 0$ και ότι $r = \frac{\alpha}{\beta}$ με $(\alpha, m) = (\beta, m) = 1$. Η απεικόνιση:

$$\mathscr{I}_\mathbb{Q}(\mathfrak{m}) \to (\mathbb{Z}/m\mathbb{Z})^\times$$

που ορίζεται από τη σχέση:

$$\langle r\rangle \mapsto \alpha\beta^{-1}(\mathrm{mod}m)$$

είναι καλώς ορισμένη και εύκολο είναι να δει κανείς ότι είναι επί. Ο πυρήνας της είναι:

$$\{\langle r\rangle : r > 0, r = \frac{\alpha}{\beta}, (\alpha, m) = (\beta, m) = 1, \alpha \equiv \beta(\mathrm{mod}m)\} = \mathscr{P}^+_{\mathbb{Q},\mathfrak{m}}$$

Κατά συνέπεια έχουμε:

$$\mathscr{I}_Q(\mathfrak{m})/\mathscr{P}^+_{\mathbb{Q},\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

Ορισμός 3.2.5. *Για ένα μη μηδενικό ιδεώδες $\mathfrak{m}$ του δακτυλίου $\mathscr{O}_F$ ορίζουμε την ray modulo $\mathfrak{m}$ ως:*

$$\mathscr{P}_{F,\mathfrak{m}} = \{\langle\alpha\rangle : \alpha \overset{*}{\equiv} (1mod\mathfrak{m})\}$$

Ορισμός 3.2.6. *Η ray class ομάδα του F για το $\mathfrak{m}$ είναι:*

$$\mathscr{R}_{F,\mathfrak{m}} = \mathscr{I}_F(\mathfrak{m})/\mathscr{P}_{F,\mathfrak{m}}$$

Συνεπώς αν λάβουμε υπόψη μας τους ορισμούς 3.2.5 και 3.2.6 για $F = \mathbb{Q}$ και $\mathfrak{m} = m\mathbb{Z}$ έχουμε:

$$\mathscr{R}^+_{\mathbb{Q},\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

και

$$\mathscr{R}_{\mathbb{Q},\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$$

Παρατήρηση 3.2.7. *Οι καινούργιες αυτές έννοιες είναι συνεπείς με την αρχική έννοια της ideal class ομάδας του F και αν $\mathfrak{m} = \mathscr{O}_F$ έχουμε:*

$$\mathscr{R}_{F,\mathfrak{m}} = \mathscr{I}_F/\mathscr{P}_F = \mathscr{C}_F$$

που είναι η συνήθης ideal class ομάδα και

$$\mathscr{R}^+_{F,\mathfrak{m}} = \mathscr{I}_F/\mathscr{P}^+_F$$

η αυστηρή (στενή) ideal class ομάδα.

Ορισμός 3.2.8. *Ένας γενικευμένος χαρακτήρας Dirichlet ή χαρακτήρας Weber χ που έχει modulus m είναι ένας ομομορφισμός ομάδων:*

$$\chi : \mathscr{R}^+_{\mathbb{Q},\mathfrak{m}} \to \mathbb{C}^\times$$

Παρατήρηση 3.2.9. *Είδαμε προηγουμένως ότι για $F = \mathbb{Q}$ και $\mathfrak{m} = m\mathbb{Z}$ ισχύει: $\mathscr{R}^+_{\mathbb{Q},\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$ συνεπώς ο ορισμός αυτός είναι με συνέπεια μία γενίκευση των χαρακτήρων Dirichlet.*

Ορισμός 3.2.10. *Ορίζουμε ως την L-συνάρτηση για γενικευμένους χαρακτήρες Dirichlet ως:*

$$L_\mathfrak{m}(s,\chi) = \sum_{integral\ ideals\ \alpha \in \mathscr{O}_F, (\alpha,\mathfrak{m})=1} \chi(\alpha) N\alpha^{-s}$$

όπου με $\chi(\alpha)$ εννοούμε την εικόνα του α μέσω της χ στον $\mathscr{R}^+_{F,\mathfrak{m}}$. Τέτοιες L-συναρτήσεις λέγονται και L συναρτήσεις Weber.

Παρατήρηση 3.2.11. *Για $F = \mathbb{Q}$ έχουμε τις L-συναρτήσεις Dirichlet.*

Όπως και με τις L-συναρτήσεις Dirichlet έτσι και με τις L συναρτήσεις Weber έχουμε ένα γινόμενο Euler για την $L_\mathfrak{m}(s,\chi)$:

$$L_\mathfrak{m}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} (1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s})^{-1}$$

που ορίζεται για $\mathrm{Re}(s) > 1$.

Παίρνοντας λογαρίθμους και προχωρώντας όπως με τις L-συναρτήσεις Dirichlet αποδεικνύουμε ότι υπάρχουν άπειροι πρώτοι $\mathfrak{p}$ σε κάθε κλάση υπό την προυπόθεση ότι η $L_{\mathfrak{m}}(s,\chi)$ ορίζεται και $L_{\mathfrak{m}}(s,\chi) \neq 0$ για κάθε $\chi \neq \chi_0$.

Για να ακολουθήσουμε το επιχείρημα του Dirichlet πρέπει να βρούμε μια επέκταση K/F όπου η $L_{\mathfrak{m}}(s,\chi)$ να είναι παράγοντας του $\zeta_K(s)$. Η θεωρία κλάσεων σωμάτων θα καθορίσει αυτό το σώμα K.

Πρώτα όμως θα μελετήσουμε την αυστηρή ray class ομάδων $\mathscr{R}^+_{F,\mathfrak{m}}$. Είναι αρκετά γνωστό ότι η συνήθης ομάδα κλάσεων ιδεωδών είναι πεπερασμένη και η τάξη της είναι αντικείμενο αρκετής μελέτης. Θα αναρωτηθεί κανείς αν η ray class ομάδων είναι επίσης πεπερασμένες ομάδες. Το ερώτημα αυτό απαντάται από το παρακάτω θεώρημα:

Πρόταση 3.2.12. *Η ομάδα $\mathscr{R}^+_{F,\mathfrak{m}}$ έχει πεπερασμένη τάξη με:*

$$\#\mathscr{R}^+_{F,\mathfrak{m}} = \frac{h_F 2^{r_1}\phi(\mathfrak{m})}{[\mathscr{U}_F : \mathscr{U}^+_{F,\mathfrak{m}}]}$$

όπου:
$h_F = \#\mathscr{C}_F$
$r_1 = \#$*πραγματικών εμφυτεύσεων στο* F
$\phi(\mathfrak{m}) = \#(\mathscr{O}_F/\mathfrak{m})^\times = \prod_{\mathfrak{p}|\mathfrak{m}} N\mathfrak{p}^{e_\mathfrak{p}-1}(N\mathfrak{p}-1)$ *όπου* $\mathfrak{m} = \prod_{\mathfrak{p}|\mathfrak{m}} \mathfrak{p}^{e_\mathfrak{p}}$
$\mathscr{U}_F = \mathscr{O}_F^\times$ *οι μονάδες του* $\mathscr{O}_F$
$\mathscr{U}^+_{F,\mathfrak{m}} = \{\epsilon \in \mathscr{U}_F : \epsilon \gg 0, \epsilon \equiv 1 (mod \mathfrak{m})\}$

Ορισμός 3.2.13. *Ο αριθμός $\mathscr{R}^+_{F,\mathfrak{m}}$ λέγεται ο αυστηρός ray class αριθμός modulo $\mathfrak{m}$ ή ο ray class αριθμός modulo $\mathfrak{m}\mathfrak{m}_\infty$.*

Ο ορισμός της κλάσεως σωμάτων ωφείλεται στον Weber. Νωρίτερα ο Kronecker παρατήρησε ότι κάθε αβελιανή επέκταση του $\mathbb{Q}$ είναι κυκλοτομική. Το 1886-1887 ο Weber έδωσε την πρώτη ολοκληρωμένη απόδειξη. Ο Kronecker επίσης παρατήρησε ότι οι εξισώσεις μετασχηματισμών και διαίρεσης σε modular και ελλειπτικές συναρτήσεις που παράγουν αβελιανές επεκτάσεις φανταστικών quadratic σωμάτων. (Ο Kronecker έλπιζε να αποδείξει ότι κάθε αβελιανή επέκταση ενός φανταστικού quadratic σώματος επιτυγχάνεται κατά αυτόν τον τρόπο. Ο Weber μερικώς το πέτυχε αυτό το 1908 αλλά η πρώτη ολοκληρωμένη απόδειξη ωφείλεται στον Takagi το 1920.) Σε αυτά τα παραδείγματα ο Weber παρατήρησε ότι οι πρώτοι που αναλύονται πλήρως σε αυτές τις αβελιανές επεκτάσεις δείχνουν να συσχετίζονται με ομάδες Galois. Αυτές οι ιδέες οδήγησαν τον Weber στον ορισμό των κλάσεων σώματος.

Ορισμός 3.2.14. *Έστω K/F επέκταση Galois και $\mathfrak{m}$ ακέραιο ιδεώδες του $\mathscr{O}_F$. Το σώμα K είναι το class field (σώμα κλάσεων) υπέρ F του $\mathscr{P}^+_{F,\mathfrak{m}}$ αν:*
$\mathscr{S}_{K/F} = \{$ *πρώτα ιδεώδη* $\mathfrak{p}$ *του* $\mathscr{O}_F : \mathfrak{p}$ *αναλύεται πλήρως στην* $K/F\}$
$\approx \{$ *πρώτα ιδεώδη* $\mathfrak{p}$ *του* $\mathscr{O}_F : \mathfrak{p} \in \mathscr{P}^+_{F,\mathfrak{m}}\}$
(Θυμίζουμε ότι $\mathscr{S} \approx \mathscr{T}$ αν τα $\mathscr{S}$ και $\mathscr{T}$ διαφέρουν κατά ένα σύνολο με πυκνότητα Dirichlet μηδέν)

Ορισμός 3.2.15. *Έστω $\mathfrak{m}$ ένα μη μηδενικό ακέραιο ιδεώδες του $\mathscr{O}_F$ και το σύνολο $\mathscr{H}$ ικανοποιεί τη σχέση:*

$$\mathscr{P}^+_{F,\mathfrak{m}} < \mathscr{H} < \mathscr{I}_{F,\mathfrak{m}}$$

Τότε λέμε ότι το K είναι το class field υπέρ F για το $\mathscr{H}$ αν η επέκταση K/F είναι Galois και επιπλέον:

$$\mathscr{S}_{K/F} \approx \{ \text{ πρώτα ιδεώδη } \mathfrak{p} \text{ του } \mathscr{O}_F : \mathfrak{p} \in \mathscr{H}\}$$

Ο Weber παρατήρησε ότι στις περιπτώσεις που $F = \mathbb{Q}$ και το F είναι ίσο με μια φανταστική quadratic επέκταση του $\mathbb{Q}$ η ομάδα Galois για την K/F είναι ισόμορφη με την συσχετιζόμενες ομάδες παραγόντων $\mathscr{I}_F(\mathfrak{m})/\mathscr{H}$ (ολοφάνερα αβελιανές). Ο ισομορφισμός με την ομάδα Galois σε αυτά τα παραδείγματα είναι μια εικονογράφηση του Isomorphy theorem στο οποίο θα αναφερθούμε σύντομα παρακάτω.

Εύκολα μπορεί να αποδείξει κανείς την μοναδικότητα ενός class field για κάθε τέτοιο $\mathscr{H}$. Γι αυτό έχουμε το παρακάτω θεώρημα που αποδίδεται στον Weber:

Θεώρημα 3.2.16 (Weber)**.** *Αν υποθέσουμε ότι το class field του $\mathscr{H}$ υπάρχει τότε αυτό είναι μοναδικό.*

Απόδειξη. Ας θυμηθούμε την πυκνότητα Dirichlet ενός συνόλου $\mathscr{S}$ πρώτων αριθμών του F:

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathscr{S}} p^{-s}}{\log(\frac{1}{s-1})} = \delta_F(\mathscr{S})$$

Έχουμε αποδείξει ότι:

$$\delta_F(\mathscr{S}_{K/F}) = \frac{1}{[K:F]}$$

Εάν K_1, K_2 δύο σωμάτα κλάσεων για το $\mathscr{H}$ τότε έστω $K = K_1K_2$.Τότε:

$$\mathscr{S}_{K/F} = \mathscr{S}_{K_1/F} \cap \mathscr{S}_{K_2/F}$$

$$\approx \{\mathfrak{p} \subset \mathscr{O}_F : \mathfrak{p} \in \mathscr{H}\}$$

δηλαδή:

$$\mathscr{S}_{K/F} \approx \mathscr{S}_{K_1/F} \approx \mathscr{S}_{K_2/F}$$

Κατά συνέπεια:

$$\frac{1}{[K:F]} = \frac{1}{[K_1:F]} = \frac{1}{[K_2:F]}$$

Άρα

$$K = K_1 = K_2$$

□

Θα αναφέρουμε τώρα κάποιες ιδιότητες για την συνάρτηση $L_{\mathfrak{m}}(s,\chi)$.

(i) Κατάρχήν για $\chi \neq \chi_0$ η $L_{\mathfrak{m}}(s,\chi)$ συνεχίζεται αναλυτικά σε ολόκληρο το μιγαδικό επίπεδο.

(ii) Η $L_{\mathfrak{m}}(s,\chi_0)$ συνεχιζεται αναλυτικά σε ολόκληρο το μιγαδικό επίπεδο εκτός από ένα απλό πόλο στο $s=1$

(iii) Για $\chi=\chi_0$ ισχύει:

$$\begin{aligned} L_{\mathfrak{m}}(s,\chi) &= \prod_{\mathfrak{p}\nmid\mathfrak{m}}(1-N\mathfrak{p}^{-s})^{-1} \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{m}}(1-N\mathfrak{p}^{-s})\zeta_F(s) \end{aligned}$$

Επιπλέον ισχύει ότι αν το $\mathscr{S}$ είναι πεπερασμένο τότε έχει πυκνότητα Dirichlet $\delta_F(\mathscr{S})=0$ ενώ αν το $\mathscr{S}$ περιέχει όλους τους πρώτους του F τότε $\delta_F(\mathscr{S})=1$.

Ορισμός 3.2.17. *Αν $\alpha\in\mathscr{I}_F(\mathfrak{m})$ ορίζουμε:*

$$\begin{aligned} \mathscr{S}_{\alpha,\mathfrak{m}} &= \{\mathfrak{p} \text{ πρώτο του } \mathscr{O}_F : \mathfrak{p}\equiv\alpha \text{ στο } \mathscr{R}^{+}_{F,\mathfrak{m}}\} \\ &= \{ \text{ πρώτα } \mathfrak{p}\in\alpha\mathscr{P}^{+}_{F,\mathfrak{m}}\} \end{aligned}$$

Ισχυριζόμαστε ότι αν για $\chi\neq\chi_0$ στο $\mathscr{R}^{+}_{F,\mathfrak{m}}$ έχουμε $L_{\mathfrak{m}}(s,\chi)\neq 0$ τότε:

$$\delta_F(\mathscr{S}_{\alpha,\mathfrak{m}}) = \frac{1}{\#\mathscr{R}^{+}_{F,\mathfrak{m}}}.$$

Αυτό λέει ότι το $\mathscr{S}_{\alpha,\mathfrak{m}}$ περιέχει άπειρα πρώτα ιδεώδη. Συνεπώς η γενίκευση του θεωρήματος για πρώτους σε αριθμητικές προόδους προκύπτει αν αποδείξουμε ότι $L_{\mathfrak{m}}(s,\chi)\neq 0$ όταν $\chi\neq\chi_0$. Αυτό καταλήγει να σχετίζεται με την έννοια του Weber για το class field. Πρώτα θα αποδείξουμε τον ισχυρισμό για το $\delta_F(\mathscr{S}_{\alpha,\mathfrak{m}})$.

Πρόταση 3.2.18. *Έστω $\alpha\in\mathscr{I}_F(\mathfrak{m})$. Υποθέτουμε ότι $\mathscr{P}^{+}_{F,\mathfrak{m}}<\mathscr{H}<\mathscr{I}_F(\mathfrak{m})$. Εάν για όλους τους χαρακτήρες $\chi\neq\chi_0$ του $\mathscr{I}_F(\mathfrak{m})$ που είναι τετριμμένοι στο $\mathscr{H}$ έχουμε $L_{\mathfrak{m}}(s,\chi)\neq 0$ τότε:*

$$\delta_F(\text{ πρώτοι } \mathfrak{p} \text{ στο } \mathscr{O}_F : \mathfrak{p}\in\alpha\mathscr{H}\}) = \frac{1}{[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}]}$$

Απόδειξη. Ισχύει ότι:

$$L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}}(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s})^{-1}$$

Λογαριθμώντας παίρνουμε:

$$\log L_{\mathfrak{m}}(s,\chi) = -\sum_{\mathfrak{p}\nmid\mathfrak{m}}\log(1-\chi(\mathfrak{p})N\mathfrak{p}^{-s})^{-1}$$

$$= \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n=1}^{\infty} \frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n}$$

$$= \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s} + \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n=2}^{\infty} \frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n}$$

$$\sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}$$

Εάν χ χαρακτήρας του $\mathscr{I}(\mathfrak{m})$ που είναι τεριμμένος στο $\mathscr{H}$ τότε μπορούμε να δούμε τον x σαν ένα χαρακτήρα του $\mathscr{I}_F(\mathfrak{m})/\mathscr{H}$. Για ένα σταθερό πρώτο $\mathfrak{p}$ του $\mathscr{O}_F$ έχουμε:

$$\sum_{\chi} \chi(\alpha)^{-1}\chi(\mathfrak{p}) = \begin{cases} 0 & \mathfrak{p} \notin \alpha\mathscr{H} \\ [\mathscr{I}(\mathfrak{m}) : \mathscr{H}] & \mathfrak{p} \in \alpha\mathscr{H} \end{cases}$$

όπου το άθροισμα εκτείνεται στους $\chi \in \widehat{\mathscr{I}_F(\mathfrak{m})/\mathscr{H}}$. Αν

$$\beta_{\chi}(s) = \sum_{\mathfrak{p}\nmid\mathfrak{m}} \sum_{n=2}^{\infty} \frac{\chi(\mathfrak{p})^n N\mathfrak{p}^{-ns}}{n}$$

παίρνουμε:

$$\sum_{\chi} \chi(\alpha)^{-1} \log L_{\mathfrak{m}}(s,\chi) = \sum_{\chi} \chi(\alpha)^{-1} [\sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s} + \beta_{\chi}(s)]$$

$$= \sum_{\chi} \chi(\alpha)^{-1} [\log L_{\mathfrak{m}}(s,\chi) - \beta_{\chi}(s)]$$

$$= \sum_{\mathfrak{p}\in\alpha\mathscr{H}} [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H})] N\mathfrak{p}^{-s} \tag{3.1}$$

Έστω $\mathscr{S} = \{\mathfrak{p}$ πρώτοι του $\mathscr{O}_F : \mathfrak{p} \in \alpha\mathscr{H}\}$. Πρέπει να δείξουμε ότι το:

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathscr{S}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})}$$

συγκλίνει στο επιθυμητό όριο. Από την (3.1) έχουμε:

$$\sum_{\mathfrak{p}\in\mathscr{S}} [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H})] N\mathfrak{p}^{-s} = \sum_{\chi\neq\chi_0} \chi(\alpha)^{-1} [\log L_{\mathfrak{m}}(s,\chi) - \beta_{\chi}(s)]$$

$$+ \log(s-1) L_{\mathfrak{m}}(s,\chi_0) - \log(s-1) - \beta_{\chi_0}(s)$$

Θέτοντας $h = [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}]$ το τελευταίο γίνεται:

$$\sum_{\mathfrak{p}\in\mathscr{S}} N\mathfrak{p}^{-s} = \frac{1}{h} \sum_{\chi\neq\chi_0} \chi(\alpha)^{-1} [\log L_{\mathfrak{m}}(s,\chi) - \beta_{\chi}(s)]$$

$$+\frac{1}{h}\log[(s-1)L_{\mathfrak{m}}(s,\chi_0)]+\frac{1}{h}\log(\frac{1}{s-1})-\frac{1}{h}\beta_{\chi_0}(s)$$

Από την τελευταία σχέση έχουμε:

$$\sum_{\mathfrak{p}\in\mathscr{S}}N\mathfrak{p}^{-s}-\frac{1}{h}\log(\frac{1}{s-1})=\frac{1}{h}\sum_{\chi\neq x_0}x(\alpha)^{-1}[\log L_{\mathfrak{m}}(s,\chi)-\beta_{\chi}(s)]+\frac{1}{h}\log[(s-1)L_{\mathfrak{m}}(s,\chi_0)]-\frac{1}{h}\beta_{\chi_0}(s)$$

Το δεξιό μέλος της παραπάνω εξίσωσης είναι φραγμένο όταν $s\to 1_+$ (μια και $L_{\mathfrak{m}}(1,x)\neq 0$ για κάθε $\chi\neq\chi_0$ και η $L_{\mathfrak{m}}(1,\chi_0)$ έχει έναν απλό πόλο στο $s=1$). Γι αυτό:

$$\frac{\sum_{\mathfrak{p}\in\mathscr{S}}N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})}-\frac{1}{h}\to 0$$

καθώς $s\to 1^+$. Αλλά τότε:

$$\delta_F(\mathscr{S})=\frac{1}{h}=\frac{1}{[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}]}$$

□

Θυμίζουμε ότι χρειάζεται να αποδείξουμε ότι $L_{\mathfrak{m}}(1,\chi)\neq 0$ όταν ο $\chi\neq\chi_0$ είναι τεριμμένος στο $\mathscr{H}$.Το επόμενο θεώρημα σχεδόν το επιτυγχάνει:

Θεώρημα 3.2.19. *Έστω η Galois επέκταση K/F όπου $\mathscr{P}^+_{F,\mathfrak{m}}<\mathscr{H}<\mathscr{I}_F(\mathfrak{m})$. Α υποθέσουμε ότι υπάρχει κάποιο σύνολο πρώτων $\mathscr{J}\subset\mathscr{H}$ με $\mathscr{S}_{K/F}\approx\mathscr{J}$. Τότε:*

$$[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}]\leq[K:F]$$

και $L_{\mathfrak{m}}(1,\chi)\neq 0$ όταν $\chi\neq\chi_0$ και ο x δεν είναι τεριμμένος στο $\mathscr{H}$.

Απόδειξη. Θεωρούμε $m(x)=\mathrm{ord}_{s=1}(L_{\mathfrak{m}}(s,\chi))$. Για $\chi\neq\chi_0$ ξέρουμε ότι $m(\chi)\geq 0$ ενώ $m(\chi_0)=-1$. Μια και ο χ είναι τετριμμένος στο $\mathscr{H}$ μπορούμε να δούμε τον x σαν έναν χαρακτήρα του $\mathscr{I}_F(\mathfrak{m})/\mathscr{H}$.

Υπάρχει σταθερά α τέτοια ώστε:

$$\prod_{x\in\widehat{\mathscr{I}(\mathfrak{m})/\mathscr{H}}}L_{\mathfrak{m}}(s,x)=\alpha(s-1)^{\sum_x m(\chi)}+\dots$$

Παίρνοντας λογαρίθμους παίρνουμε:

$$\sum_{\chi}\log L_{\mathfrak{m}}(s,\chi)\sim(\sum_{\chi}m(\chi))\log(s-1)$$
$$-(\sum_{\chi}m(\chi))\log(\frac{1}{s-1})$$

Ισχύει τώρα:

$$\log L_{\mathfrak{m}}(s,\chi)=\sum_{\mathfrak{p}\nmid\mathfrak{m}}\sum_{n=1}^{\infty}\frac{\chi(\mathfrak{p})^n}{nN\mathfrak{p}^{ns}}$$

$$\sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p}) N\mathfrak{p}^{-s}$$

όπως πριν, έτσι:

$$\sum_{\chi} \log L_{\mathfrak{m}}(s,\chi) \sim \sum_{\mathfrak{p}\in\mathscr{H}} [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}] N\mathfrak{p}^{-s}$$

όπως πριν. Συνεπώς:

$$\sum_{\mathfrak{p}\in\mathscr{H}} [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}] N\mathfrak{p}^{-s} \sim -(\sum_{\chi} m(\chi)) \log(\frac{1}{s-1})$$

Όμως ισχύει:

$$\sum_{\mathfrak{p}\in\mathscr{H}} [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}] N\mathfrak{p}^{-s} = [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}](\sum_{\mathfrak{p}\in\mathscr{J}} N\mathfrak{p}^{-s} + \sum_{\mathfrak{p}\in\mathscr{H}/\mathscr{J}} N\mathfrak{p}^{-s})$$

Διαιρώντας με $\log(\frac{1}{s-1})$ και παίρνοντας όρια για $s \to 1^+$ παίρνουμε:

$$-(\sum_{\chi} m(\chi)) = \lim_{s\to 1^+} \frac{[\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}] \sum_{\mathfrak{p}\in\mathscr{S}_{K/F}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})} +$$

$$\lim_{s\to 1^+} \frac{[\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}] \sum_{\mathfrak{p}\in\mathscr{H}-\mathscr{S}_{K/F}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})}$$

$$= [\mathscr{I} : \mathscr{H}]\delta_F(\mathscr{S}_{K/F}) + [\mathscr{I} : \mathscr{H}]\Theta$$

όπου Θ μια πεπαρασμένη και μη αρνητική σταθερά.

$$\geq [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}]/[K : F].$$

Αναφέρουμε εδώ ότι ο πρώτος όρος στο δεξί μέλος της παραπάνω ισότητας συγκλίνει αφού η πυκνότητα Dirichlet $\delta_F(\mathscr{S})_{K/F})$ υπάρχει, ενώ ο δεύτερος όρος στο δεξί μέλος συγκλίνει επίσης γιατί το αριστερό μέλος είναι πεπερασμένος αριθμός.

Επειδή $m(\chi) \geq 0$ κάθε $\chi \neq \chi_0$ και $m(\chi_0) = -1$ έχουμε:

$$1 \geq 1 - \sum_{\chi\neq\chi_0} m(\chi) \geq [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}]/[K : F] > 0$$

Ως εκ τούτου:

$$0 \geq -\sum_{\chi\neq\chi_0} m(\chi) > -1$$

Τότε όμως θα πρέπει:

$m(\chi) = 0$ για κάθε $\chi \neq \chi_0$. Άρα $-(\sum_{\chi} m(\chi)) = 1$ και:

$$1 \geq [\mathscr{I}_F(\mathfrak{m}) : \mathscr{H}]/[K : F]$$

δηλαδή

$$[K:F] \geq [\mathscr{I}_F(\mathfrak{m}:\mathscr{H}].$$

Τελικά όταν $x \neq x_0$ επειδή $m(\chi)=0$ εχουμε ότι η συνάρτηση $L_m(s,\chi)$ έχει ένα σταθερό και μη μηδενικό όρο ο οποίος αναπτύσεται σε δυνάμεις του $s-1$. Από αυτό συνεπάγεται ότι $L_m(s,\chi) \neq 0$ για κάθε $\chi \neq \chi_0$.

□

Πρόταση 3.2.20. *Πρόταση 3.2.20*

Εάν η επέκταση K/F είναι Galois και K είναι το class field για την $\mathscr{H}$ όπου $\mathscr{P}^+_{F,\mathfrak{m}} < \mathscr{H} < \mathscr{I}_F(\mathfrak{m})$ τότε:

$$[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}] = [K:F]$$

Απόδειξη

Έστω K το class field για την $\mathscr{H}$ δηλαδή:

$\{$πρώτα ιδεώδη $\mathfrak{p}$ του $\mathscr{O}_F : \mathfrak{p} \in \mathscr{H}\} \approx \mathscr{S}_{K/F}$

Τότε:

$\delta_F(\{$πρώτα ιδεώδη $\mathfrak{p} \in \mathscr{H}\} - \mathscr{S}_{K/F}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathscr{H}-\mathscr{S}_{K/F}} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})} = 0$

Προχωρώντας όπως στην απόδειξη του θεωρήματος 3.2.19 παίρνουμε:

$$1 = -\sum_{\chi} m(x) = [\mathscr{I}_F(\mathfrak{m}):\mathscr{H})]/[K:F].$$

Με την βοήθεια του θεωρήματος 3.2.19 θα είχαμε ολοκληρώσει την απόδειξη της γενίκευσης του θεωρήματος για πρώτους σε αριθμητικές προόδους αν είχαμε επιβεβαιώσει την ύπαρξη ενός class field για $\mathscr{H} = \mathscr{P}^+_{F,\mathfrak{m}}$. Με αυτό όμως δεν ασχολείται η εργασία αυτή.

Με όσα αναφέραμε έως τώρα μπορούμε να παρουσιάσουμε το παρακάτω θεώρημα που αποδίδεται στον Weber:

Θεώρημα 3.2.21 (Η δεύτερη θεμελιώδης ανισότητα της θεωρίας κλάσεων σωμάτων)**.** *Εάν η επέκταση K/F είναι επέκταση Galois σωμάτων αριθμών και με $\mathscr{H}$ συμβολίσουμε: $\mathscr{P}_{F,\mathfrak{m}} N_{K/F}(\mathfrak{m})$ όπου:*

$$N_{K/F}(\mathfrak{m}) = \{\alpha \in \mathscr{I}_F(\mathfrak{m}) : \alpha = N_{K/F}(\mathscr{U}), \mathscr{U} \in \mathscr{I}_K\}$$

(Ας επισημάνουμε εδώ ότι η παραγοντοποίηση του κλασματικού ιδεώδους $\mathscr{U}$ του K δεν μπορεί να περιέχει μια μη τετριμμένη δύναμη ενός πρώτου ιδεώδους που διαιρεί το $\mathfrak{m}\mathscr{O}_K$ δηλαδή $\mathscr{U} \in \mathscr{I}_K(\mathfrak{m}\mathscr{O}_K)$.)

Τότε:

$$[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}] \leq [K:F]$$

Απόδειξη. Έστω $\mathfrak{p} \in \mathscr{S}_{K/F}$ και $\mathscr{Q}|\mathfrak{p}$ όπου $\mathscr{Q}$ ένα πρώτο ιδεώδες του $\mathscr{O}_K$.Τότε $N_{K/F}\mathscr{Q} = \mathfrak{p}$ γιατί αφού $\mathfrak{p} \in \mathscr{S}_{K/F}$ αναλύεται πλήρως στην K/F δίνοντας $f(\mathscr{Q}/\mathfrak{p}) = 1$. Συνεπώς $\mathscr{S}_{K/F} \approx \mathscr{J}$ για κάποιο $\mathscr{J} \subset \mathscr{H}$ και μπορούμε να εφαρμόσουμε το προηγούμενο θεώρημα για να συμπεράνουμε ότι:

$$[\mathscr{I}_F(\mathfrak{m}):\mathscr{H}] \leq [K:F].$$

□

3.2.1 Τα κύρια θεωρήματα της θεωρίας κλάσεων σωμάτων.

Σε αυτή την ενότητα είδαμε από ιστορικής απόψεως τα αρχικά στάδια μερικών από τις κύριες ιδέες της θεωρίας class field. Πολλές από αυτές τις ιδέες αποδίδονται στους Kronecker,Weber και Hilbert. Παρόλα ταύτα οι ιδέες τους έμειναν ασαφείς έως τον εικοστό αιώνα. Η πλειονότητα αυτών των ιδεών γενικεύτηκαν από τον Takagi . Τα κυριότερα θεωρήματα λοιπόν της θεωρίας class field είναι:

Θεώρημα 3.2.22 (Ύπαρξης)**.** *Για κάθε $\mathscr{H}$ με:*

$$\mathscr{P}^{+}_{F,\mathfrak{m}} < \mathscr{H} < \mathscr{I}_F(\mathfrak{m})$$

υπάρχει ένα class field K/F συσχετιζόμενο με το $\mathscr{H}$.

Θεώρημα 3.2.23 (Πληρότητας)**.** *Για κάθε αβελιανή επέκταση K/F υπάρχει ένα:*

$\mathfrak{m}$ *και ένα $\mathscr{H}$ με:*

$$\mathscr{P}^{+}_{F,\mathfrak{m}} < \mathscr{H} < \mathscr{I}_F(\mathfrak{m})$$

τέτοια ώστε το K να είναι το class field του F υπέρ $\mathscr{H}$.

Θεώρημα 3.2.24 (Ισομορφισμού)**.** *Όταν $\mathscr{P}^{+}_{F,\mathfrak{m}} < \mathscr{H} < \mathscr{I}_F(\mathfrak{m})$ και K είναι το class field του F υπέρ $\mathscr{H}$ ισχύει:*

$$\mathrm{Gal}(K/F) \cong \mathscr{I}_F(\mathfrak{m})/\mathscr{H}$$

όπου ο ισομορφισμός εισάγεται από την απεικόνιση του Artin.

Βιβλιογραφία

1 Ι.Αντωνιάδης Α.Κοντογεώργης. Αριθμητική Γεωμετρία , Ιστορία , Επιτεύγματα και μέλλον. Τόμος της Ελληνικής Μαθηματικής Εταιρείας για τα 100 χρόνια από την ίδρυση της , 2018

2 Nancy Childress . Class Field Theory Springer , 2009

3 Gerald J. Janusz . Algebraic Number Fields volume 7 of Graduate Studies in Mathematics American Mathematical Society , 1996

4 Fernando Q. Gouvea. p-adic Numbers , p-adic Analysis and Zeta -Functions Second Edition volume 58 of Graduate Texts in Mathematics Springer , 1977

5 Ι. Αντωνιάδης, Αλγεβρική Θεωρία Αριθμών, σημειώσεις μεταπτυχιακού μαθήματος.