Μια Εισαγωγή στη Θεωρία Iwasawa

Δημήτριος Νούλας

Μεταπτυχιακή Εργασία

Πανεπιστήμιο Αθηνών,
Τμήμα Μαθηματικών

Αθήνα, Δεκέμβριος 2022

Εισηγητής:

Αριστείδης Κοντογεώργης

Επιτροπή:

Αριστείδης Κοντογεώργης

Ιωάννης Εμμανουήλ

Μαρία Χλουβεράκη

Στον αδερφό μου Θωμά.

Περιεχόμενα

Εισαγωγή

Αρχικά, η θεωρία Iwasawa είχε ως στόχο την μελέτη των μεθεθών των ομάδων κλάσεων ιδεωδών για τα κυκλοτομικά σώματα και σώματα που σχετίζονται με αυτά. Τα πιο πρόσφατα αποτελέσματα της θεωρίας αυτής πλέον διατυπώνονται ως διάφορες μορφές μιας «κύριας εικασίας» της θεωρίας Iwasawa. Η πρώτη απλή μορφή που σχετίζεται με αβελιανές επεκτάσεις του $\mathbb{Q}$ αποδείχθηκε το 1984 από τους Mazur και Wiles και στην συνέχεια το 1990 για τα πλήρως πραγματικά σώματα από τον Wiles. Μια κύρια εικασία αυτής της μορφής συσχετίζει τα μεγέθη των ομάδων κλάσεων, ή ειδικότερα των ομάδων Selmer, στις p-αδικές L-συναρτήσεις. Σε αυτήν την μεταπτυχιακή εργασία θα εστιάσουμε στην κλασική θεωρία και στα βασικά αποτελέσματα με απώτερο στόχο να αποδείξουμε το θεώρημα του Iwasawa για τα μεγέθη των ομάδων κλάσεων για τα σώματα που βρίσκονται ενδιάμεσα σε $\mathbb{Z}_p$-επεκτάσεις.

Η δομή της εργασίας είναι ως εξής. Στο επόμενο κεφάλαιο, δίνουμε τα απαραίτητα προαπαιτούμενα που θα χρειαζόταν ένας μεταπτυχιακός φοιτητής για να ακολουθεί εύκολα τα επιχειρήματα που θα ακολουθήσουν για την βασική θεωρία. Στην συνέχεια, δίνουμε τους απαραίτητους ορισμούς και εργαλεία για τα διάφορα αποτελέσματα της κλασικής θεωρίας Iwasawa που σχετίζονται με τις τάξεις των ομάδων κλάσεων, όπου γίνεται εμφανής η σύνδεση των τάξεων αυτών με ειδικές τιμές των L-συναρτήσεων, των p-αδικών L-συναρτήσεων, των αριθμών Bernoulli και των irregular πρώτων αριθμών.

Στο τρίτο κεφάλαιο αναπτύσσουμε τις ιδιότητες που έχει η άλγεβρα Iwasawa $\Lambda = \mathbb{Z}_p[[T]]$ και κάθε πεπερασμένη επέκτασή της, βασιζόμενοι στην δομή των τοπικών σωμάτων K που είναι επεκτάσεις του $\mathbb{Q}_p$ και τα εργαλεία που αποκτούμε με το να θεωρήσουμε δακτύλιους τυπικών δυναμοσειρών με συντελεστές από τους δακτύλιους ακεραίων $\mathcal{O}_K$. Με αυτά τα εργαλεία, δείχνουμε αρχικά ότι το Λ επιδέχεται έναν αλγόριθμο διαίρεσης, ο οποίος με την σειρά του μας δίνει ένα πολύ ισχυρό θεώρημα δομής των Λ-προτύπων, όμοιο με το κλασικό θεώρημα δομής πάνω από περιοχές κυρίων ιδεωδών.

Στο τέταρτο κεφάλαιο χρησιμοποιούμε μια διαφορετική προσέγγιση για την άλγεβρα Iwasawa, βλέποντας την ως το προβολικό όριο ομαδοδακτυλίων $\mathbb{Z}_p[\Gamma_n]$. Ταυτόχρονα, κοιτάμε την p-Sylow υποομάδα X_n της ομάδας κλάσεων σε κάθε πεπερασμένο στρώμα καθώς ανεβαίνουμε μια $\mathbb{Z}_p$-επέκταση, όπου γίνεται η συσχέτιση των X_n ως $\mathbb{Z}_p[\Gamma_n]$-προτύπων. Ως συνέπεια, με τις πληροφορίες που μας δίνει η θεωρία κλάσεων σωμάτων για τα X_n, το ισχυρό θεώρημα δομής και τις δύο διαφορετικές όψεις της άλγεβρας Λ, παίρνουμε το επιθυμητό αποτέλεσμα για τον ρυθμό αύξησης των $|X_n|$ που είναι γνωστό ως θεώρημα Iwasawa.

Τέλος, στο κεφάλαιο 5 αναπτύσσουμε περαιτέρω τις ιδέες του προηγούμενου κεφαλαίου ώστε να παρέχουμε το κατάλληλο υπόβαθρο για να διατυπωθεί η κύρια εικασία για τα πλήρως πραγματικά σώματα. Επιπλέον, χρησιμοποιώντας την κύρια εικασία παίρνουμε ένα ακόμα αποτέλεσμα για τα μεγέθη των ομάδων κλάσεων.

Δίνουμε παρακάτω μια γρήγορη περιγραφή των όρων και την αλληλεπίδρασή τους, όπως αυτή γίνεται εμφανής στα επόμενα κεφάλαια.

Έστω $K_n = \mathbb{Q}(\zeta_{p^n})$ για $n \geq 1$ και $K_\infty = \mathbb{Q}(\zeta_{p^\infty}) = \cup K_n$. Έχουμε τον ισομορφισμό

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times$$

$$\sigma \longmapsto a_\sigma \in \mathbb{Z}_p^\times$$

που καθορίζεται πλήρως από την σχέση

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_\sigma}.$$

Υπενθυμίζουμε ότι έχουμε επιπλέον τον ισομορφισμό

$$\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p.$$

Θέτουμε $\mathbb{Q}_\infty = K_\infty^{(\mathbb{Z}/p\mathbb{Z})^\times}$, έτσι ώστε

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p.$$

Η επέκταση $\mathbb{Q}_\infty/\mathbb{Q}$ είναι αυτό που εννοούμε ως $\mathbb{Z}_p$-επέκταση. Έστω $\gamma \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ να είναι τέτοιο ώστε $\gamma \longmapsto 1+p \in \mathbb{Z}_p^\times$ στον παραπάνω ισομοριψμό. Η εικόνα του γ μέσα στην $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ είναι ένας τοπολογικός γεννήτορας και θα συνεχίζουμε να τον συμβολίζουμε με γ.

Έστω $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times$ ένας πρωταρχικός χαρακτήρας Dirichlet. Βλέπουμε τον χ ως χαρακτήρα της $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ μέσα από την προβολή στο πηλίκο:

$$\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times.$$

Έστω $\mathbb{Q}^\chi = \overline{\mathbb{Q}}^{\ker\chi}$ να είναι το σώμα διάσπασης του χ. Δηλαδή, έχουμε ότι

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^\chi) \cong \ker\chi,$$

άρα το χ μπορούμε να το βλέπουμε και σαν χαρακτήρα της $\mathrm{Gal}(\mathbb{Q}^\chi/\mathbb{Q})$. Υποθέτουμε ότι $\mathbb{Q}^\chi \cap \mathbb{Q}_\infty = \mathbb{Q}$ και θέτουμε $F_\infty = \mathbb{Q}^\chi\mathbb{Q}_\infty$. Με αυτά, θα έχουμε ότι

$$\mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Gamma \times \Delta,$$

όπου

$$\Delta = \mathrm{Gal}(F_\infty/\mathbb{Q}_\infty) \cong \mathrm{Gal}(\mathbb{Q}^\chi/\mathbb{Q}),$$

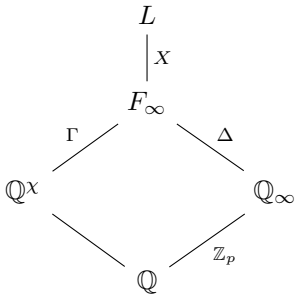
άρα βλέπουμε το χ και σαν χαρακτήρα του Δ και σαν χαρακτήρα του Γ, εφόσον

$$\Gamma = \mathrm{Gal}(F_\infty/\mathbb{Q}_\chi) \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p.$$

Έχουμε ότι υπάρχουν σώματα $F_n \subset F_\infty$ που αντιστοιχούν στις υποομάδες Γ^{p^n} του Γ, όπως και $\mathbb{Q}_n$ να αντιστοιχούν στις υποομάδες $p^n\mathbb{Z}_p$ του $\mathbb{Z}_p$, έτσι ώστε

$$\mathrm{Gal}(F_n/\mathbb{Q}^\chi) \cong \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Έστω L_n να είναι η μέγιστη αδιακλάδιστη αβελιανή p-επέκταση του F_n. Η ομάδα $X_n = \mathrm{Gal}(L_n/F_n)$ είναι ισόμορφη με την p-Sylow υποομάδα A_n της ομάδας κλάσεων ιδεωδών του F_n. Για $L = \cup L_n$, θέτουμε $X = \mathrm{Gal}(L/F_\infty)$ και έτσι έχουμε το ακόλουθο διάγραμμα σωμάτων.



Συνεπώς, το X είναι ένα $\Delta \times \Gamma$-πρότυπο. Ειδικότερα, είναι ένα $\mathbb{Z}_p[[\Gamma]]$-πρότυπο και αποδεικνύουμε ότι $\mathbb{Z}_p[[\Gamma]] \cong \Lambda := \mathbb{Z}_p[[T]]$. Δηλαδή, έχουμε ότι το X είναι ένα Λ-πρότυπο και μάλιστα πεπερασμένα παραγόμενο Λ-στρέψης, οπότε υπάρχει ένας ομομορφισμός Λ-προτύπων

$$X \longrightarrow \left(\bigoplus_{i=1}^{r} \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda/(f_j(T)^{m_j})\right).$$

Έχουμε ότι ο πυρήνας και συνπυρήνας του παραπάνω ομομορφισμού είναι πεπερασμένοι και $\mu_i, m_j \geq 0$ και τα $f_j(T)$ είναι ανάγωγα μονικά πολυώνυμα στο $\mathbb{Z}_p[T]$. Επιπλέον, οι όροι μ_i και το πολυώνυμο $f_X(T) = \prod f_j(T)^{m_j}$ καθορίζονται μοναδικά από το X.

Τα προηγούμενα που αναφέραμε είναι λόγω του θεωρήματος δομής των Λ-προτύπων και το ακόλουθο είναι το θεώρημα του Iwasawa που μας λέει ακριβώς τον ρυθμό αύξησης του p-μέρους της ομάδας κλάσεων ιδεωδών μέσα σε μια $\mathbb{Z}_p$-επέκταση.

Θεώρημα 1.1 (Iwasawa). *Έστω p^{e_n} να είναι η δύναμη του p που διαιρεί την τάξη της ομάδας κλάσεων του F_n. Τότε υπάρχουν ακέραιοι $\lambda \geq 0, \mu \geq 0$ και ν, όλα ανεξάρτητα από το n, μαζί με $n_0 \in \mathbb{N}$ τέτοιο ώστε για κάθε $n \geq n_0$ να έχουμε*

$$e_n = \lambda n + \mu p^n + \nu.$$

Θέτουμε $V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$. Το V είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος καθώς

$$V \cong \overline{\mathbb{Q}}_p(T)/(f_X(T)).$$

Επιπλέον, θέτουμε

$$V^\chi = \{v \in V : \ \sigma v = \chi(\sigma) v \ \forall \ \sigma \in \Delta\}.$$

Αυτό είναι το χ-ισοτυπικό κομμάτι του V. Έστω $f_\chi(T)$ να είναι το χαρακτηριστικό πολυώνυμο της δράσης του $\gamma - 1$ στο V^χ, όπως το $f_X(T)$ είναι το χαρακτηριστικό πολυώνυμο της δράσης του $\gamma - 1$ στο V. Άρα έχουμε και ότι $f_\chi(T) \mid f_X(T)$. Αν αντί να θεωρήσουμε το τανυστικό γινόμενο με το $\overline{\mathbb{Q}}_p$ και παίρναμε στην θέση του το $\mathcal{O}_\chi := \mathbb{Z}_p[\chi]$ θα παίρναμε έναν επιπλέον όρο μ_χ, που θα αντιστοιχούσε στην δύναμη που εμφανίζεται ο uniformizer π του $\mathcal{O}_\chi$.

Η κύρια εικασία συσχετίζει το χαρακτηριστικό πολυώνυμο $f_\chi(T)$ και τον όρο μ_χ με μια p-αδική L-συνάρτηση και έναν αναλυτικό όρο μ. Έστω ψ ένας πρωταρχικός χαρακτήρας Dirichlet. Θέτουμε

$$H_\psi(T) = \begin{cases} \psi(1+p)(1+T) - 1 & \psi = 1 \ \text{ή έχει conductor μια δύναμη του } p, \\ 1 & \text{διαφορετικά.} \end{cases}$$

Υπάρχει $G_\psi(T) \in \mathcal{O}_\psi[[T]]$ τέτοια ώστε

$$\mathcal{L}_p(1-s, \psi) = G_\psi((1+p)^s - 1)/H_\psi((1+p)^s - 1) \quad (s \in \mathbb{Z}_p)$$

έτσι ώστε

$$\mathcal{L}_p(1-n, \psi) = (1 - \psi\omega^{-n}(p)p^{n-1})L(1-n, \psi\omega^{-n}) \quad (n \geq 1).$$

Αυτή είναι η p-αδική L-συναρτήση για την οποία θα δώσουμε περισσότερες λεπτομέρειες αργότερα. Από το θεώρημα προπαρασκευής του Weierstrass μπορούμε να γράψουμε

$$G_\psi(T) = \pi^{\mu_\psi^{\text{an}}} g_\psi(T) u_\psi(T),$$

όπου $\mu_\psi^{\text{an}} \geq 0$, το $g_\psi(T)$ είναι μονικό πολυώνυμο στο $\mathcal{O}_\psi[T]$ και το $u_\psi(T)$ είναι αντιστρέψιμο στο $\mathcal{O}_\psi[[T]]$.

Θεώρημα 1.2 (Κύρια Εικασία της Θεωρίας Iwasawa)**.** *Έστω χ ένας περιττός χαρακτήρας τάξης σχετικά πρώτης με το p για τον οποίο ισχύει ότι $\mathbb{Q}^{\chi} \cap \mathbb{Q}_{\infty} = \mathbb{Q}$. Τότε*

$$f_{\chi}(T) = g_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1)$$

και

$$\mu_{\chi} = \mu^{\mathrm{an}_{\chi^{-1}\omega}}.$$

Χρησιμοποιώντας την κύρια εικασία παίρνουμε ένα ακόμα αποτέλεσμα για τα μεγέθη των τάξεων των ομάδων κλάσεων.

Θεώρημα 1.3. *Έστω p ένας περιττός πρώτος και F μια αβελιανή φανταστική επέκταση του $\mathbb{Q}$ βαθμού σχετικά πρώτου με το p. Έστω $\chi : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}_p^{\times}$ να είναι ένας περιττός χαρακτήρας. Υποθέτουμε ότι $\chi \neq \omega$, τότε*

$$|A_F^{\chi}| = |\mathcal{O}_{\chi}/(\mathcal{L}_p(0, \chi^{-1}\omega))|,$$

όπου A_F^{χ} είναι το χ-ισοτυπικό κομμάτι του p-μέρους της ομάδας κλάσεων ιδεωδών του F.

Προαπαιτούμενα

Σε αυτό το κεφάλαιο θα υπενθυμίσουμε διάφορα αποτελέσματα που χρειαζόμαστε, ξεκινώντας από την αλγεβρική θεωρία αριθμών. Στην συνέχεια, θα αναφέρουμε τα βασικά στοιχεία των κυκλοτομικών σωμάτων, καθώς σε αυτά επικεντρώνεται κυρίως η κλασική θεωρία Iwasawa. Επιπλέον, θα είναι αναγκαίο να εργαζόμαστε με επεκτάσεις σωμάτων άπειρου βαθμού και τις αντίστοιχες ομάδες Galois, οπότε διατυπώνουμε το θεμελιώδης θεώρημα για τις άπειρες επεκτάσεις που γενικεύει με την χρήση της τοπολογίας την πεπερασμένη περίπτωση. Θα κλείσουμε το κεφάλαιο με κάποια βασικά στοιχεία της θεωρίας κλάσεων σωμάτων, η οποία έχει σκοπό να περιγράψει τις αβελιανές επεκτάσεις των σωμάτων αριθμών. Για να δει κανείς τα αποτελέσματα από όσα αναφέραμε παραπάνω πιο λεπτομερώς και με αποδείξεις μπορεί να ανατρέξει στα βιβλία του Milne [14], [15] ή στα [2], [12].

2.1 Άλγεβρική Θεωρία Αριθμών

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

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

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

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

Έχοντας ένα πρώτο ιδεώδες $\mathfrak{p} \subset \mathcal{O}_K$, μπορούμε να θεωρήσουμε το ιδεώδες $\mathfrak{p}\mathcal{O}_L$ στον δακτύλιο $\mathcal{O}_L$. Οπότε, με βάση το προηγούμενο θεώρημα μπορούμε να το παραγοντοποιήσουμε σε γινόμενο πρώτων ιδεωδών:

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

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

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

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

Θεώρημα 2.4. *Με βάση τα παραπάνω έχουμε:*

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

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

Πρόταση 2.5. *Η ομάδα* $\mathrm{Gal}(L/K)$ *δρα μεταβατικά στο σύνολο των πρώτων ιδεωδών* $\mathfrak{p}_i$ *του* $\mathcal{O}_L$ *που στέκονται πάνω από το* $\mathfrak{p}$.

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

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

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

Ορισμός 2.7. *Έστω* $\mathfrak{q}$ *ένα πρώτο ιδεώδες του* $\mathcal{O}_L$. *Η υποομάδα*

$$D_{\mathfrak{q}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

λέγεται η ομάδα διάσπασης του $\mathfrak{q}$ *υπεράνω του* K.

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

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

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

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

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

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

Έχουμε μια φυσιολογική απεικόνιση:

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

όπου ένα $\sigma \in D_{\mathfrak{q}}$, εφόσον κρατάει σταθερό το $\mathfrak{q}$, επάγει έναν $\mathcal{O}_L/\mathfrak{q}$-αυτομορφισμό $\overline{\sigma}$. Ο αυτομορφισμός $\overline{\sigma}$ με την σειρά του κρατάει σταθερό το υπόσωμα $\mathcal{O}_K/\mathfrak{p}$, διότι ο σ κρατάει σταθερό το K. Όπως αποδεικνύεται στην πρόταση 14 του βιβλίου του Lang [13], αυτή η απεικόνιση είναι επί.

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

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

Από το πόρισμα 2.8 έχουμε ότι:

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

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

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

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

Επιπλέον, είναι σημαντικό το ακόλουθο αποτέλεσμα για τις ομάδες διάσπασης.

Πρόταση 2.11. *Έστω L/K επέκταση Galois, $\mathfrak{p}$ πρώτο ιδεώδες του $\mathcal{O}_K$ και $\mathfrak{q}$ πρώτο ιδεώδες του $\mathcal{O}_L$ με $\mathfrak{q} \mid \mathfrak{p}$. Υπάρχει ισομορφισμός $D_{\mathfrak{q}} \cong \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}})$ όπου με $L_{\mathfrak{q}}$ και $K_{\mathfrak{p}}$ συμβολίζουμε τις πληρώσεις των σωμάτων ως προς τις αντίστοιχες νόρμες που επάγουν τα πρώτα ιδεώδη.*

2.2 Κυκλοτομικά Σώματα

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

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

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

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

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

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

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

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

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

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

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

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

Χρησιμοποιώντας το ακόλουθο λήμμα, το παραπάνω αποτέλεσμα γενικεύεται για τα κυκλοτομικά σώματα $\mathbb{Q}(\zeta_n)$ όπου $n \in \mathbb{N}$.

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

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

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

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

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

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

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

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

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

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

Παρατήρηση. *Εφόσον $\phi(p^r) = p^{r-1}(p-1)$, αν το n είναι 2 επί κάποιον περιττό αριθμό και $p = 2$, τότε θα ισχύει η περίπτωση που το 2 διαιρεί το n αλλά δεν διακλαδίζεται. Επιπλέον, σε αυτήν την περίπτωση έχουμε ότι $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.*

Παρατήρηση. *Έστω $K = \mathbb{Q}(\zeta_p)$. Οι μόνες ρίζες της μονάδας που βρίσκονται στο K είναι οι ζ_p^s για τα $1 \leq s \leq p-1$. Αυτό έπεται από το αποτέλεσμα ότι $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ αν $\gcd(m, n) = 1$.*

Μπορούμε να πούμε κάποια παραπάνω αποτελέσματα σχετικά με το πως ένας πρώτος p διασπάται στο $\mathbb{Q}(\zeta_n)$ αν $p \nmid n$.

Λήμμα 2.16. *Έστω p ένας πρώτος τέτοιος ώστε $p \nmid n$. Έστω $\mathfrak{p}$ πρώτος του $\mathbb{Q}(\zeta_n)$ που στέκεται πάνω από το p. Τότε οι n-οστές ρίζες της μονάδας είναι διακεκριμένες modulo $\mathfrak{p}$.*

Λήμμα 2.17. *Έστω p ένας πρώτος τέτοιος ώστε $p \nmid n$. Έστω f να είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε $p^f \equiv 1 (\mathrm{mod}\, n)$. Τότε ο p διασπάται σε $\phi(n)/f$ διακεκριμένους πρώτους του $\mathbb{Q}(\zeta_n)$, όπου για τον καθένα η αντίστοιχη τάξη του σώματος υπολοίπων είναι f. Ειδικότερα, το p διασπάται πλήρως αν και μόνο αν $p \equiv 1 (\mathrm{mod}\, n)$.*

2.3 Άπειρη Θεωρία Galois

Έστω K/k μια Galois επέκταση σωμάτων. Όπως συνηθίζεται, θα γράφουμε $\mathrm{Gal}(K/k)$ για το σύνολο των αυτομορφισμών του K που διατηρούν το k σταθερό κατά σημείο. Έστω F μια ενδιάμεση πεπερασμένη επέκταση, δηλαδή $k \subseteq F \subseteq K$ με $[F : k] < \infty$. Ειδικότερα, η $\mathrm{Gal}(K/F)$ είναι υποομάδα πεπερασμένου δείκτη της $\mathrm{Gal}(K/k)$. Ορίζουμε μια τοπολογία στην $\mathrm{Gal}(K/k)$ όπου τα σύνολα $\mathrm{Gal}(K/F)$ σχηματίζουν μια βάση περιοχών του ουδέτερου στοιχείου της $\mathrm{Gal}(K/k)$. Αυτή η τοπολογία αναφέρεται στην βιβλιογραφία ως τοπολογία του Krull και κάνει την ομάδα $\mathrm{Gal}(K/k)$ pro-πεπερασμένη, δηλαδή σαν τοπολογικό χώρο την κάνει Hausdorff, συμπαγή και πλήρως ασυνεκτική. Επιπλέον,

$$\mathrm{Gal}(K/k) \cong \varprojlim_F \mathrm{Gal}(K/k)/\mathrm{Gal}(K/F) \cong \varprojlim_F \mathrm{Gal}(F/k)$$

όπου το F διατρέχει τις πεπερασμένες κανονικές επεκτάσεις F/k ή κάθε υπακολουθία τους, έτσι ώστε $\cup F = K$. Η διάταξη που χρησιμοποιούμε στο αντίστροφο όριο είναι του περιέχεσθαι και ως απεικονίσεις είναι οι φυσιολογικές απεικονίσεις περιορισμού $\mathrm{Gal}(F_2/k) \longrightarrow \mathrm{Gal}(F_1/k)$ για $F_1 \subseteq F_2$. Με τα παραπάνω, το θεμελιώδης θεώρημα της θεωρίας Galois διατυπώνεται ως εξής.

Θεώρημα 2.18 (Θεμελιώδης Θεώρημα Θεωρίας Galois)**.** *Έστω K/k μια Galois επέκταση. Υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ των κλειστών υποομάδων H της $\mathrm{Gal}(K/k)$ και των ενδιάμεσων επεκτάσεων $k \subseteq F \subseteq K$ έτσι ώστε*

$$H \longleftrightarrow K^H$$

$$\mathrm{Gal}(K/L) \longleftrightarrow L$$

Οι ανοιχτές υποομάδες αντιστοιχούν στις πεπερασμένες υποεπεκτάσεις.

Ένα σημαντικό παράδειγμα είναι η επέκταση $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$. Την αποκτάμε με το να επισυνάψουμε όλες τις n-οστές ρίζες της μονάδας, όπου το n διατρέχει τις δυνάμεις του p. Βασιζόμενοι σε αυτήν την επέκταση θα κατασκευάσουμε στα επόμενα κεφάλαια την λεγόμενη $\mathbb{Z}_p$-επέκταση του $\mathbb{Q}$. Γνωρίζουμε ότι ένα στοιχείο της $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ καθορίζεται πλήρως από την δράση του στις ρίζες της μονάδας που αναφέραμε. Έστω $n \in \mathbb{N}$. Για ένα $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ έχουμε $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\sigma_n}$ για κάποιο $\sigma_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Παρατηρούμε ότι $\sigma_n \equiv \sigma_{n-1} (\mathrm{mod}\, p^{n-1})$ για κάθε $n \geq 1$. Ειδικότερα, αυτό μας δείχνει ότι παίρνουμε ένα στοιχείο της ομάδας

$$\mathbb{Z}_p^\times \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}).$$

Αντίστροφα, είναι εύκολο να δούμε ότι για ένα $a \in \mathbb{Z}_p^\times$ έχουμε ένα στοιχείο

$$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$$

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$$

που καθορίζεται πλήρως από την παραπάνω δράση. Άρα έχουμε ότι

$$\mathbb{Z}_p^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}).$$

Επιπλέον, η κλειστή υποομάδα $1 + p^n\mathbb{Z}_p$ αντιστοιχεί στο σταθερό της σώμα $\mathbb{Q}(\zeta_{p^n})$.

Έστω τώρα K/k μια Galois επέκταση, η οποία δεν είναι απαραίτητα πεπερασμένη. Έστω $\mathcal{O}_K$ και $\mathcal{O}_k$ να είναι οι δακτύλιοι ακεραίων των K και k αντίστοιχα. Θα θέλαμε να έχουμε κάτι αντίστοιχο με την διακλάδωση των πρώτων ιδεωδών όπως γίνεται στα σώματα αριθμών, ωστόσο δεν ισχύει γενικά ότι οι $\mathcal{O}_K$ και $\mathcal{O}_k$ είναι περιοχές Dedekind, ώστε να έχουμε το μονοσήμαντο της παραγοντοποίησης. Για παράδειγμα, στο σώμα $K = \mathbb{Q}(\zeta_{p^\infty})$ που αναφέραμε πριν, ο δακτύλιος $\mathcal{O}_K$ δεν είναι περιοχή του Dedekind. Για να το δει κανείς, αρκεί να θεωρήσει την p-οστή δύναμη του πρώτου ιδεωδούς $\mathfrak{p} = (\zeta_p - 1, \zeta_{p^2} - 1, \ldots)$.

Εφόσον δεν γίνεται να ορίσουμε την διακλάδωση των πρώτων ιδεωδών ως προς την παραγοντοποίησή τους, πρέπει να το κάνουμε με άλλο τρόπο. Υπενθυμίζουμε ότι στις πεπερασμένες επεκτάσεις, αν e είναι ο δείκτης διακλάδωσης ενός πρώτου ιδεωδούς $\mathfrak{q}$ που στέκεται πάνω από το $\mathfrak{p}$, τότε έχουμε ότι $e = |I_\mathfrak{q}|$ με $I_\mathfrak{q}$ να είναι η ομάδα αδράνειας. Με βάση αυτό θα ορίσουμε την διακλάδωση στις άπειρες επεκτάσεις.

Όπως στην πεπερασμένη περίπτωση, ορίζουμε την ομάδα διάσπασης $D_\mathfrak{q}$ ενός πρώτου ιδεωδούς $\mathfrak{q} \subset \mathcal{O}_K$ που στέκεται πάνω από το $\mathfrak{p} \subset \mathcal{O}_k$ ως εξής.

$$D_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(K/k) : \ \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

και την ομάδα αδράνειας ως

$$I_\mathfrak{q} = \{\sigma \in D_\mathfrak{q} : \ \sigma(a) \equiv a (\mathrm{mod}\, \mathfrak{q}) \quad \forall\, a \in \mathcal{O}_K\}$$

Συνεπώς, ορίζουμε τον δείκτη διακλάδωσης $e = e(\mathfrak{q} \mid \mathfrak{p})$ να είναι η τάξη, όχι απαραίτητα πεπερασμένη, της ομάδας $I_\mathfrak{q}$.

Η αντίστοιχη κατάσταση για τις άπειρες θέσεις, δηλαδή τους αρχιμήδειους πρώτους, διαφέρει ελάχιστα. Σε αυτή τη περίπτωση, το e παίρνει μόνο τις τιμές 1 ή 2. Συγκεκριμένα, το $I_\mathfrak{q}$ είναι μη-τετριμμένο στην άπειρη επέκταση μόνο όταν το $\mathfrak{p}$ είναι πραγματικό και το $\mathfrak{q}$ μιγαδικό. Ειδικότερα, η ομάδα αδράνειας παράγεται από την απεικόνιση του μιγαδικού συζυγή.

2.4 Θεωρία Κλάσεων Σωμάτων

Έστω k ένα σώμα αριθμών και $I = I_k$ να είναι η ομάδα των κλασματικών ιδεωδών του k. Θεωρούμε S να είναι ένα πεπερασμένο σύνολο θέσεων του k και I^S η υποομάδα της I που παράγεται από τα πρώτα ιδεώδη που δεν ανήκουν στο S. Επιπλέον, έστω $\mathfrak{m}_f = \prod \mathfrak{p}_i^{e_i}$ να είναι ένα ακέραιο ιδεώδες του k και $\mathfrak{m}_\infty$ να είναι ένα ελεύθερο τετραγώνων γινόμενο πραγματικών αρχιμήδειων θέσεων του k. Θα λέμε το $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$ έναν *διαιρέτη* του k, με $\mathfrak{m}(\mathfrak{p}_i) = e_i$. Για $a \in \mathcal{O}_k$, θα γράφουμε $a \equiv 1 (\mathrm{mod}^*\, \mathfrak{m})$ αν

(1) $\nu_{\mathfrak{p}_i}(a-1) \geq e_i$ για όλους τους πρώτους $\mathfrak{p}_i \mid \mathfrak{m}_f$.

(2) $a > 0$ για όλους τους πραγματικούς πρώτους που διαιρούν το $\mathfrak{m}_\infty$.

Θέτουμε $P_{\mathfrak{m},1}$ να είναι το σύνολο των κύριων ιδεωδών του $\mathcal{O}_k$ που παράγονται από ένα στοιχείο a, έτσι ώστε $a \equiv 1 (\mathrm{mod}^* \mathfrak{m})$. Θα γράφουμε ως $S(\mathfrak{m})$ το σύνολο των πρώτων που διαιρούν το $\mathfrak{m}$.

Ορισμός 2.19. *Έστω $\mathfrak{m}$ ένας διαιρέτης του k. Η ομάδα $C_\mathfrak{m} = I^{S(\mathfrak{m})}/P_{\mathfrak{m},1}$ ονομάζεται ray ομάδα κλάσεων του k modulo $\mathfrak{m}$.*

Θεώρημα 2.20 (Θεώρημα 1.7 στο [15])**.** *Για κάθε $\mathfrak{m}$ διαιρέτη του k, υπάρχει ακριβής ακολουθία*

$$0 \longrightarrow U/U_{\mathfrak{m},1} \longrightarrow P_\mathfrak{m}/P_{\mathfrak{m},1} \longrightarrow C_\mathfrak{m} \longrightarrow 0$$

και κανονικοί ισομορφισμοί

$$P_\mathfrak{m}/P_{\mathfrak{m},1} \cong \prod_{\substack{\mathfrak{p}|\infty \\ \mathfrak{p}|\mathfrak{m}}} \{\pm 1\} \times \prod_{\substack{\mathfrak{p}\nmid\infty \\ \mathfrak{p}|\mathfrak{m}}} \left(\mathcal{O}_k/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\right)^\times \cong \prod_{\substack{\mathfrak{p}|\infty \\ \mathfrak{p}|\mathfrak{m}}} \{\pm 1\} \times (\mathcal{O}_k/\mathfrak{m}_f)^\times$$

όπου

$$\begin{aligned} P_\mathfrak{m} &= \{a \in k^\times : \ \mathrm{ord}_\mathfrak{p}(a) = 0 \ \ \textit{για κάθε } \mathfrak{p} \mid \mathfrak{m}_f\}, \\ U &= \mathcal{O}_k^\times, \\ U_{\mathfrak{m},1} &= U \cap P_{\mathfrak{m},1}. \end{aligned}$$

Για παράδειγμα, αν $\mathfrak{m} = 1$ η ray ομάδα κλάσεων $C_\mathfrak{m}$ δεν είναι τίποτα παραπάνω από την συνήθη ομάδα κλάσεων ιδεωδών. Επιπλέον, αν $n \in \mathbb{N}$ και $\mathfrak{m} = n$, τότε το $I^{S(\mathfrak{m})}$ είναι το σύνολο των ιδεωδών που παράγονται από τους ρητούς αριθμούς, οι οποίοι είναι σχετικά πρώτοι ως προς το n. Αν $(x) \in P_{\mathfrak{m},1}$, τότε αναγκαστικά $x \equiv 1 (\mathrm{mod}\, n)$ και $x > 0$. Η ακριβής ακολουθία γίνεται

$$0 \longrightarrow \{\pm 1\} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow C_\mathfrak{m} \longrightarrow 0.$$

Συνεπώς, έχουμε σε αυτήν την περίπτωση ότι η ray ομάδα κλάσεων είναι ισόμορφη με την

$$C_\mathfrak{m} \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}.$$

Έστω K μια πεπερασμένη επέκταση Galois του k. Επιπλέον υποθέτουμε ότι η K/k είναι αβελιανή, δηλαδή η $\mathrm{Gal}(K/k)$ είναι αβελιανή ομάδα. Έστω $\mathfrak{q}$ ένας πρώτος του $\mathcal{O}_K$ και $\mathfrak{p}$ ένας πρώτος του $\mathcal{O}_k$ με $\mathfrak{q} \mid \mathfrak{p}$. Υπενθυμίζουμε από την αλγεβρική θεωρία αριθμών ότι αν το $\mathfrak{p}$ είναι αδιακλάδιστο στο K, τότε υπάρχει Frobenius στοιχείο και ορίζεται καλά ως $\mathrm{Frob}_\mathfrak{p}$, που ανήκει στην $\mathrm{Gal}(K/k)$. Έστω S να είναι το σύνολο των πρώτων ιδεωδών του k που διακλαδίζονται στο K. Ορίζουμε την απεικόνιση Artin ως εξής.

$$\begin{aligned} \psi_{K/k} : I^S &\longrightarrow \mathrm{Gal}(K/k) \\ \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} &\longmapsto \prod_{i=1}^r \mathrm{Frob}_{\mathfrak{p}_i}^{e_i} \end{aligned}$$

Επιπλέον, υπενθυμίζουμε ότι έχουμε μια απεικόνιση νόρμας $\mathrm{Nm}_{K/k} : I_K \longrightarrow I_k$ που ορίζεται ως $\mathrm{Nm}_{K/k}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}|\mathfrak{p})}$, όπου $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_k$. Έχουμε την ακόλουθη πρόταση η οποία βασίζεται στις ιδιότητες του στοιχείου Frobenius και το πώς συμπεριφέρεται ως προς τις επεκτάσεις σωμάτων.

Πρόταση 2.21. *Έστω L μια αβελιανή επέκταση του k, έτσι ώστε $k \subset K \subset L$ και S ένα οποιοδήποτε πεπερασμένο σύνολο πρώτων του k που στέκονται κάτω από όλους τους πρώτους που διακλαδίζονται στο L, μαζί με όσους πρώτους του K στέκονται πάνω από τους πρώτους του k που διαλέξαμε ήδη. Έχουμε ότι το ακόλουθο διάγραμμα είναι μεταθετικό.*

$$\begin{array}{ccc} I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow{\scriptstyle \mathrm{Nm}_{K/k}} & & \downarrow \\ I_k^S & \xrightarrow{\psi_{L/k}} & \mathrm{Gal}(L/k) \end{array}$$

Πόρισμα 2.22. *Έστω L μια αβελιανή επέκταση του k. Τότε*

$$\mathrm{Nm}_{L/k}(I_L^S) \subset \ker(\psi_{L/k} : I^S \longrightarrow \mathrm{Gal}(L/k))$$

Ορισμός 2.23. *Έστω $\psi : I^S \longrightarrow G$ ένας ομομορφισμός ομάδων. Λέμε ότι ο ψ επιδέχεται έναν διαιρέτη αν υπάρχει διαιρέτης $\mathfrak{m}$ του k τέτοιος ώστε $S(\mathfrak{m}) \subset S$ και $\psi(P_{\mathfrak{m},1}) = 1$, δηλαδή ο ψ επιδέχεται διαιρέτη $\mathfrak{m}$ αν και μόνο αν παραγοντοποιείται μέσα από το $C_{\mathfrak{m}}$.*

Θεώρημα 2.24 (Νόμος Αντιστροφής)**.** *Έστω K μια πεπερασμένη αβελιανή επέκταση του k και S το σύνολο των πρώτων του k που διακλαδίζονται στο K. Η απεικόνιση Artin $\psi_{K/k}$: $I^S \longrightarrow \mathrm{Gal}(K/k)$ επιδέχεται διαιρέτη $\mathfrak{m}$ με $S(\mathfrak{m}) = S$ και επάγει ισομορφισμό*

$$I_k^S / P_{\mathfrak{m},1} \,\mathrm{Nm}_{K/k}(I_K^S) \cong \mathrm{Gal}(K/k)$$

Αξίζει να σημειωθεί ότι αυτό το θεώρημα δεν υπόσχεται την ύπαρξη μια αβελιανής επέκτασης του k. Στην ουσία, διατυπώνει ότι αν έχουμε ήδη μια αβελιανή επέκταση τότε αυτή θα είναι πηλίκο της ray ομάδας κλάσεων με μια συγκεκριμένη υποομάδα, την εικόνα της I_K^S κάτω από την απεικόνιση νόρμας.

Ορισμός 2.25. *Λέμε ότι μια υποομάδα $H \subset I_k^{S(m)}$ είναι μια congruence υποομάδα modulo $\mathfrak{m}$ αν $P_{\mathfrak{m},1} \subset H \subset I_k^{S(\mathfrak{m})}$.*

Θεώρημα 2.26. *Έστω H μια congruence υποομάδα της $I^{S(\mathfrak{m})}$. Τότε υπάρχει μοναδική αβελιανή επέκταση K/k με την μόνη πιθανή διακλάδωση να γίνεται στους πρώτους που διαιρούν το $\mathfrak{m}$ έτσι ώστε*

$$H = P_{\mathfrak{m},1} \,\mathrm{Nm}_{K/k}(I_K^{S(\mathfrak{m})})$$

και

$$I_k^{S(\mathfrak{m})} / H \cong \mathrm{Gal}(K/k)$$

μέσα από την απεικόνιση Artin.

Με άλλα λόγια, το θεώρημα μας αναφέρει ότι δοσμένης μιας H, το σώμα K που αντιστοιχεί είναι τέτοιο ώστε να ισχύουν τα ακόλουθα:

(1) Το K είναι αβελιανή επέκταση του k.

(2) Ο εκθέτης $\mathfrak{m}(\pi) = 0$ σημαίνει ότι το $\mathfrak{p}$ δεν διακλαδίζεται στο K.

(3) Τα πρώτα ιδεώδη που δεν είναι στο $S(\mathfrak{m})$ και διασπώνται στο K είναι ακριβώς αυτά που περιέχονται στην H.

Παρατηρούμε ότι αν έχουμε έναν διαιρέτη $\mathfrak{m}$ μπορούμε να θέσουμε ως $H = P_{\mathfrak{m},1}$ και να χρησιμοποιήσουμε το θεώρημα ότι υπάρχει ένα σώμα $K_{\mathfrak{m}}$ τέτοιο ώστε

$$C_{\mathfrak{m}} \cong \mathrm{Gal}(K_{\mathfrak{m}}/k)$$

Αυτό το σώμα $K_{\mathfrak{m}}$ λέγεται ray σώμα κλάσεων. Αξίζει να σημειωθεί ότι οι πρώτοι του k που διακλαδίζονται στο $K_{\mathfrak{m}}$ είναι ακριβώς οι πρώτοι που διαιρούν το $\mathfrak{m}$. Αν διαλέξουμε $\mathfrak{m} = 1$, τότε έχουμε ότι $C_{\mathfrak{m}} = C$ είναι η ομάδα κλάσεων ιδεωδών, όπως αναφέραμε πριν. Σε αυτήν την περίπτωση, το αντίστοιχο ray σώμα κλάσεων ονομάζεται *Hilbert σώμα κλάσεων*. Το Hilbert σώμα κλάσεων είναι η μέγιστη αδιακλάδιστη αβελιανή επέκταση του σώματος k. Γενικότερα, για ένα σώμα K θα συμβολίζουμε το Hilbert σώμα κλάσεων του με H_K.

Για ένα σώμα $K \subset K_{\mathfrak{m}}$, θέτουμε $\mathrm{Nm}(C_{K,\mathfrak{m}}) = P_{\mathfrak{m},1}\,\mathrm{Nm}_{K/k}(I_K^{S(\mathfrak{m})})(\mathrm{mod}\, P_{\mathfrak{m},1})$. Έχουμε το ακόλουθο πόρισμα που κατηγοριοποιεί τις αβελιανές επεκτάσεις.

Πόρισμα 2.27. *Σταθεροποιούμε έναν διαιρέτη $\mathfrak{m}$. Η απεικόνιση $K \longrightarrow \mathrm{Nm}(C_{K,\mathfrak{m}})$ είναι μια 1-1 και επί αντιστοιχία από το σύνολο των αβελιανών επεκτάσεων του k που περιέχονται στο $K_{\mathfrak{m}}$ και το σύνολο των υποομάδων της $C_{\mathfrak{m}}$. Επιπλέον, ισχύουν τα ακόλουθα:*

$$\begin{aligned} K_1 \subset K_2 &\iff \mathrm{Nm}(C_{K_1,\mathfrak{m}}) \supset \mathrm{Nm}(C_{K_2,\mathfrak{m}}) \\ \mathrm{Nm}(C_{K_1K_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{K_1,\mathfrak{m}}) \cap \mathrm{Nm}(C_{K_2,\mathfrak{m}}) \\ \mathrm{Nm}(C_{K_1\cap K_2,\mathfrak{m}}) &= \mathrm{Nm}(C_{K_1,\mathfrak{m}})\,\mathrm{Nm}(C_{K_2,\mathfrak{m}}) \end{aligned}$$

Κλείνουμε την ενότητα με μια εφαρμογή του Hilbert σώματος κλάσεων, το οποίο όπως θα δούμε έχει σημαντικό ρόλο σε όλο το υπόλοιπο της συγκεκριμένης εργασίας. Έστω K/E μια Galois επέκταση σωμάτων αριθμών. Από τα προηγούμενα έχουμε έναν ισομορφισμό ομάδων

$$C_K \cong \mathrm{Gal}(H_K/K).$$

Θα περιγράψουμε ότι αυτά τα δύο παραμένουν ισόμορφα κάτω από την δράση της $\mathrm{Gal}(K/E)$, δηλαδή είναι ισόμορφα ως $\mathrm{Gal}(K/E)$-πρότυπα. Η δράση είναι ως εξής.

$$\begin{gathered} \mathrm{Gal}(K/E) \times \mathrm{Gal}(H_K/K) \longrightarrow \mathrm{Gal}(H_K/K) \\ \tau \cdot \sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}, \end{gathered}$$

όπου επεκτείνουμε το τ σε ένα $\tilde{\tau}$ μέσα στην $\mathrm{Gal}(H_K/K)$. Έστω $\mathfrak{p}$ ένα πρώτο ιδεώδες του K. Μέσα από την απεικόνιση του Artin έχουμε ότι $\mathfrak{p} \longmapsto \mathrm{Frob}_\pi$. Συνεπώς, το $\tau\pi$ απεικονίζεται στο $\mathrm{Frob}_{\tau\mathfrak{p}} = \tilde{\tau}\,\mathrm{Frob}_{\mathfrak{p}}\,\tilde{\tau}^{-1} = \tau \cdot \mathrm{Frob}_{\mathfrak{p}}$ όπως θέλαμε.
Έχοντας τα K και E όπως προηγουμένως, υποθέτουμε ότι $H_E \cap K = E$. Αργότερα στο θεώρημα του Herbrand θα βασιστούμε στο γεγονός ότι η απεικόνιση νόρμας $C_K \longrightarrow C_E$ μεταξύ των ομάδων κλάσεων ιδεωδών είναι επιμορφισμός και το ακόλουθο διάγραμμα είναι μεταθετικό:

$$\begin{array}{ccc} C_K & \xrightarrow{\cong} & \mathrm{Gal}(H_K/K) \\ \Big\downarrow{\scriptstyle \mathrm{Norm}} & & \Big\downarrow{\scriptstyle \text{περιορισμός}} \\ C_E & \xrightarrow{\cong} & \mathrm{Gal}(H_E/E) \end{array}$$

Πράγματι, καθώς $H_E \cap K = E$ έχουμε ότι $\mathrm{Gal}(H_EK/K) \cong \mathrm{Gal}(H_E/E)$ και καθώς $H_EK \subset H_K$, παίρνουμε ότι η απεικόνιση $\mathrm{Gal}(H_K/K) \longrightarrow \mathrm{Gal}(H_E/E)$ είναι επί. Επιπλέον, το ότι το διάγραμμα είναι μεταθετικό αποδεικνύεται χρησιμοποιώντας τις ιδιότητες του στοιχείου Frobenius.

Μεγέθη των Τάξεων Ομάδων Κλάσεων

Σε αυτό το κεφάλαιο θα δώσουμε μια πληθώρα αποτελεσμάτων για τα μεγέθη των τάξεων που παίρνουν οι ομάδες κλάσεων ιδεωδών των κυκλοτομικών σωμάτων. Καθώς πολλά αποτελέσματα είναι αναλυτικής φύσεως, δεν θα δώσουμε τις αποδείξεις τους, εφόσον μας ενδιαφέρουν περισσότερο οι εφαρμογές τους. Ωστόσο, όλα αποδεικνύονται λεπτομερώς στο βιβλίο του Washington [1] στα κεφάλαια 3-6.

Ένας δεύτερος στόχος που έχει αυτό το κεφάλαιο, είναι να δώσουμε μια εισαγωγή στα εργαλεία που χρειαζόμαστε για την κύρια εικασία στο κεφάλαιο 5. Αυτά είναι οι χαρακτήρες, οι L-συναρτήσεις και οι p-αδικές L-συναρτήσεις όπου οι τελευταίες όπως θα δούμε έχουν κυρίαρχο ρόλο.

3.1 Χαρακτήρες

Ορισμός 3.1. *Ένας χαρακτήρας Dirichlet modulo m είναι ένας ομομορφισμός μεταξύ των πολλαπλασιαστικών ομάδων $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, όπου m είναι θετικός ακέραιος.*

Για έναν χαρακτήρα Dirichlet και m όπως παραπάνω, μπορούμε να πάρουμε νέους χαρακτήρες $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ για κάθε ακέραιο n με $m|n$ συνθέτοντας με την φυσιολογική απεικόνιση $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. Το ελάχιστο m έτσι ώστε το χ να είναι ομομορφισμός $(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}$ λέγεται conductor του χ και συμβολίζεται με m_χ.

Θα λέμε έναν χαρακτήρα χ πρωταρχικό αν τον ορίζουμε να έχει υπόλοιπο τον conductor του, δηλαδή

$$\chi : (\mathbb{Z}/m_\chi\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

Με την παραπάνω παρατήρηση, ξέρουμε ότι ο χ θα επάγει χαρακτήρες που θα είναι με υπόλοιπο τα πολλαπλάσια του m_χ. Και αντίστροφα, για κάθε χαρακτήρα χ υπάρχει ο αντίστοιχος πρωταχικός χαρακτήρας από τον οποίο επάγεται. Επιπλέον, θα ισχύει ότι $\chi(-1) = \pm 1$. Έτσι οι χαρακτήρες χωρίζονται στους *άρτιους* που ικανοποιούν την σχέση $\chi(-1) = 1$ και αντίστοιχα στους *περιττούς* με $\chi(-1) = -1$.

Έστω χ, ψ δύο χαρακτήρες με conductors m_χ και m_ψ αντίστοιχα. Για να οριστεί το γινόμενό τους ορίζεται πρώτα ο ομομορφισμός

$$\phi : (\mathbb{Z}/\,\varepsilon\kappa\pi(m_\chi, m_\psi)\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

ως

$$\phi(n) = \chi(n)\psi(n).$$

Καθώς ο χαρακτήρας ϕ δεν θα είναι απαραίτητα πρωταχρικός, ορίζουμε ως γινόμενο $\chi\psi$ τον πρωταρχικό χαρακτήρα που αντιστοιχεί στον ϕ. Επιπλέον, ορίζουμε ως κύριο χαρακτήρα χ_0 αυτόν που απεικονίζει κάθε κλάση στο 1. Μαζί με αυτό, για κάθε χ ορίζουμε τον αντίστροφο του $\overline{\chi}$, όπου $\overline{\chi}(a) = \chi(a)^{-1} = \overline{\chi(a)}$ με το τελευταίο να είναι ο μιγαδικός συζυγής. Με όλα τα προηγούμενα, οι χαρακτήρες Dirichlet αποτελούν πολλαπλασιαστική ομάδα.

Χρησιμοποιώντας τον ισομορφισμό

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

μπορούμε να θεωρήσουμε τους χαρακτήρες Dirichlet ως χαρακτήρες ομάδων Galois. Ο ισομορφισμός αυτός είναι ο $\sigma \longmapsto a_\sigma$, όπου a_σ είναι τέτοιο ώστε $\sigma(\zeta_n) = \zeta_n^{a_\sigma}$. Έστω χ ένας χαρακτήρας με conductor n και πεδίο ορισμού το $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Ο πυρήνας του χ είναι υποομάδα της $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ και άρα το σταθερό σώμα του $\ker\chi$ είναι υπόσωμα του $\mathbb{Q}(\zeta_n)$. Θα αναφερόμαστε σε αυτό ως το σταθερό σώμα του χ και το συμβολίζουμε με $\mathbb{Q}^\chi$.

Γενικότερα, έχοντας ως X μια πεπερασμένη ομάδα χαρακτήρων Dirichlet και n το ελάχιστο κοινό πολλαπλάσιο των conductor των χαρακτήρων στο X, τότε το X θα είναι μια υποομάδα της ομάδας των χαρακτήρων του $\mathbb{Q}(\zeta_n)$. Θέτουμε ως $\mathcal{K}$ την τομή των πυρήνων όλων των χαρακτήρων που βρίσκονται στο X και $\mathbb{Q}^X$ το σταθερό σώμα του $\mathcal{K}$. Το $\mathbb{Q}^X$ θα λέγεται το σώμα που αντιστοιχεί στην ομάδα χαρακτήρων X.

Ακολουθούν κάποια βασικά αποτελέσματα για τις ομάδες χαρακτήρων, τα οποία μπορούμε να τα δούμε γενικότερα στο πλαίσιο των πεπερασμένων αβελιανών ομάδων. Έστω G μια πεπερασμένη αβελιανή ομάδα, θα συμβολίζουμε με $G^\wedge$ την ομάδα των πολλαπλασιαστικών χαρακτήρων της G. Σαν G θα εννούμε μια τυχαία πεπερασμένη αβελιανή ομάδα μέχρις ότου να αναφερθεί διαφορετικά.

Λήμμα 3.2. *$G \cong G^\wedge$ (όχι με φυσιολογικό τρόπο).*

Απόδειξη. Η G γράφεται ως ευθύ άθροισμα κυκλικών ομάδων της μορφής $\mathbb{Z}/m\mathbb{Z}$. Συνεπώς, η $G^\wedge$ γράφεται ως ευθύ γινόμενο ομάδων της μορφής $(\mathbb{Z}/m\mathbb{Z})^\wedge$. Για ένα $\chi \in (\mathbb{Z}/m\mathbb{Z})^\wedge$, εφόσον η δομή εδώ είναι προσθετική και το 1 είναι γεννήτορας, το $\chi(1)$ θα είναι οποιαδήποτε m-οστή ρίζα της μονάδας. Συνεπώς, ισχύει το λήμμα για την $\mathbb{Z}/m\mathbb{Z}$ και άρα για την G. □

Θεώρημα 3.3. *$G \cong G^{\wedge\wedge}$ (με φυσιολογικό τρόπο).*

Απόδειξη. Ορίζουμε:

$$G \longrightarrow G^{\wedge\wedge}$$

$$g \longmapsto (\chi \mapsto \chi(g))$$

και έχοντας από το προηγούμενο λήμμα ότι $|G| = |G^\wedge| = |G^{\wedge\wedge}|$, αρκεί να δείξουμε ότι η απεικόνιση είναι μονομορφισμός. Έστω $g \in G$ τέτοιο ώστε $\chi(g) = 1$ για κάθε $\chi \in G^\wedge$. Θέτουμε ως $H = \langle g \rangle$ και τότε οι χαρακτήρες της G αντιστοιχούν στους χαρακτήρες της G/H, αφού έχουν τετριμμένη δράση στο H. Αυτοί είναι $|G/H| = |G|$ το πλήθος, δηλαδή $g = 1$. □

Είναι βοηθητικό να ταυτίζουμε τις $G, G^{\wedge\wedge}$ και έτσι έχουμε την απεικόνιση:

$$G \times G^\wedge \longrightarrow \mathbb{C}^\times$$

$$(g, \chi) \longmapsto \chi(g),$$

η οποία είναι non-degenerate, δηλαδή αν $\chi(g) = 1$ για κάθε $\chi \in G^\wedge$ τότε $g = 1$ και αντίστοιχα, αν $\chi(g) = 1$ για κάθε $g \in G$, τότε φυσικά $\chi = 1$. Έστω H υποομάδα της G. Θέτουμε:

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

Λήμμα 3.4. *Για G πεπερασμένη αβελιανή ομάδα και H υποομάδα της ισχύουν τα εξής:*

(1) $H^\perp \cong (G/H)^\wedge$.

(2) $H^\wedge \cong G^\wedge / H^\perp$.

(3) $H = (H^\perp)^\perp$ *(Ταυτίζοντας $G^{\wedge\wedge} = G$).*

Απόδειξη. Για το (1) έχουμε τον φυσιολογικό ισομορφισμό όπου ένα $\chi \in G^\wedge$ που δρα τετριμμένα σε όλο το H θα αντιστοιχεί σε έναν χαρακτήρα $\bar{\chi} \in (G/H)^\wedge$ με $\bar{\chi}(gH) = \chi(g)$. Για το (2) έχουμε τον περιορισμό $G^\wedge \to H^\wedge$ με $\chi \mapsto \chi|_H$ και πυρήνα $H^\perp$. Για το επί ισχύει ότι $|H^\perp| = |(G/H)^\wedge| = |G/H| = |G|/|H|$ και άρα $|H^\wedge| = |H| = |G|/|H^\perp| = |G^\wedge|/|H^\perp|$. Για το (3) με όμοιο υπολογισμό δείχνουμε ότι οι τάξεις είναι ίσες και έχουμε ότι:

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

από όπου φαίνεται ξεκάθαρα ότι $H \subseteq (H^\perp)^\perp$. □

Θα θέλαμε να ενισχύσουμε την αντιστοιχία Galois για πεπερασμένες επεκτάσεις, ώστε να αντιστοιχούν τα υποσώματα σε υποομάδες χαρακτήρων. Αρχικά, δείχνουμε ότι το $\mathbb{Q}(\zeta_n)$ αντιστοιχεί σε συγκεκριμένη ομάδα χαρακτήρων Dirichlet.

Πρόταση 3.5. *Το $\mathbb{Q}(\zeta_n)$ είναι το σώμα που αντιστοιχεί στην ομάδα χαρακτήρων $X = \{\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \mathbb{C}^\times\}$.*

Απόδειξη. Είναι ξεκάθαρο ότι το σώμα που αντιστοιχεί στο X θα είναι υπόσωμα του $\mathbb{Q}(\zeta_n)$, από τον ορισμό του. Αρκεί να δείξουμε ότι το $\mathcal{K}$, δηλαδή η τομή όλων των πυρήνων των χαρακτήρων του X είναι τετριμμένη. Έστω $g \in \mathcal{K}$, δηλαδή $\chi(g) = 1$ για κάθε $\chi \in X$. Για $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n))$ και $X = G^\wedge$, μιμούμενοι την απόδειξη του θεωρήματος 3.3 παίρνουμε ότι $g = 1$. □

Στην συνέχεια το X θα είναι η ομάδα χαρακτήρων που αντιστοιχεί στο $\mathbb{Q}(\zeta_n)$. Έχουμε δηλαδή την nondegenerate απεικόνιση:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \times X \longrightarrow \mathbb{C}^\times$$

Έστω $K/\mathbb{Q}$ μια πεπερασμένη αβελιανή επέκταση. Από το θεώρημα Kronecker-Weber έχουμε ότι υπάρχει n τέτοιο ώστε $K \subset \mathbb{Q}(\zeta_n)$. Θέτουμε:

$$Y = \{\chi \in X : \ \chi(\sigma) = 1 \ \forall \ \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)\}$$

και παρατηρούμε ότι

$$\begin{aligned} Y &= \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)^\perp \\ &\cong (\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K))^\wedge \\ &= \mathrm{Gal}(K/\mathbb{Q})^\wedge \end{aligned}$$

Άρα ξεκινώντας με ένα σώμα K έχουμε συσχετίσει μια ομάδα χαρακτήρων Dirichlet Y. Έστω τώρα ότι έχουμε Y μια υποομάδα του X. Θέτουμε ως K να είναι το σταθερό σώμα του

$$Y^\perp = \{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \ \chi(\sigma) = 1 \ \forall \ \chi \in Y\}$$

Όπου έχουμε κάνει την ταύτιση $G = G^{\wedge\wedge}$. Αυτό είναι στην ουσία το $\mathcal{K}$ που αναφέραμε πριν. Εφόσον έχουμε θέσει $K := \mathbb{Q}(\zeta_n)^{Y^\perp}$ η θεωρία Galois μας λέει ότι $Y^\perp = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$. Έτσι έχουμε ότι

$$\begin{aligned} Y &= (Y^\perp)^\perp \\ &= \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})^\perp \\ &\cong \mathrm{Gal}(K/\mathbb{Q})^\wedge \end{aligned}$$

Άρα έχουμε κατασκευάσει μια 1-1 και επί αντιστοιχία:

$$\begin{aligned} \{\Upsilon\text{ποομάδες του } X\} &\longleftrightarrow \{\ \Upsilon\text{ποσώματα του } \mathbb{Q}(\zeta_n)\} \\ \mathrm{Gal}(K/\mathbb{Q})^\wedge &\longleftrightarrow K \\ Y &\longleftrightarrow \mathbb{Q}(\zeta_n)^{Y^\perp} \end{aligned}$$

Δηλαδή, σχηματικά έχουμε ενισχύσει την αντιστοιχία Galois ως εξής:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & 1 & X = G^\wedge \\ | & | & | \\ K & H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K) & H^\perp \cong (G/H)^\wedge \\ | & | & | \\ \mathbb{Q} & G & \{\chi_0\} = G^\perp \end{array}$$

Αυτή η αντιστοιχία θα εννοείται όταν αναφερόμαστε στο σώμα που ανήκει σε μια ομάδα χαρακτήρων. Θα εισάγουμε τώρα τον χαρακτήρα Teichmüller. Υποθέτουμε ότι p είναι ένας περιττός πρώτος, ωστόσο μπορούν τα ίδια αποτελέσματα να γίνουν στην περίπτωση που $p = 2$, αλλά θα χρειαζόταν να επιβαρύνουμε επιπλέον τον συμβολισμό. Χρειαζόμαστε το γνωστό λήμμα του Hensel για τους p-αδικούς ακέραιους και ένα πόρισμα του. Την απόδειξη του λήμματος μπορεί να την βρει κανείς στο [9].

Λήμμα 3.6 (Hensel's lemma)**.** *Έστω $f(x) \in \mathbb{Z}_p[x]$ και $a \in \mathbb{Z}_p$ που ικανοποιεί:*

$$f(a) \equiv 0 \mod p,\ f'(a) \not\equiv 0 \mod p$$

τότε υπάρχει μοναδικό $b \in \mathbb{Z}_p$ τέτοιο ώστε $f(b) = 0$ στο $\mathbb{Z}_p$ και $a \equiv b \mod p$.

Πόρισμα 3.7. *Υπάρχουν ακριβώς $p-1$ διακεκριμένες $(p-1)$-οστές ρίζες της μονάδας στο $\mathbb{Z}_p$. Επιπλέον αυτές παραμένουν διακεκριμένες modulo p.*

Απόδειξη. Έστω $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x] \subseteq \mathbb{Q}_p[x]$. Το $f(x)$ μπορεί να έχει το πολύ $p-1$ ρίζες στο $\mathbb{Q}_p$. Έστω $a \in \mathbb{Z}_p$, $a \neq 0$. Έχουμε ότι $f(a) = 0 (\mathrm{mod}\, p)$ και $f'(a) \neq 0 (\mathrm{mod}\, p)$. Από το λήμμα του Hensel υπάρχει μοναδική ρίζα του $f(x)$ στο $\mathbb{Z}_p$ που είναι ισοδύναμη στο a modulo p. □

Συνεπώς, για κάθε μη μηδενικό $a \in \mathbb{Z}_p$ αντιστοιχεί μια καλά ορισμένη ρίζα της μονάδας στο $\mathbb{Z}_p$. Έτσι, ορίζεται ο χακακτήρας Teichmüller να είναι το $\omega : \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$ όπου ως $\omega(a)$ θα είναι η ρίζα της μονάδας που αντιστοιχεί στο a. Στην παραπάνω κατασκευή κάθε $a \in \mathbb{Z}_p$ απεικονίζεται στο $\bar{a} \in \mathbb{F}_p$ και με το λήμμα του Hensel αυτό γίνεται lift στο $\mathbb{Z}_p$. Δηλαδή, εφόσον πετυχαίνουμε τις ρίζες τις μονάδας στο πεδίο τιμών, μπορούμε να βλέπουμε το ω σαν p-αδικό χαρακτήρα Dirichlet με conductor p:

$$\omega : \mathbb{F}_p \longrightarrow \mathbb{Z}_p^\times.$$

Θα μπορούσαμε να το βλέπουμε και σαν μιγαδικό χαρακτήρα Dirichlet, αλλά αυτή η γραφή θα είναι πιο χρήσιμη στη συνέχεια.

Πρόταση 3.8. *Έστω $Y = \{1, \omega^2, \omega^4, \ldots, \omega^{p-3}\}$. Το σώμα που αντιστοιχεί στο Y είναι το $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.*

Απόδειξη. Το $X = \{1, \omega, \omega^2, \ldots, \omega^{p-2}\}$ είναι η ομάδα χαρακτήρων που αντιστοιχεί στο $\mathbb{Q}(\zeta_p)$, εφόσον αυτοί οι χαρακτήρες είναι $p-1$ το πλήθος και διακεκριμένοι. Άρα αποτελούν όλο το $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})^\wedge$. Επιπλέον, έχουμε ότι $|Y^\perp| = |X|/|Y| = 2$. Καθώς $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p)^+] = 2$ και η ομάδα $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ είναι κυκλική, δηλαδή έχει μοναδική υποομάδα τάξης 2, παίρνουμε ότι το $\mathbb{Q}(\zeta_p)^+$ είναι το σταθερό σώμα της $Y^\perp$. □

3.2 L-συναρτήσεις

Σε αυτό το σημείο θα αναφέρουμε κάποια βασικά αποτελέσματα για τις L-συναρτήσεις που συνδέονται με τους χαρακτήρες. Αυτά χρειάζονται ώστε αργότερα να είναι ξεκάθαρες οι αναλογίες όταν θα κοιτάμε τοπικά στις p-αδικές L-συναρτήσεις. Όπως αναφέραμε πιο πριν, οι αποδείξεις τους είναι αναλυτικής φύσεως και για αυτές μπορεί κάποιος να ανατρέξει στο [1]. Γενικά, για ένα αντικείμενο A αριθμο-θεωρητικού ενδιαφέροντος υπάρχει μια L-συνάρτηση που του αντιστοιχεί, δηλαδή ένα αντικείμενο το οποίο επεξεργαζόμαστε με εργαλεία της μιγαδική ανάλυσης. Με βάση αυτά, οι τιμές που παίρνει η L-συνάρτηση επιστρέφουν πίσω πληροφορία για το αντικείμενο A. Έτσι, με το σύνηθες Hasse principle κοιτάμε αυτές τις τιμές τοπικά στις ανάλογες $\mathcal{L}_p$ που είναι οι p-αδικές εκδόσεις των L-συναρτήσεων. Το αντικείμενο εδώ για το οποίο μας ενδιαφέρει να πάρουμε πληροφορίες είναι ο αριθμός κλάσεων h_n του σώματος αριθμών $\mathbb{Q}(\zeta_n)$.

Υπενθυμίζουμε ότι αν έχουμε έναν χαρακτήρα Dirichlet με conductor k

$$\chi' : (\mathbb{Z}/k\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

μπορούμε να τον βλέπουμε ως αριθμητική συνάρτηση

$$\chi : \mathbb{Z} \longrightarrow \mathbb{C}$$
$$\chi(n) = \chi'([n]_k)$$

που πληρεί τις ιδιότητες:

(1) $\chi(mn) = \chi(m)\chi(n)$ για κάθε $m, n \in \mathbb{Z}$.

(2) $|\chi(n)| = \begin{cases} 1, & \text{αν } (n,k) = 1 \\ 0, & \text{αλλιώς} \end{cases}$.

(3) $\chi(n + km) = \chi(n)$ για κάθε $n, m \in \mathbb{Z}$.

(4) $\chi^{\phi(k)}(n) = 1$ για $(n,k) = 1$

Ορισμός 3.9. *Έστω χ ένας χαρακτήρας Dirichlet με conductor k που επεκτείνεται στο $\mathbb{Z}$ όπως παραπάνω. Η L-συνάρτηση που αντιστοιχεί στο χ είναι η εξής*

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}, \quad \mathrm{Re}(s) > 1.$$

Είναι γνωστό ότι η $L(s, \chi)$ δέχεται αναλυτική συνέχιση σε όλο το $\mathbb{C}$ αν $\chi \neq 1$. Για $\chi = 1$ ειναι η γνωστή συνάρτηση ζήτα του Riemann, που έχει μερόμορφη συνέχιση σε όλο το $\mathbb{C}$, εκτός από έναν απλό πόλο με ολοκληρωτικό υπόλοιπο 1 στο $s = 1$. Η L-συνάρτηση $L(s, \chi)$ έχει γινόμενο Euler που συγκλίνει:

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

Υπενθυμίζουμε ότι οι αριθμοί Bernoulli B_m ορίζονται ως:

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}$$

και όμοια ορίζονται οι γενικευμένοι αριθμοί Bernoulli $B_{m,\chi}$ για έναν χαρακτήρα με conductor n:

$$\sum_{j=1}^{n} \frac{\chi(j) t e^{jt}}{e^{nt} - 1} = \sum_{m=0}^{\infty} B_{m,\chi} \frac{t^m}{m!}$$

Οι γενικευμένοι αριθμοί Bernoulli έχουν σημαντικό ρόλο καθώς σχετίζονται με ειδικές τιμές που παίρνουν οι L-συναρτήσεις. Πιο συγκεκριμένα, ισχύει το ακόλουθο θεώρημα:

Θεώρημα 3.10 (Θεώρημα 4.2 στο [1])**.** *Για $m \geq 1$ έχουμε*

$$L(1 - m, \chi) = -\frac{B_{m,\chi}}{m}.$$

Έστω K ένα αβελιανό σώμα αριθμών και X η ομάδα χαρακτήρων που του αντιστοιχεί. Έχουμε ότι υπάρχουν $r_1 + 2r_2$ εμφυτεύσεις του K στο $\mathbb{C}$, όπου r_1 είναι το πλήθος των πραγματικών εμφυτεύσεων και r_2 είναι το πλήθος των ζευγαριών των συζυγών μιγαδικών εμφυτεύσεων. Επιπλέον, έχουμε R_K να είναι το regulator του K, ω_K ο αριθμός των ριζών της μονάδας που περιέχει το K, D_K η διακρίνουσα του K και h_K ο αριθμός κλάσεων του K. Οι ακριβείς ορισμοί των παραπάνω μεγεθών υπάρχουν στο [14].

Με τα παραπάνω, είμαστε σε θέση να γράψουμε τον τύπο του Dirichlet για τους αριθμούς κλάσεων. Όπως είναι ξεκάθαρο, ο τύπος αυτός ακολουθεί την φιλοσοφία των L-συναρτήσεων που αναφέραμε προηγουμένως.

Θεώρημα 3.11 (Dirichlet's Class Number Formula)**.** *Έστω K ένα αβελιανό σώμα αριθμών και X η ομάδα χαρακτήρων που του αντιστοιχεί. Για τα μεγέθη όπως παραπάνω έχουμε ότι*

$$\prod_{\substack{\chi\in X\\ \chi\neq 1}} L(1,\chi) = \frac{2^{r_1}(2\pi)^{r_2}R_K}{\omega_K\sqrt{|D_K|}}\cdot h_K.$$

Με αυτό το θεώρημα έχουμε μια θεωρητική μέθοδο για να υπολογίζουμε τον αριθμό κλάσεων ενός αβελιανού σώματος αριθμών, ωστόσο χρειάζεται να γίνει υπολογισμός του regulator. Εκείνος απαιτεί την εύρεση μιας βάσης της $\mathcal{O}_K^\times$. Συνήθως, η εύρεση μιας τέτοιας βάσης απαιτεί πολλούς υπολογισμούς για να είναι πρακτική η μέθοδος. Για αυτό, θα χωρίσουμε τον αριθμό κλάσεων σε δύο παράγοντές του και θα δουλέψουμε με τον έναν εκ των οποίων είναι ευκολότερο.

Θα αναφέρουμε το επόμενο θεώρημα εστιάζοντας στο $K=\mathbb{Q}(\zeta_n)$, ωστόσο ισχύει το γενικότερο όχι μόνο για τα αβελιανά σώματα αριθμών, αλλά και για τα λεγόμενα CM-σώματα (complex multiplication). Ένα σώμα λέγεται *πλήρως πραγματικό* αν όλες του οι εμφυτεύσεις στο $\mathbb{C}$ βρίσκονται μέσα στο $\mathbb{R}$, ενώ αντίθετα *πλήρως φανταστικό* αν καμία τέτοια εμφύτευση δεν βρίσκεται ολόκληρη μέσα στο $\mathbb{R}$. Ένα CM-σώμα είναι μια πλήρως φανταστική τετραγωνική επέκταση ενός πλήρως πραγματικού σώματος. Μπορούμε να πάρουμε ένα τέτοιο σώμα K ξεκινώντας από ένα πλήρως πραγματικό F και επισυνάπτοντας μια ρίζα $\sqrt{a}$, για κάποιο στοιχείο $a\in F\subseteq\mathbb{R}$ όπου το $Irr(a,\mathbb{Q})$ να έχει μόνο μιγαδικές ρίζες. Ισοδύναμα, για κάθε εμφύτευση σ του F στους πραγματικούς να ισχύει ότι $\sigma(a)<0$. Όλα τα σώματα $\mathbb{Q}(\zeta_n)$ είναι CM-σώματα, αφού έχουν ως μέγιστο πραγματικό υπόσωμα το $\mathbb{Q}(\zeta_n+\zeta_n^{-1})=\mathbb{Q}(\cos 2\pi/n)$ και παίρνουμε το $\mathbb{Q}(\zeta_n)$ επισυνάπτοντας την ρίζα του $\zeta_n^2+\zeta_n^{-2}-2$, η οποία είναι η διακρίνουσα του αναγώγου πολυωνύμου $x^2-(\zeta_n+\zeta_n^{-1})x+1$ με μιγαδικές ρίζες $\zeta_n,-\zeta_n$. Αν h_n είναι ο αριθμός κλάσεων του $\mathbb{Q}(\zeta_n)$ και h_n^+ είναι ο αριθμός κλάσεων του $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$, τότε έχουμε το ακόλουθο θεώρημα:

Θεώρημα 3.12. *Για κάθε θετικό ακέραιο n ισχύει ότι $h_n^+|h_n$.*

Για την απόδειξη του θεωρήματος χρειάζεται η ακόλουθη πρόταση που βασίζεται στην θεωρία κλάσεων σωμάτων.

Πρόταση 3.13. *Έστω K/E μια επέκταση σωμάτων αριθμών που δεν έχει μη τετριμμένη ενδιάμεση αδιακλάδωτη αβελιανή επέκταση F/E. Τότε $h_E|h_K$.*

Υπενθυμίζουμε ότι μια επέκταση F/E είναι αδιακλάδωτη αν κάθε επέκταση πραγματικής εμφύτευσης του E σε εμφύτευση του F παραμένει πραγματική και κάθε πρώτο ιδεώδες του $\mathcal{O}_E$ παραμένει αδιακλάδωτο στο $\mathcal{O}_F$.

Απόδειξη. Από την θεωρία κλάσεων σωμάτων, υπάρχει το σώμα κλάσεων Hilbert H_E του E που είναι η μέγιστη αδιακλάδωτη αβελιανή επέκταση του E τέτοιο ώστε

$$C_E\cong \mathrm{Gal}(H_E/E),$$

όπου C_E είναι η ομάδα κλάσεων του E. Η υπόθεση μας λέει ότι $K\cap H_E=E$ και άρα

$$h_E=[H_E:E]=[H_EK:K],$$

όπου χρησιμοποιούμε ότι $\mathrm{Gal}(H_EK/K)\cong\mathrm{Gal}(H_E/H_E\cap K)=\mathrm{Gal}(H_E/E)$. Αυτός ο ισομορφισμός μας λέει ότι και η H_EK/K είναι αβελιανή. Επιπλέον, εφόσον η H_E/E είναι αδιακλάδωτη θα παραμένει αδιακλάδωτη και η μεταφορά H_EK/K. Πράγματι, αν θεωρήσουμε έναν πρώτο q του HK που βρίσκεται πάνω από έναν πρώτο p του K τότε

$$e=e(q\mid p)=|I_q|=\#\{\sigma\in\mathrm{Gal}(H_EK/K):\ \sigma(a)\equiv a \mod q\}$$

και έχουμε ότι το $q \cap H_E$ είναι πρώτος πάνω από τον πρώτο $p \cap H_E$ στην αδιακλάδιστη επέκταση H_E/E, δηλαδή

$$1 = |I_{q\cap H_E}| = \#\{\sigma \in \mathrm{Gal}(H_E/E) : \ \sigma(a) \equiv a \mod q \cap H\}$$

Άρα ξεκινώντας με ένα $\sigma \in I_q$ ο ισομορφισμός μας δίνει:

$$\sigma(a) \equiv a \mod q \ \forall a \in \mathcal{O}_{H_E K}$$

$$\sigma|_{H_E}(a) \equiv a \ \forall a \in \mathcal{O}_{H_E}$$

$$\sigma|_{H_E} = 1 \implies \sigma = 1$$

οπότε $e = 1$, δηλαδή το q θα παραμείνει αδιακλάδιστο. Όμοια, για έναν αρχιμήδειο πρώτο w του $H_E K$ πάνω από το v του K θα έχουμε ότι

$$I_w = \{\sigma \in \mathrm{Gal}(H_E K/K) : \ w \circ \sigma = w\}$$

$$I_{w|_{H_E}} = \{\sigma \in \mathrm{Gal}(H_E/K) : \ w|_{H_E} \circ \sigma = w|_{H_E}\}$$

και $|I_w| = |I_{w|_{H_E}}| = 1$.

Άρα η αδιακλάδιστη επέκταση $H_E K/K$ θα στέκεται μέσα στην μέγιστη αδιακλάδιστη επέκταση H_K/K. Συνεπώς,

$$h_K = [H_K : K] = [H_K : H_E K][H_E K : E] = [H_K : H_E K] \cdot h_E$$

δηλαδή

$$h_E | h_K$$

□

Απόδειξη. (του Θεωρήματος)

Η επέκταση $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ έχει βαθμό 2 και άρα δεν υπάρχει ενδιάμεση επέκταση. Επιπλέον, αυτή διακλαδίζεται στον πραγματικό πρώτο, αφού το $\mathbb{Q}(\zeta_n)$ είναι CM-σώμα και το $\mathbb{Q}(\zeta_n + \zeta_\nu^{-1})$ είναι πλήρως πραγματικό. Άρα ικανοποιούνται οι προϋποθέσεις της προηγούμενης πρότασης. □

Ορισμός 3.14. *Ορίζουμε τον σχετικό αριθμό κλάσεων του $\mathbb{Q}(\zeta_n)$ να είναι $h_n^- := h_n/h_n^+$.*

Με εργαλεία της ανάλυσης και χρησιμοποιώντας τον τύπο του Dirichlet για τους αριθμούς κλάσεων δείχνεται ότι

$$h_n^- = 2^a 2n \prod_{\substack{\chi \in X \\ \chi(-1) = -1}} \left(-\frac{1}{2} B_{1,\chi}\right)$$

όπου το X είναι η ομάδα χαρακτήρων που αντιστοιχεί στο $\mathbb{Q}(\zeta_n)$ και το a είναι 0 αν το n είναι πρώτος ή 1 διαφορετικά. Ειδικότερα, για p πρώτο έχουμε

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ περιττός}}} \left(-\frac{1}{2} B_{1,\omega^j}\right) \tag{3.1}$$

και αυτός ο τύπος θα χρησιμοποιηθεί για να αποδειχτεί το ότι $p | h_p^-$ αν και μόνο αν $p | B_j$ για κάποιο $j = 2, 4, \ldots, p-3$.

3.3 P-adic L-συναρτήσεις

Σε αυτήν την ενότητα θα διατυπώσουμε την θεωρία γύρω από τις p-αδικές εκδόσεις των Dirichlet L-συναρτήσεων. Στον ορισμό των L-συναρτήσεων που υπάρχει το $1/n^s$, ξέρουμε ότι αυτό θα παίρνει αυθαίρετα μεγάλες τιμές στην p-αδική νόρμα, καθώς όταν το n θα τείνει στο άπειρο θα το διαιρούν μεγάλες δυνάμεις του p. Άρα οι p-αδικές L-συναρτήσεις δεν μπορούν εδώ να οριστούν με τον ίδιο τρόπο, καθώς οι σειρές τους θα αποκλείνουν στο $\mathbb{Q}_p$. Ωστόσο, οι τιμές της $L(s,\chi)$ στους αρνητικούς ακέραιους είναι αλγεβρικές και άρα μπορούμε να θεωρήσουμε ότι βρίσκονται σε κάποια επέκταση του $\mathbb{Q}_p$. Συνεπώς, ψάχνουμε κάποια p-αδική συνάρτηση που να συμφωνεί με την $L(s,\chi)$ στους αρνητικούς ακεραίους.

Με τις συναρτήσεις που θα κατασκευάσουμε θα δείξουμε ισοτιμίες μεταξύ των γενικευμένων αριθμών Bernoulli, από όπου θα καταλήξουμε στο κριτήριο του Kummer για το irregularity των πρώτων. Αρχικά, θα κοιτάξουμε τις p-αδικές L-συναρτήσεις στο $s=1$ και θα βρούμε έναν τύπο όμοιο με την κλασική περίπτωση. Αυτό με την σειρά του θα μας δώσει μια p-αδική έκδοση του τύπου Dirichlet για αριθμούς κλάσεων, από το οποίο θα πάρουμε το αποτέλεσμα του Kummer: $p|h_p^+ \implies p|h_p^-$.

Χρειαζόμαστε βασικά αποτελέσματα της ανάλυσης στους p-αδικούς αριθμούς, ξεκινώντας από το $\mathbb{Q}_p$. Καθώς θα χρειαστούμε όπως αναφέραμε αλγεβρικές επεκτάσεις του $\mathbb{Q}_p$ που παράγονται από τιμές των χαρακτήρων Dirichlet. Επομένως, επεκτείνουμε στην αλγεβρική θήκη $\overline{\mathbb{Q}}_p$ του $\mathbb{Q}_p$. Η κατασκευή της γίνεται παίρνοντας την ένωση όλων των πεπερασμένων επεκτάσεων $K/\mathbb{Q}_p$, όπου σε κάθε τέτοια επέκταση η p-αδική νόρμα επεκτείνεται μοναδικά σε μια μη-αδχιμηδιανή απόλυτη τιμή στο K ως εξής.

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$$
$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

όπου $n=[K:\mathbb{Q}_p]$, όπως αποδεικνύεται στο [9]. Επιπλέον, δείχνεται ότι η τιμή του $|x|$ για $x \in K/\mathbb{Q}_p$ δεν επηρεάζεται από τα μεγαλύτερα σώματα που περιέχουν το K. Άρα κοιτώντας σε ένα $x \in \overline{\mathbb{Q}}_p$, έχουμε την πεπερασμένη επέκταση $\mathbb{Q}_p(x)$ και την μοναδική επέκταση της p-αδικής απόλυτης τιμής σε αυτό το σώμα. Έτσι, επεκτείνεται μοναδικά η p-αδική απόλυτη τιμή σε

$$|\cdot| : \overline{\mathbb{Q}}_p \longrightarrow \mathbb{R}_{\geq 0}$$

Πρόταση 3.15. *Το $\overline{\mathbb{Q}}_p$ δεν είναι πλήρες.*

Απόδειξη. Έστω

$$a = \sum_{n=1}^{\infty} \zeta_{n'} p^n$$

όπου $n'=n$ αν $\gcd(n,p)=1$ και $n'=1$ διαφορετικά. Η ακολουθία των μερικών αθροισμάτων της παραπάνω σειράς τείνει στο 0 ως προς την p-αδική νόρμα, άρα έχουμε ότι η σειρά συγκλίνει και ως επακόλουθο αν το $\overline{\mathbb{Q}}_p$ ήταν πλήρες θα ίσχυε ότι $a \in \overline{\mathbb{Q}}_p$. Οπότε, το a θα άνηκε σε μια πεπερασμένη επέκταση K του $\mathbb{Q}_p$. Υποθέτουμε ότι $\zeta_{n'} \in K$ για όλα τα $n<m$ για κάποιο m. Επιπλέον, υποθέτουμε ότι $p \nmid m$. Τότε

$$b = p^{-m}\left(a - \sum_{n=0}^{m-1} \zeta_{n'} p^n\right) \in K$$

και $b \equiv \zeta_m (\mathrm{mod}\, p)$. Συνεπώς η εξίσωση $X^m - 1 \equiv 0 (\mathrm{mod}\, p)$ έχει ρίζα στο K. Από την γενικότερη έκδοση του λήμματος του Hensel που βρίσκεται στο [11], το K περιέχει ρίζα του πολυωνύμου X^m-1 η οποία είναι ισοϋπόλοιπη με το $b (\mathrm{mod}\, p)$, άρα και με το $\zeta_m (\mathrm{mod}\, p)$. Καθώς οι m-οστές ρίζες της μονάδας είναι διακεκριμένες modulo p, εφόσον ισχύει ότι

$$m = \prod_{\substack{\zeta^m=1 \\ \zeta \neq 1}} (1-\zeta)$$

παίρνουμε ότι $\zeta_m \in K$. Από επαγωγή, έχουμε ότι $\zeta_m \in K$ για κάθε m με $p \nmid m$. Όπως παραπάνω, οι ρίζες της μονάδας τάξης σχετικά πρώτης ως προς το p είναι διακεκριμένες modulo p, άρα ο δακτύλιος των ακεραίων του K περιέχει άπειρες τέτοιες. Φυσικά, αυτό είναι άτοπο καθώς η επέκταση $K/\mathbb{Q}_p$ είναι πεπερασμένη. Άρα το $\overline{\mathbb{Q}}_p$ δεν είναι πλήρες. □

Για τα εργαλεία της ανάλυσης, είναι πιο βολικό να εργαζόμαστε σε πλήρες σώμα. Θέτουμε $\mathbb{C}_p$ να είναι η πλήρωση του $\overline{\mathbb{Q}}_p$ ως προς την p-αδική απόλυτη τιμή. Αυτή με την σειρά της επεκτείνεται φυσιολογικά στο $\mathbb{C}_p$ ως

$$|\cdot| : \mathbb{C}_p \longrightarrow \mathbb{R}_{\geq 0}$$
$$|z| = \lim_{n\to\infty} |x_n|$$

για (x_n) οποιαδήποτε ακολουθία στο $\overline{\mathbb{Q}}_p$ που τείνει στο x, εφόσον από κατασκευή το $\overline{\mathbb{Q}}_p$ είναι πυκνό στο $\mathbb{C}_p$. Ξεκινήσαμε από ένα πλήρες σώμα το $\mathbb{Q}_p$, το οποίο δεν είναι αλγεβρικά κλειστό. Για να δείξουμε ότι δεν συνεχίζεται άλλο αυτή η διαδικασία, δηλαδή ότι το $\mathbb{C}_p$ είναι αλγεβρικά κλειστό, χρειαζόμαστε το ακόλουθο λήμμα:

Λήμμα 3.16 (Krasner)**.** *Έστω K ένα πλήρες σώμα ως προς μια μη-αρχημηδιανή εκτίμηση. Έστω $a, b \in \overline{K}$, η αλγεβρική θήκη του K, με a διαχωρίσιμο πάνω από το $K(b)$. Επιπλέον, υποθέτουμε ότι για κάθε $a_i \neq a$ συζυγή με το a έχουμε:*

$$|b - a| < |a_i - a|$$

Τότε $K(a) \subseteq K(b)$ (εδώ $|x|$ είναι η μοναδική επέκταση της απόλυτης τιμής του K).

Με άλλα λόγια, αν το b είναι αρκετά κοντά στο a τότε το a θα ανήκει στο $K(b)$.

Απόδειξη. Θεωρούμε την επέκταση $K(a,b)/K(b)$ και έστω $L/K(b)$ να είναι η Galois θήκη. Έστω $\sigma \in \mathrm{Gal}(L/K(b))$. Τότε $\sigma(b-a) = b - \sigma(a)$. Καθώς $|\sigma(x)| = |x|$ από την μοναδικότητα της επέκτασης της απόλυτης τιμής, έχουμε

$$|b - \sigma(a)| = |b - a| < |a_i - a|$$

για όλα τα $a_i \neq a$. Συνεπώς

$$|a - \sigma(a)| \leq \max\{|a - b|, |b - \sigma(a)|\} < |a_i - a|$$

Από το οποίο έπεται ότι $\sigma(a) = a$, άρα $a \in K(b)$ όπως θέλαμε.

□

Πρόταση 3.17. *Το $\mathbb{C}_p$ είναι αλγεβρικά κλειστό.*

Απόδειξη. Έστω a να είναι αλγεβρικό πάνω από το $\mathbb{C}_p$ και έστω $f(X)$ να είναι το ελάχιστό του πολυώνυμο στο $\mathbb{C}_p[X]$. Καθώς το $\overline{\mathbb{Q}}_p$ είναι πυκνό στο $\mathbb{C}_p$, μπορούμε να διαλέξουμε ένα πολυώνυμο $g(X) \in \overline{\mathbb{Q}}_p[X]$ του οποίου οι συντελεστές να είναι κοντά στους συντελεστές του $f(X)$. Τότε το $g(a) - f(a)$ θα είναι πολύ μικρό. Γράφοντας $g(X) = \prod(X - b_j)$, βλέπουμε ότι το $|a - b|$ είναι μικρό για κάποια ρίζα b του $g(X)$. Ειδικότερα, μπορούμε να διαλέξουμε το $g(X)$ και μετά το b έτσι ωστε

$$|b - a| < |a_i - a|$$

για όλα τα συζυγή $a_i \neq a$ του a. Συνεπώς, από το λήμμα του Krasner έχουμε ότι $a \in \mathbb{C}_p(b) = \mathbb{C}_p$, διότι $b \in \overline{\mathbb{Q}}_p \subset \mathbb{C}_p$. □

Ουσιαστικά, το $\mathbb{C}_p$ είναι η p-αδική έκδοση των μιγαδικών $\mathbb{C}$. Αυτά τα δύο σώματα είναι ισόμορφα με την αλγεβρική έννοια, αλλά όχι τοπολογικά. Και τα δύο έχουν μη-αριθμήσιμο βαθμό υπερβατικότητας πάνω από το $\mathbb{Q}$ και για να τα πάρουμε ξεκινάμε από το $\mathbb{Q}$ επισυνάπτοντας μια υπερβατική βάση και μετά παίρνουμε την αλγεβρική θήκη. Για αυτό, για τεχνικούς λόγους όπου είναι βολικό μπορούμε να εμφυτεύουμε το $\mathbb{C}$ στο $\mathbb{C}_p$ και αντίστροφα.

Αν σταθεροποιήσουμε μια εμφύτευση $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, μπορούμε να βλέπουμε τις τιμές που παίρνουν οι Dirichlet χαρακτήρες μέσα στο $\mathbb{C}_p$. Είδικότερα, βλέπουμε τον χαρακτήρα Teichmüller ως

$$\omega : \mathbb{F}_p^\times \longrightarrow \mathbb{C}_p$$

με $\omega(a)$ να είναι μια $(p-1)$-οστή ρίζα της μονάδας με $\omega(a) \equiv a (\mathrm{mod}\, p)$.

Θεώρημα 3.18 (Θεώρημα 5.11 στο [1]). *Έστω χ ένας χαρακτήρας Dirichlet. Υπάρχει μια p-αδική μερόμορφη απεικόνιση (αναλυτική αν $\chi \neq 1$) $\mathcal{L}_p(s,\chi)$ που ορίζεται στο $\{s \in \mathbb{C}_p : |s| < p^{1-1/(p-1)}\}$ έτσι ώστε:*

$$\mathcal{L}_p(1-n,\chi) = -(1-\chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}, \quad n \geq 1.$$

Αν $\chi = 1$ τότε η $\mathcal{L}_p(s,1)$ είναι αναλυτική εκτός από έναν πόλο στο $s=1$ με ολοκληρωτκό υπόλοιπο $1-1/p$.

Το $\chi\omega^{-n}$ είναι ο πρωταρχικός χαρακτήρας που επάγει τον $a \mapsto \chi(a)\omega^{-n}(a)$. Γενικά, αυτοί οι δύο δεν ταυτίζονται καθώς για $\chi = \omega^n$ έχουμε

$$\omega^n\omega^{-n}(p) = p \neq 0 = \omega^n(p)\omega^{-n}(p)$$

Μπορεί να βλέπει κανείς την p-αδική L-συνάρτηση $\mathcal{L}_p(s,\chi)$ ως μια παρεμβολή, για τα διαφορετικά p, στην συνήθη $L(s,\chi)$. Συγκεκριμένα, για $n \geq 1$ έχουμε

$$\mathcal{L}_p(1-n,\chi) = (1-\chi\omega^{-n}(p)p^{n-1})L(1-n,\chi\omega^{-n})$$

Άρα, αν $n \equiv 0 (\mathrm{mod}\, p-1)$ τότε παίρνουμε

$$\mathcal{L}_p(1-n,\chi) = (1-\chi(p)p^{n-1})L(1-n,\chi)$$

Θέλουμε να καταργήσουμε τον p-οστό παράγοντα στο γινόμενο Euler, καθώς όπως αναφέραμε πριν αν το p μπορεί να διαρεί το $1/n^s$, τότε η p-αδική απόλυτη τιμή θα παίρνει αυθαίρετα μεγάλες τιμές και έτσι το άθροισμα των στοιχείων δεν θα συγκλίνει. Επιπλέον, αν το χ είναι περιττός χαρακτήρας τότε θα ισχύει ότι $B_{n,\chi\omega^{-n}} = 0$. Άρα η p-αδική L-συνάρτηση ενός περιττού χαρακτήρα είναι ταυτοτικά 0. Ωστόσο, αν ο χ είναι άρτιος χαρακτήρας τότε το ίδιο δεν ισχύει. Οι ρίζες της p-αδικής L-συνάρτησης δεν μας είναι ακόμα πλήρως κατανοητές.

Θεώρημα 3.19 (Θεώρημα 5.12 στο [1]). *Έστω χ ένας μη τετριμμένος χαρακτήρας και $p^2 \nmid m_x$. (Υπενθυμίζουμε ξανά ότι αποφεύγουμε την περίπτωση $p=2$ αν και είναι εύκολα διαχειρίσιμη). Τότε*

$$\mathcal{L}_p(s,\chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

όπου $|a_0|_p \leq 1$ και $p|a_i$ για κάθε $i \geq 1$.

Πόρισμα 3.20. *Έστω m,n ακέραιοι με $m \equiv n (\mathrm{mod}\, p-1)$ και $n \not\equiv 0 (\mathrm{mod}\, p-1)$. Τότε ισχύει ότι*

$$\frac{B_m}{m} \equiv \frac{B_n}{n} (\mathrm{mod}\, p).$$

Απόδειξη. Καθώς $m \equiv n (\mathrm{mod}\, p-1)$ έχουμε ότι $\mathcal{L}_p(s,\omega^m) = \mathcal{L}_p(s,\omega^n)$. Ξέρουμε ότι

$$\mathcal{L}_p(1-m,\omega^m) = -(1-p^{m-1})\frac{B_m}{m}$$

και όμοια για το $\mathcal{L}_p(s,\omega^n)$. Από το προηγούμενο θεώρημα και αφού $m,n \not\equiv 0 (\mathrm{mod}\, p-1)$ μπορούμε να γράψουμε

$$\mathcal{L}_p(s,\omega^m) = a_0 + a_1(s-1) + a_2(s-1)^2 + \cdots$$

με $|a_0|_p \leq 1$ και $p|a_i$ για κάθε $i \geq 1$. Συνεπώς

$$\mathcal{L}_p(1-m,\omega^m) = a_0 + a_1(-m) + a_2(-m^2)^2 + \cdots \equiv a_0 (\mathrm{mod}\, p)$$

και όμοια για το $\mathcal{L}_p(1-n,\omega^n)$. Άρα, $\mathcal{L}_p(1-m,\omega^m) \equiv \mathcal{L}_p(1-n,\omega^n)(\mathrm{mod}\, p)$ δηλαδή έπεται το αποτέλεσμα. □

Λέμε ότι ένα στοιχείο $a/b \in \mathbb{C}_p$ είναι p-ακέραιο αν $|a/b|_p \geq 0$, δηλαδή όταν το p δεν διαιρεί τον παρονομαστή στην απλοποιημένη μορφή. Άμεσο πόρισμα του προηγούμενου θεωρήματος είναι το ακόλουθο:

Πόρισμα 3.21. *Έστω $m, n \in \mathbb{Z}$ και χ ένας μη τετριμένος χαρακτήρας με $p^2 \nmid m_\chi$. Τότε το $\mathcal{L}_p(m,\chi)$ είναι p-ακέραιο και*

$$\mathcal{L}_p(m,\chi) \equiv \mathcal{L}_p(n,\chi)(\mathrm{mod}\, p).$$

Πόρισμα 3.22. *Έστω n ένας περιττός ακέραιος και $n \not\equiv -1(\mathrm{mod}\, p-1)$. Τότε έχουμε*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1}(\mathrm{mod}\, p)$$

Απόδειξη. Παρατηρούμε ότι $\omega^{n+1} \neq 1$, καθώς $n \neq -1(\mathrm{mod}\, p-1)$. Επιπλέον, έχουμε ότι $\omega^n \neq 1$ αφού το n είναι περιττό και $\omega^n(p) = 0$. Από το θεώρημα 3.18 έχουμε ότι

$$\mathcal{L}_p(-n,\omega^{n+1}) = -(1-p^n)\frac{B_{n+1}}{n+1}$$

και

$$\mathcal{L}_p(0,\omega^{n+1}) = -(1-\omega^n(p))B_{1,\omega^n} = -B_{1,\omega^n}$$

και καθώς τα $\mathcal{L}_p(-n,\omega^{n+1})$ και $\mathcal{L}_p(0,\omega^{n+1})$ είναι και τα δύο p-ακέραια και ισότιμα $\mathrm{mod}\, p$ από το πόρισμα 3.21, έπεται το αποτέλεσμα. □

Θεώρημα 3.23. *Έστω p ένας περιττός πρώτος. Τότε $p|h_p^-$ αν και μόνο αν $p|B_j$ για κάποιο $j = 2, 4, \ldots, p-3$. Με το $p|B_j$ εννοούμε ότι το p διαιρεί τον αριθμητή του B_j.*

Απόδειξη. Υπενθυμίζουμε την σχέση 3.1

$$h_p^- = 2p \prod_{\substack{j=1 \\ j \text{ περιττός}}} \left(-\frac{1}{2}B_{1,\omega^j}\right)$$

και ξεκινάμε με το

$$2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) = -pB_{1,\omega^{p-2}}$$

Έχουμε ότι $B_{1,\omega^{p-2}} = B_{1,\omega^{-1}}$. Από τον ορισμό του $B_{1,\omega^{-1}}$ και τον ορισμό των Bernoulli πολυωνύμων στο [1], βλέπουμε ότι

$$B_{1,\omega^{-1}} = \frac{1}{p}\sum_{a=1}^{p-1} a\omega^{-1}(a)$$

Άρα έχουμε

$$2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) = -\sum_{a=1}^{p-1} a\omega^{-1}(a)$$

και καθώς $a \equiv \omega(a)\, \mathrm{mod}\, p$ παίρνουμε ότι

$$2p\left(-\frac{1}{2}B_{1,\omega^{p-2}}\right) \equiv -(p-1) \equiv 1(\mathrm{mod}\, p)$$

Συνεπώς,

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ περιττός}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^j}\right) (\mathrm{mod}\, p).$$

και εφαρμόζοντας το προηγούμενο πόρισμα παίρνουμε

$$\prod_{\substack{j=1 \\ j \text{ περιττός}}}^{p-4} \left(-\frac{1}{2}B_{1,\omega^j}\right) \equiv \prod_{\substack{j=1 \\ j \text{ περιττός}}}^{p-4} \left(-\frac{1}{2}\frac{B_{j+1}}{j+1}\right) (\mathrm{mod}\, p).$$

από το οποίο έπεται το θεώρημα. □

Ορισμός 3.24. *Λέμε ότι ένας πρώτος p είναι irregular αν $p|B_j$ για κάποιο $j = 2, 4, \ldots, p-3$. Διαφορετικά, τον λέμε κανονικό.*

Με το προηγούμενο θεώρημα έχουμε ότι το p είναι irregular πρώτος αν και μόνο αν $p|h_p^-$. Όπως θα δούμε στη συνέχεια ότι $p|h_p$ αν και μόνο αν $p|B_j$ για κάποιο $j = 2, 4, \ldots, p-3$. Άρα, το p είναι irregular αν και μόνο αν $p|h_p$. Αυτό χρησιμοποείται και ως εναλλακτικός ορισμός.

Θεώρημα 3.25. *Υπάρχουν άπειροι irregular πρώτοι.*

Απόδειξη. Έστω $p_1, \ldots, p_r$ είναι όλοι οι irregular πρώτοι και έστω $m = N(p_1 - 1) \cdots (p_r - 1)$ όπου το N διαλέγεται αρκετά μεγάλο ώστε $|B_m/m| > 1$. Μπορούμε να το κάνουμε αυτό, εφόσον από το [1] παίρνουμε ότι $|B_n/n| \to \infty$ καθώς $n \to \infty$. Έτσι, υπάρχει πρώτος p που διαιρεί τον αριθμητή του B_m/m. Καθώς τα p_i βρίσκονται στον παρονομαστή του B_m για $i = 1, \ldots, r$ από το θεώρημα Von Staudt-Clausen (Θεώρημα 5.10 στο [1]), δεν μπορούμε να έχουμε $p = p_i$ για κάποιο i. Επιπλέον, για τους ίδιους λόγους $m \not\equiv 0 (\mathrm{mod}\, p-1)$. Έστω $m' \equiv m (\mathrm{mod}\, p-1)$ με $0 < m' < p-1$. Τότε

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m} (\mathrm{mod}\, p)$$

και άρα $p|B_{m'}$. Συνεπώς, το p είναι irregular. Έπεται ότι υπάρχουν άπειροι irregular πρώτοι. □

Εικασία. *Υπάρχουν άπειροι κανονικοί πρώτοι.*

Στην συνέχεια θα δώσουμε την p-αδική έκδοση του τύπου του Dirichlet για τον τύπο του αριθμού κλάσεων. Εκτός από την αναλογία του με τον κλασικό τύπο, αυτό χρησιμοποιείται για να δωθεί ένα ακόμα αποτέλεσμα στους αριθμούς κλάσεων. Το αποτέλεσμα αυτό στο οποίο δεν θα επικεντρωθούμε είναι το ακόλουθο:

Θεώρημα 3.26. *Έστω $\chi \neq 1$ ένας άρτιος χαρακτήρας Dirichlet. Τότε $\mathcal{L}_p(1, \chi) \neq 0$.*

Θα διατηρήσουμε ως στόχο το παρακάτω θεώρημα.

Θεώρημα 3.27. *Αν $p|h_p^+$, τότε $p|h_p^-$. Ειδικότερα, $p|h_p$ αν και μόνο αν $p|B_j$ για κάποιο $j = 2, 4, \ldots, p-3$.*

Για να το αποδείξουμε χρειαζόμαστε τον p-αδικό τύπο του αριθμού κλάσεων του Dirichlet μαζί με τον ορισμό του p-αδικού regulator R_p, καθώς και μια επιπλέον πρόταση. Για τις αποδείξεις και τον πλήρη ορισμό του p-αδικού regulator μπορεί να ανατρέξει κανείς στο κεφάλαιο 5 στο [1] ή στο [14].

Θεώρημα 3.28. *Έστω K ένα πλήρως πραγματικό αβελιανό σώμα αριθμών με $[K : \mathbb{Q}] = n$. Έστω X η ομάδα χαρακτήρων που αντιστοιχεί στο K. Τότε έχουμε*

$$\prod_{\substack{\chi \in X \\ \chi \neq 1}} \left(1 - \frac{\chi(p)}{p}\right)^{-1} \mathcal{L}_p(1, \chi) = \frac{2^{n-1} h_K R_p(K)}{\sqrt{\Delta_K}}$$

Πρόταση 3.29 (Πρόταση 5.33 στο [1]). *Έστω K πλήρως πραγματικό Galois σώμα. Αν υπάρχει μόνο ένας πρώτος $\mathfrak{p}$ ετσι ώστε $\mathfrak{p}|p$ και αν $e(\mathfrak{p} \mid p) \leq p-1$, τότε*

$$\left| \frac{[K:\mathbb{Q}]R_p(K)}{\sqrt{\Delta_K}} \right|_p \leq 1$$

Απόδειξη. (Του θεωρήματος 3.27)

Υπενθυμίζουμε ότι η ομάδα χαρακτήρων που αντιστοιχεί στο $\mathbb{Q}(\zeta_p)^+$ είναι η

$$\{1, \omega^2, \omega^4, \ldots, \omega^{p-3}\}$$

δηλαδή οι άρτιοι χαρακτήρες του $\mathbb{Q}(\zeta_p)$, όπου όλοι τους δίνουν την τιμή 0 στο p. Εφόσον το $\mathbb{Q}(\zeta_p)^+$ είναι πλήρως πραγματικό, παίρνουμε από τον p-αδικό τύπο του Dirichlet

$$\prod_{\substack{j=2 \\ j \text{ άρτιο}}}^{p-3} \mathcal{L}_p(1, \omega^j) = \frac{2^{n-1} h_p^+ R_p^+}{\sqrt{\Delta_p^+}} \tag{3.2}$$

και το $\mathbb{Q}(\zeta_p)^+$ ικανοποιεί τις υποθέσεις της πρότασης 3.29, εφόσον γνωρίζουμε ότι

$$[\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}] = \frac{p-1}{2}$$

δηλαδή, έχουμε υποχρεωτικά ότι $e \leq p-1$ και στην μεγαλύτερη επέκταση υπάρχει μοναδικός πρώτος πάνω από το p, εφόσον ξέρουμε από την αλγεβρική θεωρία αριθμών ότι

$$p\mathcal{O}_{\mathbb{Q}(\zeta_p)} = (1-\zeta_p)^{p-1}$$

Συνεπώς:

$$\left| \frac{[\mathbb{Q}(\zeta_p)^+ : \mathbb{Q}]R_p^+}{\sqrt{\Delta_p^+}} \right|_p = \left| \frac{R_p^+}{\sqrt{\Delta_p^+}} \right|_p \leq 1$$

Άρα, αυτή η ποσότητα είναι p-ακέραια, οπότε αν υποθέσουμε ότι $p|h^+$ τότε δεν μπορεί το p να διαιρεί τον παρονομαστή $\sqrt{\Delta_p^+}$ και έτσι μπορούμε να καταλήξουμε στο ότι το p θα διαιρεί και το άλλο μέλος της ισότητας (3.2). Δηλαδή, έχουμε ότι $p|\mathcal{L}_p(1, \omega^j)$ για κάποιο $j \in \{2, 4, \ldots, p-3\}$. Από το πόρισμα 3.21 παίρνουμε ότι

$$\begin{aligned} -B_{1,\omega^{j-1}} &= -\left(1 - \omega^{j-1}(p)\right) B_{1,\omega^{j-1}} \\ &= \mathcal{L}_p(0, \omega^j) \\ &\equiv \mathcal{L}_p(1, \omega^j) (\mathrm{mod}\, p) \\ &\equiv 0 (\mathrm{mod}\, p) \end{aligned}$$

και καθώς τα B_{1,ω^i} είναι p-ακέραια και

$$h_p^- \equiv \prod_{\substack{i=1 \\ i \text{ περιττό}}}^{p-4} \left(-\frac{1}{2} B_{1,\omega^i} \right) (\mathrm{mod}\, p)$$

έπεται ότι

$$h_p^- \equiv 0 (\mathrm{mod}\, p)$$

□

Κλείνουμε την ενότητα με μια εικασία, ότι οι συνθήκη για το θεώρημα 3.27 δεν ικανοποιείται στην πραγματικότητα ποτέ.

Εικασία (Vandiver). *Για κάθε p πρώτο αριθμό έχουμε $p \nmid h_p^+$.*

3.4 Θεώρημα Herbrand

Σε αυτή την ενότητα θα αποδείξουμε ένα ισχυρότερο κριτήριο από το θεώρημα 3.27 κοιτώντας κομμάτια της ομάδας κλάσεων αντί για ολόκληρη την ομάδα. Αυτή η περιγραφή είναι γνωστή ως το θεώρημα του Herbrand. Θα αναφέρουμε επίσης το αντίστροφο σε αυτό το θεώρημα που απευθύνεται στον Ribet [7]. Η απόδειξη του αντιστρόφου δίνει μια εικόνα της μεθόδου που χρησιμοποίησε ο Wiles για να αποδείξει την κύρια εικασία της θεωρίας Iwasawa για τα πλήρως πραγματικά σώματα στο [4].

Το τι εννούμε με τα κομμάτια της ομάδας κλάσεων ιδεωδών θα γίνει ξεκάθαρο στη συνέχεια. Έστω G μια πεπερασμένη αβελιανή ομάδα και $G^\wedge$ η πολλαπλασιαστική ομάδα των χαρακτήρων της G όπως προηγουμένως. Έστω R ένας μεταθετικός δακτύλιος που περιέχει το $|G|^{-1}$ καθώς και όλες τις τιμές των $x \in G^\wedge$. Ορίζουμε τα κάθετα ταυτοδύναμα στοιχεία του ομαδοδακτύλιου $R[G]$ να είναι τα στοιχεία

$$\epsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in R[G].$$

Πρόταση 3.30. *Ισχύουν τα ακόλουθα:*

(1) $\varepsilon_\chi^2 = \varepsilon_\chi$.

(2) $\varepsilon_\chi \varepsilon_\psi = 0$ *αν* $\chi \neq \psi$.

(3) $\sum_{x \in G^\wedge} \varepsilon_\chi = 1$.

(4) $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$.

Απόδειξη.

(1) Το να πούμε ότι τα σ, h διατρέχουν τα στοιχεία της G είναι το ίδιο με το να πούμε τα $g = \sigma h$ και σ διατρέχουν την G, όπου αναγκαστικά $h = \sigma^{-1}g$. Συνεπώς

$$\begin{aligned}
\varepsilon_\chi^2 &= \frac{1}{|G|^2} \sum_{\sigma,h \in G} \chi(\sigma)\chi(h)\sigma^{-1}h^{-1} \\
&= \frac{1}{|G|^2} \sum_{\substack{g=\sigma h \\ \sigma \in G}} \sum_{g \in G} \chi(g)g^{-1} \\
&= \frac{1}{|G|} \sum_{\sigma \in G} \varepsilon_\chi \\
&= \varepsilon_\chi
\end{aligned}$$

(2)

$$\begin{aligned}
\varepsilon_\chi \varepsilon_\psi &= \frac{1}{|G|^2} \sum_{\sigma,h \in G} \chi(\sigma)\psi(h)\sigma^{-1}h^{-1} \\
&= \frac{1}{|G|^2} \sum_{\sigma \in G} \left(\sum_{h \in G} \chi(h)\psi(\sigma h^{-1}) \right) \sigma^{-1} \\
&= 0
\end{aligned}$$

καθώς από τις σχέσεις ορθογωνιότητας χαρακτήρων έχουμε

$$\sum_{h \in G} \chi(h)\psi(\sigma h^{-1}) = \psi(\sigma) \sum_{h \in G} \chi(h)\psi^{-1}(h) = 0$$

(3)

$$\begin{aligned}\sum_{\chi\in G^\wedge}\varepsilon_\chi &= \frac{1}{|G|}\sum_{\chi\in G^\wedge}\chi(g)g^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}\left(\sum_{\chi\in G^\wedge}\chi(g)\right)g^{-1}\\ &= \frac{1}{|G|}\left(|G|\cdot 1_G\right)\\ &= 1_G\end{aligned}$$

εφόσον

$$\sum_{\chi\in G^\wedge}\chi(g) = \begin{cases}|G|, & \text{αν } g = 1_G\\ 0, & \text{διαφορετικά}\end{cases}$$

το οποίο είναι αναδιατύπωση της σχέσης ορθογωνιότητας

$$\sum_{\chi\in G^\wedge}\chi(g)\chi^{-1}(h) = \sum_{\chi\in G^\wedge}\chi(gh^{-1}) = \begin{cases}|C_G(g)|, & \text{αν } g,h \text{ συζυγή}\\ 0, & \text{διαφορετικά}\end{cases}$$

και εφόσον η G είναι αβελιανή έχουμε $C_G(g) = G$ και τα g, h είναι συζυγή αν και μόνο αν $g = h$.

(4) Αρκεί να παρατηρήσουμε ότι καθώς το g διατρέχει τα στοιχεία της G, το ίδιο κάνει και το σg

$$\begin{aligned}\varepsilon_\chi\sigma &= \frac{1}{|G|}\sum_{g\in G}\chi(g)g^{-1}\sigma\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(\sigma g)(\sigma g)^{-1}\sigma\\ &= \frac{\chi(\sigma)}{|G|}\sum_{g\in G}\chi(g)g^{-1}\\ &= \chi(\sigma)\varepsilon_\chi\end{aligned}$$

□

Με τα παραπάνω έχουμε αποδείξει το ακόλουθο θεώρημα:

Θεώρημα 3.31. *Έστω M ένα $R[G]$-πρότυπο. Τότε έχουμε $M = \bigoplus_\chi \varepsilon_\chi M$.*

Παρατηρούμε ότι αν δούμε ένα $\sigma \in G$ να δρα στο M, τότε ο χώρος $\varepsilon_\chi M$ είναι ο ιδιοχώρος της δράσης με ιδιοτιμή $\chi(\sigma)$. Θα ειδικεύσουμε τώρα στην περίπτωση που το πρότυπο που κοιτάμε είναι μια ομάδα κλάσεων ιδεωδών. Έστω C η ομάδα κλάσεων ιδεωδών μιας αβελιανής επέκτασης $K/\mathbb{Q}$ και θέτουμε $G = \mathrm{Gal}(K/\mathbb{Q})$. Έχουμε από το θεώρημα Kronecker-Weber ότι $K \subseteq \mathbb{Q}(\zeta_n)$ για κάποιο n. Επιπλέον, ο ομαδοδακτύλιος $\mathbb{Z}[G]$ δρα με φυσιολογικό τρόπο στο C. Έστω $x = \sum x_\sigma\sigma \in \mathbb{Z}[G]$ και $\mathfrak{a}$ ένα κλασματικό ιδεώδες του K. Τότε η δράση δίνεται από:

$$x\cdot\mathfrak{a} = \mathfrak{a}^x = \prod_\sigma(\sigma\mathfrak{a})^{x_\sigma}$$

Έστω τώρα A να είναι η p-Sylow υποομάδα της ομάδας κλάσεων C. Επάγεται μια δράση του $\mathbb{Z}_p[G]$ στο A ως εξής:

$$\left(\sum_{j=0}^{\infty} a_j p^j\right) \cdot \mathfrak{a} = \prod_{j=1}^{\infty} (\mathfrak{a}^{a_j p^j})$$

καθώς ισχύει ότι $p^m A = 0$ για αρκετά μεγάλο m. Για έναν πραγματικό αριθμό x θα συμβολίζουμε με $\{x\}$ το μη ακέραιο μέρος του, δηλαδή $x - \{x\} \in \mathbb{Z}$ και $0 \leq \{x\} < 1$.

Ορισμός 3.32. *Το στοιχείο Stickelberger του K ορίζεται ως*

$$\theta = \theta(K) = \sum_{\substack{a (\mathrm{mod}\, n) \\ \gcd(a,n)=1}} \left\{\frac{a}{n}\right\} \sigma_a^{-1} \in \mathbb{Q}[G]$$

όπου σ_a είναι το στοιχείο της ομάδας $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ που δίνεται από την σχέση $\zeta_n \mapsto \zeta_n^a$ περιορισμένο στο K. Το ιδεώδες Stickelberger $I(K)$ του K ορίζεται να είναι το $\mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$. Με άλλα λόγια, είναι τα $\mathbb{Z}[G]$-πολλαπλάσια του θ που έχουν ακέραιους συντελεστές.

Αναφέρουμε το θεώρημα του Stickelberger το οποίο δεν θα αποδείξουμε. Για την απόδειξη μπορεί να ανατρέξει κανείς στο [1] στις σελίδες 96-100.

Θεώρημα 3.33 (Stickelberger's Theorem)**.** *Το ιδεώδες Stickelberger μηδενίζει την ομάδα κλάσεων ιδεωδών του K, δηλαδή αν $\mathfrak{a}$ είναι ένα κλασματικό ιδεώδες του K και b να ανήκει στο $\mathbb{Z}[G]$ έτσι ώστε $b\theta \in \mathbb{Z}[G]$, τότε το $(b\theta) \cdot \mathfrak{a}$ είναι κύριο.*

Υποθέτουμε τώρα ότι $K = \mathbb{Q}(\zeta_p)$ για p έναν περιττό πρώτο. Έχουμε ότι $G^\wedge = \{\omega^i : 0 \leq i \leq p-2\}$. Θα σταθούμε στον ομαδοδακτύλιο $\mathbb{Z}_p[G]$, όπου τα κεντρικά ταυτοδύναμα στοιχεία είναι:

$$\varepsilon_i := \varepsilon_{\omega^i} = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a) \sigma_a^{-1}$$

για $0 \leq i \leq p-2$ και το στοιχείο Stickelberger είναι το

$$\theta = \frac{1}{p} \sum_{a=1}^{p-1} a \sigma_a^{-1}$$

Παρατηρούμε ότι

$$\begin{aligned}
\varepsilon_i \theta &= \frac{1}{p} \sum_{a=1}^{p-1} a \varepsilon_i \sigma_a^{-1} \\
&= \frac{1}{p} \sum_{a=1}^{p-1} a \omega^i(\sigma_a^{-1}) \varepsilon_i \\
&= \frac{1}{p} \sum_{a=1}^{p-1} a \omega^{-i}(a) \varepsilon_i \\
&= B_{1,\omega^{-i}} \varepsilon_i
\end{aligned}$$

και όμοια για $c \in \mathbb{Z}$ έχουμε

$$\varepsilon_i (c - \sigma_c)\theta = (c - \omega^i(c)) B_{1,\omega^{-i}} \varepsilon_i$$

Πρόταση 3.34. *Έστω $c \in \mathbb{Z}$ με $p \nmid c$. Τότε $(c - \sigma_c)\theta \in \mathbb{Z}[G]$.*

Απόδειξη. Παρατηρούμε ότι

$$(c-\sigma_c)\theta = \sum_{a=1}^{p-1} c\left\{\frac{a}{p}\right\}\sigma_a^{-1} - \sum_{a=1}^{p-1}\left\{\frac{a}{p}\right\}\sigma_c\sigma_a^{-1}$$

Είναι προφανές ότι $\sigma_c\sigma_a^{-1} = \sigma_{ca^{-1}}$, άρα αλλάζοντας την σειρά της άθροισης των στοιχείων της G έχουμε

$$(c-\sigma_c)\theta = \sum_{a=1}^{p-1}\left(c\left\{\frac{a}{p}\right\} - \left\{\frac{ac}{p}\right\}\right)\sigma_a^{-1}$$

και καθώς $\left\{\frac{a}{p}\right\} = \frac{a}{p}$, μαζί με το $x - \{x\} \in \mathbb{Z}$ έχουμε ότι $(c-\sigma_c)\theta \in \mathbb{Z}[g]$, όπως θέλαμε. □

Έστω A η p-Sylow υποομάδα της ομάδας κλάσεων του $\mathbb{Q}(\zeta_p)$. Όπως επισημάναμε προηγουμένως, το A είναι $\mathbb{Z}_p[G]$-πρότυπο και άρα έχουμε την διάσπαση

$$A = \bigoplus_{i=0}^{p-2} A_i,$$

όπου με A_i θα γράφουμε το $\varepsilon_i A$. Το θεώρημα του Stickelberger μαζί με την προηγούμενη πρόταση έχουν ως συνέπεια ότι το $(c-\sigma_c)\theta$ θα μηδενίζει το A, άρα και κάθε A_i όπου $p \nmid |c$. Ειδικότερα, έχουμε δείξει ότι το $(c-\omega^i(c))B_{1,\omega^{-i}}$ μηδενίζει το A_i. Σημειώνουμε ότι για $i \neq 0$ άρτιο, το $B_{1,\omega^{-1}}$ είναι 0, δηλαδή δεν έχουμε δείξει κάτι καινούργιο. Για $i = 0$ έχουμε ότι το $(c-1)/2$ μηδενίζει το A_0 για κάθε c με $p \nmid c$. Άρα πρέπει να είναι $A_0 = 0$. Τώρα θα ασχοληθούμε με την περίπτωση που το i είναι περιττό. Αν $i \neq 1$, τότε υπάρχει c ώστε $c \not\equiv \omega^i(c) (\mathrm{mod}\, p)$ και άρα μπορούμε να αγνοήσουμε τον παράγοντα $(c-\omega^i(c))$ και να πάρουμε ότι το $B_{1,\omega^{-i}}$ μηδενίζει το A_i. Αν $i = 1$, θέτουμε $c = 1 + p$. Τότε

$$\begin{aligned}(c-\omega(c))B_{1,\omega^{-1}} &= pB_{1,\omega^{-1}} \\ &= \sum_{a=1}^{p-1} a\omega^{-1}(a) \\ &= p - 1 \not\equiv 0 (\mathrm{mod}\, p)\end{aligned}$$

και καθώς το A_1 είναι p-ομάδα, υποχρεωτικά έχουμε $A_1 = 0$. Άρα έχουμε αποδείξει την ακόλουθη πρόταση.

Πρόταση 3.35. *Τα κομμάτια A_0 και A_1 της ομάδας κλάσεων είναι και τα δύο 0 και για $i = 3, 5, \ldots, p-2$ έχουμε ότι το $B_{1,\omega^{-i}}$ μηδενίζει το A_i.*

Είμαστε πλέον σε θέση να αποδείξουμε το θεώρημα του Herbrand. Να σημειώσουμε ότι είναι στην μια κατεύθυνση πιο ισχυρό από το θεώρημα 3.27, όπου είχαμε αν $p|h_p$ τότε το p διαιρεί κάποιον αριθμό Bernoulli. Εδώ παίρνουμε ακριβώς ποιον αριθμό Bernoulli, που είναι αντίστοιχος με το ποιο κομμάτι της ομάδας κλάσεων είναι μη τετριμμένο.

Θεώρημα 3.36 (Herbrand's Theorem)**.** *Έστω i περιττό με $3 \leq i \leq p-2$. Αν $A_i \neq 0$, τότε $p|B_{p-i}$.*

Απόδειξη. Έχουμε ότι το $B_{1,\omega^{-i}}$ μηδενίζει το μη τετριμμένο A_i που είναι p-ομάδα, άρα έχουμε ότι $p|B_{1,\omega^{-i}}$. Ωστόσο, ισχύει επιπλέον ότι

$$B_{1,\omega^{-i}} \equiv \frac{B_{p-i}}{p-i} (\mathrm{mod}\, p)$$

και αυτές οι δύο ποσότητες είναι p-ακέραιες. Άρα πράγματι $p|B_{p-i}$. □

Θεώρημα 3.37 (Ribet). *Έστω i περιττό με $3 \leq i \leq p-2$. Αν $p|B_{p-i}$, τότε $A_i \neq 0$.*

Ο Ribet αποδεικνύει το αντίστροφο του θεωρήματος του Herbrand κατασκευάζοντας στοιχεία μέσα στο A_i. Ωστόσο, παραλείπουμε την απόδειξη του καθώς αυτή η κατασκευή βασίζεται σε τεχνικές από modular forms και Galois αναπαραστάσεων, ώστε να βρεθεί στοιχείο τάξης p στο αντίστοιχο κομμάτι της ομάδας κλάσεων. Αξίζει να σημειωθεί ότι αυτές τις τεχνικές ανέπτυξαν περεταίρω οι Mazur και Wiles στο [3], για να αποδείξουν την κύρια εικασία Iwasawa πάνω από το $\mathbb{Q}$, στην οποία θα αναφερθούμε αργότερα. Θα κλείσουμε την ενότητα με την ακόλουθη γενίκευση του παρακάτω αποτελέσματος.

$$p|h_p^+ \implies p|h_p^-.$$

Θεώρημα 3.38. *Έστω i άρτιο και j περιττό με $i+j \equiv 1 (\mathrm{mod}\, p-1)$. Τότε*

$$p\text{-rank}(A_i) \leq p\text{-rank}(A_j) \leq 1 + p\text{-rank}(A_i)$$

όπου το p-rank μιας πεπερασμένης αβελιανής ομάδας G είναι η διάσταση του G/pG ως $\mathbb{F}_p$-διανυσματικού χώρου.

Το γιατί είναι αυτό το αποτέλεσμα γενίκευση του $p|h_p^+ \implies p|h_p^-$ θα γίνει ξεκάθαρο στην συνέχεια. Υπενθυμίζουμε ότι ορίσαμε το h_p^+ να είναι το μέγεθος της ομάδας κλάσεων του $\mathbb{Q}(\zeta_p)^+$. Δείξαμε ότι $h_p^+|h_p$ και ορίσαμε το $h_p^- = h_p/h_p^+$. Θα δείξουμε τώρα ότι τα h_p^+, h_p^- είναι μεγέθη των κομματιών της ομάδας κλάσεων του $\mathbb{Q}(\zeta_p)$. Όπως συνηθίζεται, θα συμβολίζουμε τον μιγαδικό συζυγή $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ με J. Γράφουμε C_p για την ομάδα κλάσεων του $\mathbb{Q}(\zeta_p)$ και C_{p^+} για την ομάδα κλάσεων του $\mathbb{Q}(\zeta_p)^+$.

Έστω C_p^- να είναι ο (-1)-ιδιόχωρος του C_p ως προς την δράση του J, δηλαδή

$$C_p^- = \{\mathfrak{a} \in C_p : \ (1+J)\cdot \mathfrak{a} = 1\}.$$

Υπενθυμίζουμε από την θεωρία κλάσεων σωμάτων ότι αν έχουμε $H_{\mathbb{Q}(\zeta_p)^+} \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p)^+$, τότε η απεικόνιση νόρμας $C_p \longrightarrow C_{p^+}$ είναι επί, όπου το $H_{\mathbb{Q}(\zeta_p)^+}$ είναι το Hilbert σώμα κλάσης του $\mathbb{Q}(\zeta_p)^+$. Ωστόσο, ξέρουμε ότι το $\mathbb{Q}(\zeta_p)$ είναι διακλαδιζόμενο πάνω από το $\mathbb{Q}(\zeta_p)^+$ στους αρχιμήδειους πρώτους, οπότε ικανοποιείται αυτή η συνθήκη. Παρατηρούμε ότι έχουμε την ακριβή ακολουθία:

$$1 \longrightarrow C_p^- \longrightarrow C_p \xrightarrow{\mathrm{Norm}} C_{p^+} \longrightarrow 1$$

Για να δει κανείς ότι το C_p^- είναι ακριβώς ο πυρήνας της απεικόνισης νόρμας μπορεί να ανατρέξει στην σελίδα 63 του [14] για τις ιδιότητες της απεικόνισης νόρμας, σε συνδυασμό με το γεγονός ότι $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p)^+) \simeq \{1, J\}$. Συνεπώς, βλέπουμε ότι το h_p^- είναι η τάξη του C_p^-, ενός κομματιού της ομάδας κλάσεων του $\mathbb{Q}(\zeta_p)$.

Καθώς χρειάζεται να κοιτάμε μόνο την p-διαιρετότητα στο παραπάνω θεώρημα, θα περιοριστούμε να δουλεύουμε στο p-μέρος της ομάδας κλάσεων. Θέτουμε $\varepsilon_- = \frac{1-J}{2}$ και $\varepsilon_+ = \frac{1+J}{2}$. Με έναν γρήγορο υπολογισμό φαίνεται ότι ο (-1)-ιδιόχωρος της δράσης του J στο A είναι ακριβώς το $\varepsilon_- A$. Άρα θα γράφουμε $A^- = \varepsilon_- A$ και $A^+ = \varepsilon_+ A$. Έχουμε ότι $A = A^- \oplus A^+$. Έτσι, το παραπάνω αποτέλεσμα δείχνει ακριβώς ότι το A^+ είναι ακριβώς το p-μέρος του C_{p^+} όπως θέλαμε. Μπορεί να δειχτεί ότι

$$\varepsilon_+ = \sum_{i \text{ άρτιο}} \varepsilon_i$$

και

$$\varepsilon_- = \sum_{i \text{ περιττό}} \varepsilon_i$$

δηλαδή

$$A^- = A_1 \oplus A_3 \oplus \cdots \oplus A_{p-2}$$

και

$$A^+ = A_0 \oplus A_2 \oplus \cdots \oplus A_{p-3},$$

όπου τώρα φαίνεται ξεκάθαρα ότι το παραπάνω θεώρημα γενικεύει την πρόταση $p|h_p^+ \implies p|h_p^-$.

$\mathbb{Z}_p$-Επεκτάσεις

Σε αυτό το κεφάλαιο θα έχουμε ως σκοπό να αποδείξουμε το θεώρημα του Iwasawa, το οποίο περιγράφει έναν ρυθμό αύξησης του μεγέθους των ομάδων κλάσεων ιδεωδών για τις $\mathbb{Z}_p$-επεκτάσεις. Έχοντας ένα σώμα αριθμών K, μια $\mathbb{Z}_p$-επέκταση του K είναι μια επέκταση K_∞/K για την οποία ισχύει $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, όπου εδώ εννούμε την προσθετική ομάδα των p-αδικών ακέραιων. Καθώς όπως θα δούμε $K_\infty = \cup K_n$ για κάποιες ενδιάμεσες επεκτάσεις K_n/K, τα βήματα που θα ακολουθήσουμε για να αποδείξουμε το θεώρημα είναι τα εξής:

(1) Περιγραφή της άλγεβρας Iwasawa $\Lambda = \mathbb{Z}_p[[T]]$.

(2) Απόδειξη ενός θεωρήματος δομής για τα πρότυπα Iwasawa.

(3) Χρήση θεωρίας κλάσεων σωμάτων για να παίρνουμε πληροφορίες στα διάφορα στρώματα με πεπερασμένη τάξη, δηλαδή στις p-Sylow υποομάδες των ομάδων κλάσεων των K_n, καθώς ανεβαίνουμε τον πύργο K_∞.

Να σημειώσουμε ότι στα παρακάτω οι τοπολογίες που θα συναντάμε ταυτίζονται και οι ομάδες είναι ισόμορφες ως τοπολογικές. Δηλαδή, στις $\mathbb{Z}_p$-επεκτάσεις η τοπολογία Krull της άπειρης ομάδας Galois, με την επαγόμενη τοπολογία που παίρνει το αντίστροφο όριο και η την τοπολογία της προσθετικής ομάδας $\mathbb{Z}_p$ που επάγεται από την p-αδική νόρμα ταυτίζονται.

Θα σταθεροποιήσουμε τώρα έναν περιττό πρώτο p, ωστόσο και η περίπτωση $p = 2$ ακολουθεί τα ίδια αποτελέσματα, αλλά θα χρειαζόταν να επιβαρύνουμε τους συμβολισμούς. Για την πλήρη διατύπωση μπορεί να ανατρέξει κανείς στο [1]. Θα ξεκινήσουμε με την ύπαρξη μιας $\mathbb{Z}_p$-επέκτασης για ένα σώμα αριθμών. Άρχικά για το $\mathbb{Q}$, υπενθυμίζουμε ότι:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^n\mathbb{Z}.$$

Έστω $\mathbb{Q}_n$ το σταθερό σώμα του $(\mathbb{Z}/p\mathbb{Z})^\times$, δηλαδή $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^{(\mathbb{Z}/p\mathbb{Z})^\times}$. Από την θεωρία Galois ξέρουμε ότι $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Θέτουμε $\mathbb{Q}_\infty = \cup\mathbb{Q}_n$. Τότε έχουμε ότι

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) &\cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \\ &\cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z}) \\ &\cong \mathbb{Z}_p,\end{aligned}$$

εφόσον η απεικόνιση $\sigma \longmapsto (\sigma|_{\mathbb{Q}_n})_n$ είναι ισομορφισμός τοπολογικών ομάδων. Άρα υπάρχει $\mathbb{Z}_p$-επέκταση για τους ρητούς.

Για να δείξουμε την ύπαρξη για ένα τυχαίο σώμα αριθμών K, θέτουμε $K_\infty = K\mathbb{Q}_\infty$ το σύνθετο σώμα. Συνεπώς, έχουμε ότι $\mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$. Το $\mathbb{Q}_\infty \cap K$ είναι ενδιάμεση επέκταση της $\mathbb{Q}_\infty/\mathbb{Q}$ και άρα από την αντιστοιχία Galois για τις άπειρες επεκτάσεις έχουμε ότι η $\mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$ είναι κλειστή υποομάδα της $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Άρα κάτω από τον ισομορφισμό, είναι της μορφής $p^n\mathbb{Z}_p$ για κάποιο $n \in \mathbb{N}$, αφού αυτή τη μορφή έχουν τα κλειστά υποσύνολα των p-αδικών ακεραίων. Πράγματι, έστω H κλειστή υποομάδα του $\mathbb{Z}_p$ και $h \in H$ ένα στοιχείο με ελάχιστη εκτίμηση. Από την ιδιότητα της υποομάδας έχουμε ότι $h\mathbb{Z} \subseteq H$ και

λόγω ότι η H είναι κλειστή έχουμε ότι $h\mathbb{Z}_p \subseteq H$. Ωστόσο, καθώς επιλέξαμε το h να έχει ελάχιστη εκτίμηση, πρέπει να είναι της μορφής $H = h\mathbb{Z}_p = p^n\mathbb{Z}_p$ για κάποιο n. Άρα έχουμε

$$\mathrm{Gal}(K_\infty/K) \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p$$

όπως θέλαμε, εφόσον και η απεικόνιση $x \in \mathbb{Z}_p \longmapsto p^n x \in p^n\mathbb{Z}_p$ είναι ισομορφισμός τοπολογικών ομάδων. Άρα έχουμε την ύπαρξη $\mathbb{Z}_p$-επεκτάσεων για τυχαία σώματα αριθμών. Η επέκταση που κατασκευάσαμε είναι γνωστή ως *κυκλοτομική*. Μπορεί για κάποιο K να υπάρχουν και άλλες $\mathbb{Z}_p$-επεκτάσεις, αλλά έχουμε εξασφαλίσει ότι κάθε σώμα αριθμών έχει τουλάχιστον μία.

Έστω τώρα K_∞ μια τυχαία $\mathbb{Z}_p$-επέκταση του K. Θέλουμε να δείξουμε ότι μπορούμε να σκεφτόμαστε το K_∞ σαν ένωση από μια ακολουθία ενδιάμεσων σωμάτων:

$$K = K_0 \subset K_1 \cdots \subset K_\infty = \bigcup K_n$$

για τα οποία ισχύει

$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Κοιτώντας πάλι την αντιστοιχία Galois για τις άπειρες επεκτάσεις, ξέρουμε ότι οι κλειστές υποομάδες $p^n\mathbb{Z}_p$ θα απεικονίζονται σε ενδιάμεσα σώματα. Άρα θέτουμε ως K_n τα σταθερά σώματα:

$$K_n := K_\infty^{p^n\mathbb{Z}_p},$$

όπου πράγματι

$$\bigcup_{n\geq 0} K_n = \bigcup_{n\geq 0} K_\infty^{p^n\mathbb{Z}_p} = K_\infty^{\{1\}} = K_\infty.$$

Μπορούμε πλέον να διατυπώσουμε το θεώρημα που θα αποδείξουμε στο τέλος του κεφαλαίου.

Θεώρημα 4.1 (Iwasawa)**.** *Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση και h_n να είναι η τάξη της ομάδας κλάσεων του K_n. Αν $h_n = p^{e_n}r$ με $(r,p) = 1$, τότε υπάρχουν ακέραιοι $\lambda \geq 0, \mu \geq 0, \nu$ και n_0 έτσι ώστε*

$$e_n = \lambda n + \mu p^n + \nu$$

για κάθε $n \geq n_0$, όπου τα λ, μ, ν είναι όλα ανεξάρτητα του n.

4.1 Δακτύλιοι Δυναμοσειρών

Ένα από τα κύρια αντικείμενα της θεωρίας Iwasawa είναι η Iwasawa άλγεβρα $\Lambda = \mathbb{Z}_p[[T]]$, δηλαδή ο δακτύλιος τυπικών δυναμοσειρών στο T με συντελεστές από το $\mathbb{Z}_p$. Θα περιγράψουμε στη συνέχεια γενικά αποτελέσματα για τις πεπερασμένες επεκτάσεις της Λ που θα χρησιμοποιηθούν για την απόδειξη του θεωρήματος 4.1.

Έστω $K/\mathbb{Q}_p$ μια πεπερασμένη επέκταση, $\mathcal{O} := \mathcal{O}_K$ ο δακτύλιος ακεραίων του K, $\mathfrak{p}$ το μέγιστο ιδεώδες του $\mathcal{O}$ και π ένας γεννήτορας του, δηλαδή $\mathfrak{p} = (\pi)$. Ξεκινάμε με το να αποδείξουμε έναν αλγόριθμο διαίρεσης για την άλγεβρα $\Lambda_\mathcal{O} := \mathcal{O}[[T]]$.

Πρόταση 4.2. *Έστω $f, g \in \Lambda_\mathcal{O}$ με $f = a_0 + a_1T + \cdots$ με $a_i \in \mathfrak{p}$ για κάθε $0 \leq i \leq n-1$ και $a_n \in \mathcal{O}^\times$. Τότε υπάρχουν μοναδικά $q \in \Lambda_\mathcal{O}$ και $r \in \mathcal{O}[T]$ με βαθμό $\deg r \leq n-1$ έτσι ώστε*

$$g = qf + r$$

Απόδειξη. Αρχίζουμε την απόδειξη με το να ορίσουμε έναν shift τελεστή $\tau_n := \tau : \Lambda_\mathcal{O} \longrightarrow \Lambda_\mathcal{O}$ έτσι ώστε

$$b_0 + b_1T + b_2T^2 + \cdots \longmapsto b_n + b_{n+1}T + b_{n+2}T^2 + \cdots$$

δηλαδή

$$\tau\left(\sum_{i=0}^{\infty} b_iT^i\right) = \sum_{i=n}^{\infty} b_iT^{i-n}$$

Ο τελεστής τ είναι προφανώς $\mathcal{O}$-γραμμικός. Επιπλέον, ισχύουν οι σχέσεις

- $\tau(T^n h(T)) = h(T)$.
- $\tau(h(T)) = 0$ αν και μόνο αν το h είναι πολυώνυμο βαθμού $\leq n-1$.

Από την υπόθεση για το f έχουμε ότι

$$f(T) = \pi P(T) + T^n U(T), \tag{4.1}$$

όπου το $P(T)$ είναι πολυώνυμο βαθμού μικρότερου ή ίσου με $n-1$ και το $U(T)$ είναι αντιστρέψιμο στο $\Lambda_{\mathcal{O}}$, καθώς ο σταθερός όρος του a_n είναι αντιστρέψιμος. Θέτουμε

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g),$$

όπου για παράδειγμα έχουμε

$$\left(\tau \circ \frac{P}{U}\right)^2 \circ \tau(g) = \tau\left(\frac{P}{U}\left(\tau\left(\frac{P}{U} \cdot \tau(g)\right)\right)\right)$$

Καθώς στην p-αδική νόρμα που επάγεται στο K ισχύει ότι μια σειρά συγκλίνει αν και μόνο αν η ακολουθία τείνει στο μηδέν, η ύπαρξη του π^j αναγκάζει το q να ανήκει στο $\Lambda_{\mathcal{O}}$. Χρησιμοποιώντας την σχέση 4.1 έχουμε

$$qf = \pi q P + T^n q U,$$

Εφαρμόζοντας τον τ παίρνουμε

$$\tau(qf) = \pi\tau(qP) + \tau(T^n qU) = \pi\tau(qP) + qU \tag{4.2}$$

και κοιτάμε τώρα το $\pi\tau(qP)$:

$$\begin{aligned}
\pi\tau(qP) &= \pi\tau\left(\frac{P}{U}\sum_{j=0}^{\infty}(-1)^j\pi^j\left(\tau\circ\frac{P}{U}\right)^j\circ\tau(g)\right)\\
&= \sum_{j=0}^{\infty}(-1)^j\pi^{j+1}\left(\tau\circ\frac{P}{U}\right)^{j+1}\circ\tau(g)\\
&= \pi\left(\tau\circ\frac{P}{U}\right)\circ\tau(g) - \pi^2\left(\tau\circ\frac{P}{U}\right)^2\circ\tau(g) + \cdots\\
&= \tau(g) - \left(\tau(g) - \pi\left(\tau\circ\frac{P}{U}\right)\circ\tau(g) + \pi^2\left(\tau\circ\frac{P}{U}\right)^2\circ\tau(g) + \cdots\right)\\
&= \tau(g) - Uq.
\end{aligned}$$

Συνδυάζοντας το με την σχέση 4.2 παίρνουμε ότι

$$\tau(qf) = \tau(g).$$

Συνεπώς, έχουμε ότι τα $\tau(qf)$ και $\tau(g)$ διαφέρουν μόνο κατά ένα πολυώνυμο βαθμού μικρότερου ίσου του n. Για την μοναδικότητα, υποθέτουμε ότι υπάρχουν q_1, q_2, r_1 και r_2 με $g = q_1 f + r_1 = q_2 f + r_2$. Τότε έχουμε ότι $(q_1 - q_2)f + (r_1 - r_2) = 0$. Υποθέτουμε ότι $q_1 \neq q_2$ και $r_1 \neq r_2$. Άρα μπορούμε να υποθέσουμε ότι $\pi \nmid (q_1 - q_2)$ ή $\pi \nmid (r_1 - r_2)$. Κοιτώντας αυτά modulo π, έχουμε ότι $r_1 \equiv r_2 (\mathrm{mod}\, \pi)$, καθώς $\pi | a_i$ για τα $1 \leq i \leq n-1$. Έτσι, $\pi | (q_1 - q_2) f$. Ωστόσο, γνωρίζουμε ότι $\pi \not| f$ καθώς $a_n \in \mathcal{O}^\times$, άρα καταλήγουμε στο άτοπο $\pi | (q_1 - q_2)$. □

Ορισμός 4.3. *Έστω $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 \in \mathcal{O}[T]$. Θα λέμε το $P(T)$ είναι distinguished αν $a_i \in \mathfrak{p}$ για τα $0 \leq i \leq n-1$.*

Θεώρημα 4.4 (p-adic Weierstrass Preparation Theorem)**.** *Έστω* $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \Lambda_{\mathcal{O}}$ *και υποθέτουμε ότι υπάρχει* $n \in \mathbb{N}$ *με* $a_i \in \mathfrak{p}$ *για όλα τα* $0 \leq i \leq n-1$*, ενώ* $a_n \in \mathcal{O}^\times$*. Τότε υπάρχει μοναδικό* $U(T) \in \Lambda_{\mathcal{O}}$ *αντιστρέψιμο και μοναδικό* $P(T) \in \mathcal{O}[T]$ *ένα distinguished πολυώνυμο βαθμού* n*, έτσι ώστε*

$$f(T) = P(T)U(T).$$

Αν το $f(T) \in \Lambda_{\mathcal{O}}$ *είναι μη μηδενικό, τότε υπάρχει* $\mu \in \mathbb{Z}, \mu \geq 0$ *και* $P(T) \in \mathcal{O}[T]$ *distinguished πολυώνυμο βαθμού το πολύ* n *και ένα αντιστρέψιμο* $U(T) \in \Lambda_{\mathcal{O}}$ *έτσι ώστε*

$$f(T) = \pi^m P(T)U(T).$$

Απόδειξη. Ξεκινάμε εφαρμόζοντας τον αλγόριθμο διαίρεσης στο $g(T) = T^n$ και $f(T)$ ώστε να πάρουμε

$$q(T) = \sum_{i=0}^{\infty} q_i T^i \in \Lambda_{\mathcal{O}}$$

και $r(T) \in \mathcal{O}[T]$ με

$$T^n = f(T)q(T) + r(T), \tag{4.3}$$

όπου $\deg r(T) \leq n-1$. Αν θεωρήσουμε αυτή την ισότητα modulo π βλέπουμε ότι

$$T^n \equiv q(T)(a_n T^n + a_{n+1}T^{n+1} + \cdots) + r(T) (\mathrm{mod}\, \pi).$$

Καθώς $\deg r(T) \leq n-1$, έχουμε ότι $r(T) \equiv 0 (\mathrm{mod}\, \pi)$ εφόσον είναι το μόνο στην παραπάνω σχέση που έχει όρους με βαθμό μικρότερο του $n-1$. Συνεπώς, το $T^n - r(T)$ είναι distinguished πολυώνυμο, το οποίο θέτουμε ως $P(T)$. Κοιτώντας την σχέση 4.3 και τους συντελεστές του T^n, έχουμε ότι $q_0 a_n \equiv 1 (\mathrm{mod}\, \pi)$. Συνεπώς, $\pi \nmid q_0$ το οποίο σημαίνει ότι $q_0 \in \mathcal{O}^\times$, δηλαδή το $q(T)$ είναι αντιστρέψιμο. Άρα έχουμε

$$T^n - r(T) = f(T)q(T)$$

δηλαδή,

$$f(T) = P(T)U(T),$$

όπου $U(T) = q(T)^{-1}$.

Για τη μοναδικότητα, κάθε distinguished πολυώνυμο γράφεται ως $P(T) = T^n - r(T)$. Έτσι, μετατρέπουμε την σχέση $f(T) = P(T)U(T)$ σε μια σχέση της μορφής $T^n = f(T)q(T) + r(T)$ και παίρνουμε την μοναδικότητα από την μοναδικότητα στον αλγόριθμο διαίρεσης. Για το δεύτερο επιχείρημα, απλά βγάζουμε κοινό παράγοντα την μεγαλύτερη δυνατή δύναμη του π. □

Πόρισμα 4.5. *Έστω* $f(T) \in \Lambda_{\mathcal{O}}$ *μη μηδενικό. Τότε υπάρχουν πεπερασμένα το πλήθος* $z \in \mathbb{C}_p$ *με* $|z|_p < 1$ *και* $f(z) = 0$.

Απόδειξη. Γράφουμε $f(T) = \pi^m P(T)U(T)$. Καθώς το U είναι αντιστρέψιμο έχουμε ότι $U(z)U^{-1}(z) = 1$, δηλαδή $U(z) \neq 0$. Άρα αν $f(z) = 0$, έπεται ότι $P(z) = 0$. Ωστόσο, το P είναι πολυώνυμο πάνω από το σώμα K, άρα έπεται το αποτέλεσμα. □

Λήμμα 4.6. *Έστω* $P(T) \in \mathcal{O}[T]$ *ένα distinguished πολυώνυμο και* $g(T) \in \mathcal{O}[T]$*. Υποθέτουμε ότι* $\frac{g(T)}{P(T)} \in \Lambda_{\mathcal{O}}$*, τότε* $\frac{g(T)}{P(T)} \in \mathcal{O}[T]$.

Απόδειξη. Έστω $f(T) \in \Lambda_{\mathcal{O}}$ έτσι ώστε $\frac{g(T)}{P(T)} = f(T)$, δηλαδή $g(T) = f(T)P(T)$. Έστω z μια ρίζα του $P(T)$. Τότε

$$0 = P(z) = z^n + (\text{πολλαπλάσιο του } \pi)$$

εφόσον το P είναι distinguished. Τότε καθώς $\pi | z$ έχουμε ότι $|z|_p < 1$. Άρα έχουμε ότι το $f(T)$ συγκλίνει στο z και άρα $g(z) = 0$, δηλαδή $(T-z)|g(T)$. Συνεχίζοντας με το ίδιο επιχείρημα για τις υπόλοιπες ρίζες, όπου πιθανά επεκτείνουμε το K να τις περιέχει όλες και κοιτάμε τον αντίστοιχο δακτύλιο ακεραίων, βλέπουμε ότι $P(T)|g(T)$ ως πολυώνυμα. □

4.2 Θεώρημα Δομής $\Lambda_{\mathcal{O}}$-προτύπων

Έχουμε δείξει στην προηγούμενη ενότητα ότι το $\Lambda_{\mathcal{O}}$ είναι περιοχή μοναδικής παραγοντοποίησης με ανάγωγα στοιχεία το π και τα ανάγωγα distinguished πολυώνυμα. Υπενθυμίζουμε και ότι τα αντιστρέψιμα στοιχεία του $\Lambda_{\mathcal{O}}$ είναι αυτά που έχουν σταθερό όρο στο $\mathcal{O}^\times$.

Σε αυτή την ενότητα θα διατυπώσουμε ένα πολύ ισχυρό θεώρημα δομής για τα πεπερασμένα παραγόμενα $\Lambda_{\mathcal{O}}$-πρότυπα, το οποίο θα χρησιμοποιηθεί για την μελέτη ομάδων Galois με απώτερο σκοπό το θεώρημα Iwasawa.

Λήμμα 4.7. *Έστω $f, g \in \Lambda_{\mathcal{O}}$ σχετικά πρώτα. Τότε το ιδεώδες (f, g) έχει πεπερασμένο δείκτη στο $\Lambda_{\mathcal{O}}$.*

Απόδειξη. Έστω $h \in (f, g)$ με ελάχιστο βαθμό. Από το θεώρημα προπαρασκευής του Weierstrass μπορούμε να γράψουμε δίχως βλάβη γενικότητας $h(T) = \pi^n H(T)$ για κάποιον ακέραιο n και όπου $H = 1$ ή H να είναι distinguished πολυώνυμο. Έχουμε αυτή τη γραφή εφόσον θεωρούμε το h ελάχιστου βαθμού, διαφορετικά από το $h(T) = \pi^n H(T)U(T)$ θα παίρναμε ως νέο h το hU^{-1}.

Αν $H \neq 1$ τότε μπορούμε να γράψουμε $f = qH + r$ με $\deg r < \deg H$. Αυτό μας δίνει

$$\begin{aligned} \pi^n f &= q\pi^n H + \pi^n r \\ &= qh + \pi^n r. \end{aligned}$$

Ωστόσο, αυτό μας δείχνει ότι $\pi^n r \in (f, g)$ και έχει μικρότερο βαθμό από το h, το οποίο είναι άτοπο. Υποθέτουμε τώρα ότι $H = 1$ και άρα $h = \pi^n$. Μπορούμε να υποθέσουμε ότι $\pi \nmid f$, καθώς αν το διαιρεί μπορούμε να κάνουμε την ίδια υπόθεση για το g εφόσον είναι σχετικά πρώτα. Επιπλέον, δίχως βλάβη γενικότητας μπορούμε πάλι με το θεώρημα προπαρασκευής του Weierstrass να υποθέσουμε ότι το f είναι distinguished, διαφορετικά θα παίρναμε ως f το $P(T) = f(T)/U(T)$ το οποίο παράγει το ίδιο ιδεώδες. Έχουμε ότι

$$(\pi^n, f) \subseteq (f, g)$$

και άρα

$$\Lambda_{\mathcal{O}}/(\pi^n, f) \supseteq \Lambda_{\mathcal{O}}/(f, g).$$

Από τον αλγόριθμο διαίρεσης παίρνουμε ότι όλα τα στοιχεία του $\Lambda_{\mathcal{O}}$ είναι ισοδύναμα modulo (π^n, f) σε πολυώνυμα βαθμού μικρότερου του f με συντελεστές modulo π^n. Ξεκάθαρα, έχουμε πεπερασμένες το πλήθος επιλογές για αυτά τα πολυώνυμα πεπερασμένου βαθμού, άρα το (π^n, f) έχει πεπερασμένο δείκτη και συνεπώς ισχύει το ίδιο και για το (f, g). □

Λήμμα 4.8. *Αν R δακτύλιος της Noether τότε είναι της Noether και ο δακτύλιος $R[[X]]$.*

Απόδειξη. Μιμούμαστε την απόδειξη του θεωρήματος βάσης του Hilbert ότι αν R δακτύλιος της Noether, τότε θα είναι και ο δακτύλιος $R[X]$, ωστόσο με μια διαφοροποίηση. Καθώς ένα στοιχείο θα γράφεται ως $f = a_r X^r + a_{r+1}X^{r+1} + \cdots$ και δεν υπάρχει μεγιστοβάθμιος όρος θα θεωρούμε για την συγκεκριμένη απόδειξη βαθμό του f την μικρότερη δύναμη r που εμφανίζεται με κύριο συντελεστή $a_r \neq 0$. Αν $f = 0$, λέμε ότι ο βαθμός είναι άπειρος και ο κύριος συντελεστής να είναι το 0.

Έστω I ένα ιδεώδες του $R[[X]]$, όπου θα δείξουμε ότι είναι πεπερασμένα παραγόμενο. Θα κατασκευάσουμε επαγωγικά μια ακολουθία στοιχείων $f_i \in R[[X]]$ ως εξής. Έστω f_1 με ελάχιστο βαθμό ανάμεσα στα στοιχεία του I. Υποθέτουμε ότι έχουμε διαλέξει $f_1, \ldots, f_i$ με τα f_j να έχουν βαθμό d_j και κύριο συντελεστή a_j. Τότε διαλέγουμε το f_{i+1} ώστε να ικανοποιεί τις ακόλουθες τρεις συνθήκες:

(1) $f_{i+1} \in I$.

(2) $a_{i+1} \notin (a_1, \ldots, a_i)$.

(3) Από όλα τα στοιχεία που ικανοποιούν τις πρώτες δύο συνθήκες, το f_{i+1} να έχει ελάχιστο βαθμό.

Η δεύτερη συνθήκη αναγκάζει την διαδικασία να τερματίσει σε πεπερασμένα βήματα, διαφορετικά θα υπήρχε άπειρη γνήσια αύξουσα αλυσίδα

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

ιδεωδών στον δακτύλιο R που είναι της Noether. Υποθέτουμε ότι η παραπάνω ακολουθία τερματίζει στο βήμα k, έτσι θα δείξουμε ότι το I παράγεται από τα $f_1, \ldots, f_k$.

Έστω $g = aX^d + \cdots$ να είναι ένα στοιχείο του I βαθμού d με κύριο συντελεστή το a. Τότε $a \in (a_1, \ldots, a_k)$, αφού αν δεν άνηκε θα συνέχιζε την προηγούμενη διαδικασία.

Περίπτωση 1: $d \geq d_k$. Έχουμε $d_i \leq d_{i+1}$ για κάθε i, εφόσον έχουν οριστεί τα d_i με αυτή τη σειρά λόγω της συνθήκης (3) και άρα $d \geq d_i$ για κάθε $i = 1, \ldots, k$. Έστω ότι $a = \sum_{i=1}^{k} c_{i0} a_i$ με $c_{i0} \in R$. Ορίζουμε

$$g_0 = \sum_{i=1}^{k} c_{i0} X^{d-d_i} f_i$$

έτσι ώστε το g_0 να έχει βαθμό d και κύριο συντελεστή a. Συνεπώς, το $g - g_0$ θα έχει βαθμό μεγαλύτερο του d. Έχοντας με την ίδια διαδικασία ορίσει $g_0, \ldots, g_r \in (f_1, \ldots, f_k)$ έτσι ώστε το $g - \sum_{i=0}^{r} g_i$ να έχει βαθμό μεγαλύτερο του $d + r$, μπορούμε να υποθέσουμε ότι

$$g - \sum_{i=0}^{r} g_i = bX^{d+r+1} + \cdots$$

όπου φυσικά το επιχείρημα παραμένει το ίδιο για βαθμό μεγαλύτερο του $d+r+1$. Έχουμε για τον ίδιο λόγο με πριν ότι $b \in (a_1, \ldots, a_k)$ και άρα

$$b = \sum_{i=1}^{k} c_{i,r+1} a_i$$

με τα $c_{i,r+1}$ να ανήκουν στο R. Ορίζουμε

$$g_{r+1} = \sum_{i=1}^{k} c_{i,r+1} X^{d+r+1-d_i} f_i$$

έτσι ώστε το $g - \sum_{i=0}^{r} g_i$ να έχει βαθμό μεγαλύτερο του $d + r + 1$. Συνεπώς,

$$g = \sum_{r=0}^{\infty} g_r = \sum_{r=0}^{\infty} \sum_{i=1}^{k} c_{ir} X^{d+r-d_i} f_i$$

και από αυτό έπεται ότι $g \in (f_1, \ldots, f_k)$, εφόσον μπορούμε να αλλάξουμε την σειρά άθροισης καθώς στην μια περίπτωση είναι πεπερασμένο το πλήθος.

Περίπτωση 2: $d < d_k$. Όπως πριν, $a \in (a_1, \ldots, a_k)$ και άρα υπάρχει ένα ελάχιστο m μεταξύ του 1 και του k έτσι ώστε $a \in (a_1, \ldots, a_m)$. Έπεται ότι $d \geq d_m$. Όπως στην πρώτη περίπτωση έχουμε $a = \sum_{i=1}^{m} c_i a_i$ με $c_i \in R$. Ορίζουμε

$$h = \sum_{i=1}^{m} c_i X^{d-d_i} f_i \ \in (f_1, \ldots, f_k) \subseteq I.$$

Ο κύριος συντελεστής του h είναι το a, άρα ο βαθμός του $g-h$ είναι μεγαλύτερος του d. Αντικαθιστούμε το g με το $g-h$ και επαναλαμβάνουμε την διαδικασία. Έτσι, μετά από το πολύ d_k-d βήματα θα έχουμε κατασκευάσει ένα στοιχείο $g-\sum h_i$ στο I βαθμού τουλάχιστον d_k, με όλα τα h_i να είναι στο $(f_1,\dots,f_k)$. Έτσι, από την ανάλυση που κάναμε στην πρώτη περίπτωση, θα έχουμε ότι $g\in(f_1,\dots,f_k)$. □

Πόρισμα 4.9. *Ο δακτύλιος $\Lambda_{\mathcal{O}}$ είναι δακτύλιος της Noether.*

Απόδειξη. Ο δακτύλιος $\mathcal{O}$ είναι περιοχή του Dedekind και άρα δακτύλιος της Noether, συνεπώς εφαρμόζεται το προηγούμενο λήμμα. □

Παρακάτω θα χρειαστούμε ότι για ένα distinguished πολυώνυμο P, το P^n θα τείνει στο 0 στην τοπολογία του $\Lambda_{\mathcal{O}}$. Αυτό θα γίνει πιο ξεκάθαρο με το θεώρημα τομής του Krull, οπότε εφόσον είδαμε ότι το $\Lambda_{\mathcal{O}}$ είναι δακτύλιος της Noether θα κατηγοριοποιήσουμε στην συνέχεια τα πρώτα και μέγιστα ιδεώδη.

Πρόταση 4.10. *Οι πρώτοι του $\Lambda_{\mathcal{O}}$ είναι οι $0,(\pi,T),(\pi)$ και τα ιδεώδη $(P(T))$ όπου $P(T)$ είναι ανάγωγο distinguished πολυώνυμο. Το ιδεώδες (π,T) είναι το μοναδικό μέγιστο.*

Απόδειξη. Έχουμε τους ισομορφισμούς:

$$\begin{aligned}\Lambda_{\mathcal{O}}/(\pi,T)&\cong\mathcal{O}/(\pi)\\ \Lambda_{\mathcal{O}}/(\pi)&\cong(\mathcal{O}/(\pi))[[T]]\\ \Lambda_{\mathcal{O}}/(P(T))&\cong\mathcal{O}[T]/(P(T))\\ \Lambda_{\mathcal{O}}/0&\cong\Lambda_{\mathcal{O}},\end{aligned}$$

όπου το πρώτο είναι πεπερασμένο σώμα και τα υπόλοιπα είναι ακέραιες περιοχές. Άρα αρκεί να δείξουμε ότι κάθε πρώτος στο $\Lambda_{\mathcal{O}}$ είναι σε μία από αυτές τις μορφές. Έστω $\mathfrak{q}\subset\Lambda_{\mathcal{O}}$ ένα μη μηδενικό πρώτο ιδεώδες. Έστω $h\in\mathfrak{q}$ με ελάχιστο βαθμό. Από το θεώρημα προπαρασκευής του Weierstrass γράφουμε $h=\pi^nH$ με $H=1$ ή $H\in\mathfrak{q}$. Αν $H=1$, τότε δεν μπορούμε να έχουμε $H\in\mathfrak{q}$ καθώς τότε $\mathfrak{q}=\Lambda_{\mathcal{O}}$. Υποθέτουμε ότι $H\neq1$ και $H\in\mathfrak{q}$. Έτσι, το H πρέπει να είναι ανάγωγο από την υπόθεση ελαχίστου βαθμού που κάναμε για το h. Συνεπώς, $(H)\subseteq\mathfrak{q}$. Αν $(H)=\mathfrak{q}$ δεν έχουμε κάτι να δείξουμε. Άρα υποθέτουμε ότι $(H)\neq\mathfrak{q}$, δηλαδή υπάρχει $g\in\mathfrak{q}$ με $H\nmid g$. Καθώς το H είναι ανάγωγο, έχουμε αναγκαστικά ότι τα H,g είναι σχετικά πρώτα. Συνεπώς από το λήμμα 4.7 έχουμε ότι το (H,g), άρα και το $\mathfrak{q}$ έχουν πεπερασμένο δείκτη στο $\Lambda_{\mathcal{O}}$. Έχουμε ότι το $\Lambda_{\mathcal{O}}/\mathfrak{q}$ είναι ένα πεπερασμένο $\mathcal{O}$-πρότυπο και άρα $\pi^N\in\mathfrak{q}$ για αρκετά μεγάλο N. Καθώς το $\mathfrak{q}$ είναι πρώτο έπεται ότι $\pi\in\mathfrak{q}$. Για τον ίδιο λόγο έχουμε ότι θα υπάρχουν $i<j$ με $T^i\equiv T^j(\operatorname{mod}\mathfrak{q})$. Επιπλέον, το $1-T^{j-i}$ είναι αντιστρέψιμο εφόσον έχει αντιστρέψιμο σταθερό όρο. Άρα από την παρακάτω σχέση

$$T^i(1-T^{j-i})\equiv0(\operatorname{mod}\mathfrak{q})$$

παίρνουμε ότι $T^i\in\mathfrak{q}$, άρα και $T\in\mathfrak{q}$. Δείξαμε ότι $(\pi,T)\subseteq\mathfrak{q}$, ωστόσο το (π,T) είναι μέγιστο και άρα $\mathfrak{q}=(\pi,T)$. Χρησιμοποιούμε το ίδιο επιχείρημα για την περίπτωση που $H=1$ και $\pi^n\in\mathfrak{q}$. Έτσι, όλοι οι πρώτοι περιέχονται στο (π,T), άρα ο δακτύλιος $\Lambda_{\mathcal{O}}$ είναι τοπικός. □

Από τα προηγούμενα, για τον τοπικό δακτύλιο $\Lambda_{\mathcal{O}}$ της Noether με μέγιστο ιδεώδες (π,T) ισχύει από το θεώρημα τομής του Krull ότι

$$\bigcap_{n=1}^{\infty}(\pi,T)^n=0.$$

Έτσι, για ένα distinguished πολυώνυμο

$$P(T)=T^n+a_{n-1}T^{n-1}+\cdots+a_1T+a_0,\quad a_i\in(\pi)$$

έχουμε ότι $P^k\in(\pi,T)^k$ και η ακολουθία των ιδεωδών είναι προφανώς φθίνουσα, συνεπώς:

$$\text{καθώς } k \longrightarrow \infty, \quad P^k \in \bigcap_{n=1}^{\infty} (\pi, T)^n = 0$$

δηλαδή, με αυτή την έννοια $P^k \longrightarrow 0$ στο $\Lambda_{\mathcal{O}}$. Αυτό είναι ιδιαίτερα χρήσιμο όπως θα φανεί στο επόμενο λήμμα.

Λήμμα 4.11. *Έστω $f, g \in \Lambda_{\mathcal{O}}$ να είναι σχετικά πρώτα. Τότε*

(1) *Η φυσική απεικόνιση*
$$\Lambda_{\mathcal{O}}/(fg) \longrightarrow \Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g)$$
είναι μονομορφισμός με πεπερασμένο συνπυρήνα.

(2) *Υπάρχει εμφύτευση*
$$\Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g) \longrightarrow \Lambda_{\mathcal{O}}/(fg)$$
με πεπερασμένο συνπυρήνα.

Απόδειξη. (1) Έστω h να ανήκει στον πυρήνα της απεικόνισης, τότε $f \mid h$ και $g \mid h$. Αυτά είναι σχετικά πρώτα και καθώς το $\Lambda_{\mathcal{O}}$ είναι περιοχή μοναδικής παραγοντοποίησης θα εμφανίζεται το fg στην ανάλυση του h σε πρώτους. Για τον συνπυρήνα, θεωρούμε ένα στοιχείο $(a(\mathrm{mod}\, f), b(\mathrm{mod}\, g))$. Υποθέτουμε ότι $a - b \in (f, g)$. Τότε υπάρχουν c, d έτσι ώστε
$$a - b = fc + gd.$$
Θέτουμε $\gamma = a - fc = b + gd$ και παρατηρούμε ότι
$$\gamma \equiv a(\mathrm{mod}\, f), \quad \gamma \equiv b(\mathrm{mod}\, g).$$
Άρα το γ είναι στην εικόνα της απεικόνισης. Έστω $r_1, \ldots, r_n$ να είναι αντιπρόσωποι του πεπερασμένου όπως δείξαμε $\Lambda_{\mathcal{O}}/(f, g)$. Τότε έχουμε ότι το σύνολο
$$\{(0(\mathrm{mod}\, f), r_i(\mathrm{mod}\, g)) : \ 1 \leq i \leq n\}$$
είναι ένα σύνολο αντιπροσώπων του συνπυρήνα της απεικόνισης.

(2) Θέτουμε $M = \Lambda_{\mathcal{O}}/(fg)$ και $N = \Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g)$. Ξέρουμε ότι $M \subseteq N$ με πεπερασμένο δείκτη όπως δείξαμε στο (1). Έστω P ένα distinguished πολυώνυμο στο $\Lambda_{\mathcal{O}}$ σχετικά πρώτο με το fg. Καθώς έχουμε $P^k \to 0$ στο $\Lambda_{\mathcal{O}}$, ισχύει ότι $P^k N \subseteq M$ για κάποιο k. Υποθέτουμε ότι $(P^k x, P^k y) = 0$ στο N για κάποιο $(x, y) \in N$. Θα ισχύει ότι $f \mid P^k x$ και $g \mid P^k y$. Έχοντας διαλέξει P έτσι ώστε $\gcd(P, fg) = 1$, έχουμε αναγκαστικά ότι $f \mid x$ και $g \mid y$. Συνεπώς, $(x, y) = 0$ στο N. Άρα, η παρακάτω απεικόνιση είναι εμφύτευση:
$$N \xrightarrow{P^k} M$$
Η εικόνα αυτής της απεικόνισης περιέχει και το $(P^k \cdot 1, P^k \cdot 0) = (P^k, 0) = (P^k, fg)$, το οποίο σαν ιδεώδες είναι πεπερασμένου δείκτη όπως έχουμε δείξει, εφόσον τα P, fg είναι σχετικά πρώτα. Συνεπώς
$$\mathrm{Im}(P^k) \supseteq (P^k, fg)$$
$$\Lambda_{\mathcal{O}}/\mathrm{Im}(P^k) \subseteq \Lambda_{\mathcal{O}}/(P^k, fg)$$
και άρα ο συνπυρήνας έχει πεπερασμένο δείκτη.

□

Λήμμα 4.12. *Έστω $f \in \Lambda_{\mathcal{O}} - \Lambda_{\mathcal{O}}^{\times}$. Τότε το $\Lambda_{\mathcal{O}}/(f)$ έχει άπειρη τάξη.*

Απόδειξη. Υποθέτουμε ότι $f \neq 0$. Από το θεώρημα προπαρασκευής του Weierstrass γράφουμε $f = \pi^n H$ με $H = 1$ ή distinguished. Παρατηρούμε ότι $(f) \subseteq (\pi)$ ή $(f) \subseteq (H)$ και άρα αρκεί να θεωρήσουμε τις περιπτώσεις $f = \pi$ ή f να είναι distinguished πολυώνυμο. Στην δεύτερη περίπτωση παίρνουμε το αποτέλεσμα με εφαρμογή του αλγόριθμου διαίρεσης, εφόσον θα έχουμε για αντιπροσώπους πολυώνυμα βαθμού το πολύ $\deg f - 1$ αλλά άπειρο το πλήθος επιλογές για τους συντελεστές. Για την άλλη περίπτωση, αν $f = \pi$ τότε $\Lambda_{\mathcal{O}}/(\pi) \cong (\mathcal{O}/\pi)[[T]]$ το οποίο είναι άπειρης τάξης. □

Ορισμός 4.13. *Δύο $\Lambda_{\mathcal{O}}$-πρότυπα M και N θα λέγονται ψευδο-ισόμορφα και θα τα γράφουμε $M \sim N$, αν υπάρχει ακριβής ακολουθία:*

$$0 \longrightarrow A \longrightarrow M \longrightarrow N \longrightarrow B \longrightarrow 0$$

όπου τα A, B είναι πεπερασμένα $\Lambda_{\mathcal{O}}$-πρότυπα.

Ο παραπάνω ορισμός είναι ισοδύναμος με το να υπάρχει ομομορφισμός $\Lambda_{\mathcal{O}}$-προτύπων $M \longrightarrow N$ με πεπερασμένο πυρήνα και συνπυρήνα. Εδώ φαίνεται καλύτερα ότι η σχέση $M \sim N$ δεν συνεπάγεται στο ότι $N \sim M$. Πράγματι, έχουμε την ακριβή ακολουθία:

$$0 \longrightarrow (\pi, T) \longrightarrow \Lambda_{\mathcal{O}} \longrightarrow \mathcal{O}/(\pi) \longrightarrow 0$$

και άρα $(\pi, T) \sim \Lambda_{\mathcal{O}}$. Ωστόσο, δεν ισχύει το αντίστροφο. Αν είχαμε $\Lambda_{\mathcal{O}} \sim (\pi, T)$ δηλαδή έναν ομομορφισμό τ έτσι ώστε η παρακάτω ακολουθία να είναι ακριβής:

$$0 \longrightarrow \ker \tau \longrightarrow \Lambda_{\mathcal{O}} \xrightarrow{\tau} (\pi, T) \longrightarrow \operatorname{coker} \tau \longrightarrow 0$$

$$1 \longmapsto f(T)$$

Τότε $\tau(\Lambda_{\mathcal{O}}) = (f) \subseteq (\pi, T)$, όπου το f προφανώς δεν μπορεί να είναι αντιστρέψιμο μέσα στο (π, T). Άρα το $\Lambda_{\mathcal{O}}/(f)$ είναι άπειρης τάξης και συνεπώς το υποπρότυπό του $(\pi, T)/(f) = \operatorname{coker} \tau$ είναι άπειρης τάξης. Άρα δεν μπορούμε να έχουμε $\Lambda_{\mathcal{O}} \sim (\pi, T)$. Ωστόσο, η σχέση $\sim$ είναι συμμετρική όταν μιλάμε για $\Lambda_{\mathcal{O}}$-πρότυπα $\Lambda_{\mathcal{O}}$-στρέψης.

Θεώρημα 4.14 (Δομής Πεπερασμένα Παραγόμενων $\Lambda_{\mathcal{O}}$-Προτύπων)**.** *Έστω M ένα πεπερασμένα παραγόμενο $\Lambda_{\mathcal{O}}$-πρότυπο. Τότε*

$$M \sim \Lambda_{\mathcal{O}}^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda_{\mathcal{O}}/(\pi^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda_{\mathcal{O}}/(f_j(T)^{m_j}) \right)$$

όπου τα r, s, t, n_i και m_j ανήκουν στο $\mathbb{Z}$ και τα $f_j(T)$ είναι distinguished και ανάγωγα πολυώνυμα. Αυτή η διάσπαση καθορίζεται πλήρως από το M.

Απόδειξη. Το αποτέλεσμα αυτό είναι ίδιο με την διάσπαση προτύπων πάνω από περιοχές κυρίων ιδεωδών, με την διαφοροποίηση ότι εδώ έχουμε ψευδο-ισομορφισμούς. Η απόδειξη θα είναι μια γενίκευση των τεχνικών που χρησιμοποιήθηκαν σε εκείνο το θεώρημα.

Έστω M με γεννήτορες $u_1, \ldots, u_n$ με διάφορες σχέσεις

$$\lambda_1 u_1, \ldots, \lambda_n u_n = 0, \quad \lambda_i \in \Lambda_{\mathcal{O}}$$

Καθώς οι σχέσεις R είναι υποπρότυπο του $\Lambda_{\mathcal{O}}^n$ και το $\Lambda_{\mathcal{O}}$ είναι της Noether, το R είναι πεπερασμένα παραγόμενο. Άρα μπορούμε να γράφουμε το M σαν πίνακα με γραμμές της μορφής $(\lambda_1, \ldots, \lambda_n)$, όπου $\sum \lambda_i u_i = 0$ να είναι μια σχέση. Υπερφορτώνοντας τον συμβολισμό, θα λέμε αυτόν τον πίνακα R.

Ξεκινάμε με τις βασικές πράξεις γραμμών και στηλών, οι οποίες αντιστοιχούν στην αλλαγή των γεννητόρων των R και M.
Πράξη A. Μπορούμε να εναλλάσουμε τις γραμμές μεταξύ τους ή να εναλλάσουμε τις στήλες μεταξύ τους.
Πράξη B. Μπορούμε να προσθέσουμε ένα πολλαπλάσιο μιας γραμμής (ή στήλης) σε μια άλλη γραμμή (ή στήλη). Ειδική περίπτωση αν $\lambda' = q\lambda + r$ τότε

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \longrightarrow \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}$$

Πράξη C. Μπορούμε να πολλαπλασιάσουμε μια γραμμή ή στήλη με στοιχείο του $\Lambda_{\mathcal{O}}^{\times}$.
Οι παραπάνω πράξεις είναι αυτές που χρησιμοποιούνται στις περιοχές κυρίων ιδεωδών. Ωστόσο, έχουμε άλλες τρεις επιπλέον πράξεις που βασίζονται στους ψευδο-ισομορφισμούς.
Πράξη 1. Αν το R περιέχει γραμμή $(\lambda_1, \pi\lambda_2, \ldots, \pi\lambda_n)$ με $\pi \nmid \lambda_1$, τότε μπορούμε να αλλάξουμε τον R στον R', του οποίου η πρώτη γραμμή είναι $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ και οι υπόλοιπες γραμμές είναι οι γραμμές του R, όπου η πρώτη στήλη είναι πολλαπλασιασμένη με π. Εικονικά:

$$\begin{pmatrix} \lambda_1 & \pi\lambda_2 & \cdots \\ a_1 & a_2 & \cdots \\ b_1 & b_2 & \cdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ \pi a_1 & a_2 & \cdots \\ \pi b_1 & b_2 & \cdots \end{pmatrix}$$

Ως ειδική περίπτωση, αν $\lambda_2 = \cdots = \lambda_n = 0$ τότε μπορούμε να πολλαπλασιάσουμε τα $a_1, b_1, \ldots$ με οποιαδήποτε δύναμη του π.

Απόδειξη. Στο R έχουμε την σχέση

$$\lambda_1 u_1 + \pi(\lambda_2 u_2 + \cdots + \lambda_n u_n) = 0.$$

Έστω $M' = M \oplus \nu\Lambda_{\mathcal{O}}$, με έναν καινούργιο γεννήτορα ν όπου ισχύουν οι σχέσεις

$$(-u_1, \pi\nu) = 0, \quad (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 \nu) = 0.$$

Υπάρχει φυσική απεικόνιση $M \to M'$. Υποθέτουμε ότι $m \mapsto 0$. Τότε το m θα ανήκει στο πρότυπο των σχέσεων, οπότε

$$(m, 0) = a(-u_1, \pi\nu) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 \nu)$$

με τα a, b να είναι στο $\Lambda_{\mathcal{O}}$. Συνεπώς

$$a\pi = -b\lambda_1.$$

Καθώς $\pi \nmid \lambda_1$ από την υπόθεση, έχουμε ότι $\pi \mid b$. Επιπλέον, $\lambda_1 \mid a$. Άρα στην M-συνιστώσα έχουμε

$$\begin{aligned} m &= -\frac{a}{\lambda_1}(\lambda_1 u_1) - \frac{a}{\lambda_1}\pi(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\frac{a}{\lambda_1}(0) = 0. \end{aligned}$$

Καθώς οι εικόνες των $\pi\nu$ και $\lambda_1\nu$ στο M' είναι στην εικόνα του M, το ιδεώδες (π, λ_1) μηδενίζει το M'/M. Εφόσον το $\Lambda_{\mathcal{O}}/(\pi, \lambda_1)$ είναι πεπερασμένο και το M' πεπερασμένα παραγόμενο, το M'/M θα είναι πεπερασμένο. Συνεπώς

$$M \sim M'.$$

Το νέο πρότυπο M' έχει γεννήτορες $\nu, u_2, \ldots, u_n$. Κάθε σχέση $a_1 u_1 + \cdots a_n u_n = 0$ γίνεται $\pi a_1 \nu + \cdots + a_n u_n = 0$. Άρα η πρώτη στήλη έχει πολλαπλασιαστεί με το π. Επιπλέον, έχουμε την σχέση $\lambda_1\nu + \cdots + \lambda_n u_n$. Άρα ο νέος πίνακας R' έχει την μορφή που αναφέραμε. □

Πράξη 2. Αν όλα τα στοιχεία στην πρώτη στήλη του R διαιρούνται από το π^k και αν υπάρχει γραμμή $(\pi^k\lambda_1, \ldots, \pi^k\lambda_n)$ με $\pi \nmid \lambda_1$, τότε μπορούμε να αλλάξουμε τον πίνακα στον R' που είναι ο ίδιος με τον R, αλλά στην θέση της γραμμής $(\pi^k\lambda_1, \ldots, \pi^k\lambda_n)$ μπαίνει η γραμμή $(\lambda_1, \ldots, \lambda_n)$. Εικονικά:

$$\begin{pmatrix} \pi^k\lambda_1 & \pi^k\lambda_2 & \cdots \\ \pi^k a_1 & a_2 & \cdots \end{pmatrix} \longrightarrow \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ \pi^k a_1 & a_2 & \cdots \end{pmatrix}.$$

Απόδειξη. Έστω $M' = M \oplus \Lambda_{\mathcal{O}}\nu$ όπου ισχύουν οι σχέσεις

$$(\pi^k u_1, -\pi^k \nu) = 0, \quad (\lambda_2 u_2 + \cdots \lambda_n u_n, \lambda_1 \nu) = 0.$$

Όπως και πριν, το ότι $\pi \nmid \lambda_1$ μας επιτρέπει να πούμε ότι το M εμφυτεύεται στο M'. Επιπλέον, το ιδεώδες (π^k, λ_1) μηδενίζει το M'/M, οπότε το πηλίκο αυτό είναι πεπερασμένο. Συνεπώς $M \sim M'$.

Χρησιμοποιώντας το γεγονός ότι $\pi^k(u_1 - \nu) = 0$ και το ότι το π^k διαιρεί τον πρώτο συντελεστή από όλες τις σχέσεις που περιέχουν το u_1, παίρνουμε ότι

$$M' = M'' \oplus (u_1 - \nu)\Lambda_{\mathcal{O}}$$

όπου το M'' παράγεται από τα $\nu, u_1, \ldots, u_n$ και έχει σχέσεις που παράγονται από τα $(\lambda_1, \ldots, \lambda_n)$ και R. Συνεπώς το M'' έχει το R' ως τις σχέσεις του. Παρατηρούμε ότι

$$(u_1 - \nu)\Lambda_{\mathcal{O}} \cong \Lambda_{\mathcal{O}}/(\pi^k)$$

το οποίο είναι ήδη στην μορφή που θέλουμε. Άρα αρκεί να δουλέψουμε με τα M'' και R'. □

Πράξη 3. Αν το R περιέχει γραμμή $(\pi^k\lambda_1, \ldots, \pi^k\lambda_n)$ και για κάποιο $\lambda \in \Lambda_{\mathcal{O}}$ με $\pi \nmid \lambda$ η γραμμή $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ να είναι σχέση (όχι απαραίτητα γραμμή του R), τότε μπορούμε να αλλάξουμε το R με το R' που είναι το ίδιο εκτός από την γραμμή $(p^k\lambda_1, \ldots, \pi^k\lambda_n)$ που θα αντικατασταθεί με την $(\lambda_1, \ldots, \lambda_n)$.

Απόδειξη. Θεωρούμε τον επιμορφισμό:

$$M \longrightarrow M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda_{\mathcal{O}},$$

του οποίου ο πυρήνας μηδενίζεται από το ιδεώδες (λ, π^k). Καθώς το M, άρα ως Noether και ο πυρήνας, είναι πεπερασμένα παραγόμενα μαζί με το πεπερασμένο $\Lambda_{\mathcal{O}}/(\lambda, \pi)$, έχουμε ότι ο πυρήνας είναι πεπερασμένος. Άρα $M \sim M'$ και το M' έχει το R' ως πίνακα σχέσεων. □

Αυτές οι έξι A,B,C,1,2,3 είναι οι επιτρεπτές πράξεις μας, οι οποίες διατηρούν το μέγεθος του πίνακα. Είμαστε σε θέση να ξεκινήσουμε. Έστω $f \neq 0 \in \Lambda_{\mathcal{O}}$, τότε

$$f(T) = \pi^\mu P(T)U(T),$$

με P distinguished πολυώνυμο και $U \in \Lambda_{\mathcal{O}}^\times$. Έστω

$$\deg_w f = \begin{cases} \infty, & \mu > 0 \\ \deg P(T), & \mu = 0 \end{cases}$$

το οποίο αναφέρεται ως ο βαθμός Weierstrass του f. Δεδομένου ενός πίνακα R, ορίζουμε

$$\deg^{(k)}(R) = \min \deg_w(a'_{ij}) \quad \text{για } i, j \geq k,$$

όπου τα (a'_{ij}) διατρέχουν όλους τους πίνακες σχέσεων που παίρνουμε από το R μέσω των επιτρεπτών πράξεων, οι οποίες αφήνουν αναλλοίωτες τις πρώτες $(k-1)$ γραμμές. Αν ο πίνακας R έχει τη μορφή

$$\begin{pmatrix} \lambda_{11} & & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

με λ_{kk} να είναι distinguished και

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)}(R) \quad \text{για } 1 \le k \le r-1$$

τότε λέμε ότι ο R είναι σε $(r-1)$-κανονική μορφή.

Ισχυρισμός. Αν ο υποπίνακας B δεν είναι ο μηδενικός, τότε το R μπορεί μέσω των επιτρεπτών πράξεων να μετατραπεί στον R' ο οποίος είναι σε r-κανονική μορφή και έχει τα ίδια πρώτα $(r-1)$ διαγώνια στοιχεία.

Απόδειξη. Η ειδική περίπτωση στην πράξη 1 μας επιτρέπει να υποθέτουμε, όταν χρειάζεται ότι μια μεγάλη δύναμη του π διαιρεί κάθε λ_{ij} με $i \ge r$ και $j \le r-1$. Δηλαδή, $\pi^N \mid A$, με N αρκετά μεγάλο ώστε $\pi^N \nmid B$. Χρησιμοποιώντας την πράξη 2, υποθέτουμε ότι $\pi \nmid B$. Μπορούμε να υποθέσουμε ότι το B περιέχει στοιχείο λ_{ij} τέτοιο ώστε

$$\deg_w \lambda_{ij} = \deg^{(r)}(R) < \infty.$$

Αν $\lambda_{ij} = P(T)U(T)$, τότε πολλαπλασιάζουμε την j-οστή στήλη με το U^{-1}. Συνεπώς, μπορούμε να υποθέσουμε ότι το λ_{ij} είναι distinguished, εφόσον οι πρώτες $r-1$ γραμμές έχουν το 0 στην j-οστή στήλη και άρα δεν θα αλλάξουν. Λόγω της πράξης Α μπορούμε να υποθέσουμε ότι $\lambda_{ij} = \lambda_{rr}$ (όπου πάλι τα μηδενικά μας βοηθάνε). Από τον αλγόριθμο διαίρεσης (ειδική περίπτωση της πράξης Β), μπορούμε να υποθέσουμε ότι το λ_{rj} είναι πολυώνυμο με

$$\deg \lambda_{rj} < \deg \lambda_{rr}, \quad j \ne r$$

και

$$\deg \lambda_{rj} < \deg \lambda_{jj}, \quad j < r$$

Καθώς το λ_{rr} έχει ελάχιστο βαθμό Weierstrass στο B, έχουμε αναγκαστικά ότι $\pi \mid \lambda_{rj}$ για τα $j > r$. Από την πράξη 1, υποθέτουμε ότι $\pi^N \mid \lambda_{rj}, j < r$, για κάποιο μεγάλο N. Υποθέτουμε ότι $\lambda_{rj} \ne 0$ για κάποιο $j > r$. Η πράξη 1 μας επιτρέπει εδώ να διώξουμε την δύναμη του π από κάποιο μη μηδενικό λ_{rj} με $j > r$ (με τα μηδενικά από πάνω να μείνουν αναλλοίωτα). Τότε

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg_w \lambda_{rr}$$

το οποίο είναι άτοπο. Συνεπώς, $\lambda_{rj} = 0$ για $j > r$. Αν κάποιο λ_{rj} δεν είναι 0 για $j < r$, χρησιμοποιούμε την πράξη 1 για να πάρουμε ότι $\pi \nmid \lambda_{rj}$ για κάποιο j. Ωστόσο, τότε θα έχουμε

$$\deg_w \lambda_{rj} \le \deg \lambda_{rj} < \deg \lambda_{jj} = \deg_w \lambda_{jj}$$

και καθώς

$$\deg_w \lambda_{jj} = \deg^{(j)}(R)$$

αυτό έρχεται σε αντίθεση με τον ορισμό του $\deg^{(j)}(R)$. Συνεπώς, $\lambda_{rj} = 0$ για κάθε $j \ne r$. Αυτό αποδεικνύει τον ισχυρισμό. □

Αν ξεκινήσουμε με έναν πίνακα R και $r = 1$, μπορούμε μέσω των πράξεων να αλλάξουμε τον R μέχρι να πάρουμε έναν πίνακα

$$\begin{pmatrix} \lambda_{11} & & & 0 \\ & \ddots & & \\ & & \lambda_{rr} & \\ A & & & 0 \end{pmatrix},$$

με κάθε λ_{jj} να είναι distinguished και $\deg \lambda_{jj} = \deg^{(j)}(R)$ για κάθε $j \leq r$. Από τον αλγόριθμο διαίρεσης, μπορούμε να υποθέσουμε ότι το λ_{ij} είναι πολυώνυμο και

$$\deg \lambda_{ij} < \deg \lambda_{jj}, \quad \text{για } i \neq j.$$

Υποθέτουμε ότι $\lambda_{ij} \neq 0$ για κάποια $i \neq j$. Καθώς το $\deg_w \lambda_{jj}$ είναι ελάχιστο, το π διαιρεί το λ_{ij}. Άρα έχουμε μια μη μηδενική σχέση $(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$ την οποία διαιρεί το π. Θέτουμε $\lambda = \lambda_{11} \cdots \lambda_{rr}$. Τότε $\pi \nmid \lambda$, εφόσον τα λ_{jj} είναι distinguished και το παρακάτω

$$\left(\lambda\frac{1}{\pi}\lambda_{i1}\ , \ldots, \lambda\frac{1}{\pi}\lambda_{ir}\ , 0, \ldots, 0\right)$$

είναι μια σχέση, καθώς $\lambda_{jj}u_j = 0$. Από την πράξη 3 μπορούμε να υποθέσουμε ότι το π δεν διαιρεί το λ_{ij} για κάποιο j, οπότε

$$\deg_w \lambda_{ij} \leq \deg \lambda_{ij} < \deg \lambda_{jj} = \deg^{(j)}(R)$$

Το οποίο είναι άτοπο. Συνεπώς $\lambda_{ij} = 0$ για κάθε i και j με $i \neq j$. Αυτό σημαίνει ότι $A = 0$. Δηλαδή, σε όρους $\Lambda_{\mathcal{O}}$-προτύπων έχουμε

$$\Lambda_{\mathcal{O}}/(\lambda_{11}) \oplus \cdots \oplus \Lambda_{\mathcal{O}}/(\lambda_{rr}) \oplus \Lambda_{\mathcal{O}}^{n-r}.$$

Ξαναβάζοντας στην παραπάνω γραφή και τους όρους $\Lambda_{\mathcal{O}}/(p^k)$ που αφαιρέσαμε λόγω της πράξης 2, παίρνουμε το επιθυμητό αποτέλεσμα. Μια λεπτομέρεια είναι ότι τα λ_{ii} δεν είναι απαραίτητα ανάγωγα, ωστόσο εδώ έρχεται το λήμμα 4.11 και τακτοποιεί αυτό το πρόβλημα. Εδώ τελειώνει η απόδειξη του θεωρήματος δομής. □

4.3 Θεώρημα Iwasawa

Σε αυτή την ενότητα θα αποδείξουμε το θεώρημα 4.1 του Iwasawa. Θα βασιστούμε πολύ στο θεώρημα δομής που αποδείχτηκε προηγουμένως. Έστω K ένα σώμα αριθμών και K_∞/K μια $\mathbb{Z}_p$-επέκταση με $K = K_0 \subset K_1 \subset \cdots \subset K_\infty$ με $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Γράφουμε ως $\Gamma = \mathrm{Gal}(K_\infty/K)$ και έστω γ_0 ένας τοπολογικός γεννήτορας του Γ, δηλαδή η υποομάδα που παράγει το γ_0 να είναι πυκνή. Έχουμε ότι υπάρχει τέτοιος γεννήτορας καθώς με την ίδια έννοια το 1 είναι πυκνό στο $\mathbb{Z}_p$ που είναι ισόμορφο με το Γ. Ο ισομορφισμός $\mathbb{Z}_p \cong \Gamma$ δίνεται την απεικόνιση $x \longmapsto \gamma_0^x$.

Υπενθυμίζουμε ότι από την θεωρία κλάσεων σωμάτων έχουμε την ύπαρξη της μεγιστικής αδιακλάδιστης αβελιανής επέκτασης H_K/K με τον ισομορφισμό πεπερασμένων ομάδων:

$$\mathrm{Gal}(H_K/K) \cong C_K,$$

όπου C_K είναι η ομάδα κλάσεων ιδεωδών του K. Αν P είναι η p-Sylow υποομάδα της $\mathrm{Gal}(H_K/K)$, η δεύτερη ως αβελιανή θα είναι μηδενοδύναμη και άρα ευθύ γινόμενο των Sylow q-υποομάδων Q για τους υπόλοιπους πρώτους $q \neq p$ που διαιρούν την τάξη του C_K. Από την θεωρία Galois έχουμε ότι:

$$\begin{array}{ccc}
1 & 1 & H_K \\
\Big| {\scriptstyle p^n} & \Big| & \Big| \\
P & \prod\limits_{Q \neq P} Q & H_K^{\prod Q} \\
\Big| & \Big| {\scriptstyle p^n} & \Big| {\scriptstyle p^n} \\
\mathrm{Gal}(H_K/K) & \mathrm{Gal}(H_K/K) & K
\end{array}$$

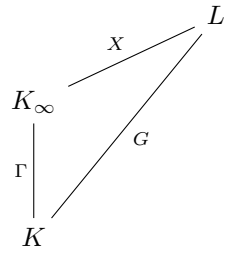
Δηλαδή για το K έχουμε την ύπαρξη της μέγιστης αδιακλάδιστης αβελιανής p-επέκτασης $H_K^{\prod Q}$. Έστω L_n να είναι η μέγιστη αδιακλάδιστη αβελιανή p-επέκταση του K_n. Έχουμε

$$\begin{array}{cc} H_{K_n} & 1 \\ | & | \\ L_n & \mathrm{Gal}(H_{K_n}/L_n) \\ |p^n & |p^n \\ K_n & \mathrm{Gal}(H_{K_n}/K_n) \end{array}$$

και

$$\mathrm{Gal}(H_{K_n}/K_n)/\mathrm{Gal}(H_{K_n}/L_n) \cong \mathrm{Gal}(L_n/K_n)$$

Θέτουμε $X_n = \mathrm{Gal}(L_n/K_n)$ έτσι ώστε από τα παραπάνω το X_n να είναι η p-Sylow υποομάδα της ομάδας κλάσεων του K_n. Αυτό που μας ενδιαφέρει για το θεώρημα του Iwasawa είναι η δύναμη του p που διαιρεί το X_n. Έστω $L = \cup_{n\geq 0} L_n$, $X = \mathrm{Gal}(L/K_\infty)$ και $G = \mathrm{Gal}(L/K)$. Έχουμε το ακόλουθο διάγραμμα σωμάτων με τις αντίστοιχες ομάδες Galois:



Παρατηρούμε ότι για οποιοδήποτε $n \geq 0$ η επέκταση K_∞/K_n παραμένει μια $\mathbb{Z}_p$-επέκταση με το ίδιο X όπως στην περίπτωση του K, εφόσον τα K_m αποτελούν αύξουσα ακολουθία και καθώς $L_m \supset K_m$, θα έχουμε ότι $L = \cup_{m\geq 0} L_m = \cup_{m\geq n} L_n$. Αυτό θα είναι σημαντικό καθώς θέλουμε να εργαστούμε στην περίπτωση που κάθε πρώτος που διακλαδίζεται στην K_∞ να διακλαδίζεται πλήρως. Θα το πετύχουμε αυτό αντικαθιστώντας το K με το K_n για κάποιο n. Καθώς θα πάρουμε αποτελέσματα για το «νέο» X είναι σημαντικό που θα ξέρουμε ότι στην πραγματικότητα παραμένει το ίδιο που μας ενδιαφέρει.

Λήμμα 4.15. *Οι ομάδες διάσπασης και αδράνειας για ομάδα* $\mathrm{Gal}(L/K)$ *είναι κλειστές ως προς την τοπολογία Krull.*

Απόδειξη. Έστω $D_\lambda = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\lambda) \equiv \lambda\}$ για έναν πρώτο λ. Έστω $\sigma \in \overline{D}_\lambda$. Τότε το D_λ τέμνει τις ανοιχτές περιοχές $\sigma\,\mathrm{Gal}(L/M)$ για κάθε πεπερασμένη υποεπέκταση M/K. Διαλέγουμε $\sigma_M \in D_\lambda$ με $\sigma_M = \sigma\tau$ για κάποιο $\tau \in \mathrm{Gal}(L/M)$. Τότε

$$\sigma_M|_M = (\sigma\tau)|_M = \sigma|_{\tau(M)} \circ \tau|_M = \sigma|_M \circ id_M = \sigma|_M.$$

Καθώς $\sigma_M(\lambda) \equiv \lambda$, έχουμε $\sigma|_M(\lambda) \equiv \lambda$ και άρα

$$\sigma|_M(\lambda \cap M) = \sigma_M(\lambda \cap M) = \lambda \cap M.$$

Το L είναι η ένωση όλων των M, συνεπώς για ένα $a \in \lambda$ έχουμε

$$\sigma(a) = \sigma|_{K(a)}(a) \in \lambda \cap K(a) \subseteq \lambda,$$

δηλαδή $\sigma(\lambda) \equiv \lambda$ και άρα $\sigma \in D_\lambda$ οπότε δείξαμε ότι η D_λ είναι κλειστή. Όμοιο είναι το επιχείρημα για αρχιμήδειους πρώτους και αντίστοιχα για την ομάδα αδράνειας. □

Υπενθυμίζουμε ότι για μια άπειρη Galois επέκταση M/N λέμε ότι ένας πρώτος $\mathfrak{p}$ του N διακλαδίζεται πλήρως αν υπάρχει μοναδικός πρώτος $\mathfrak{q}$ του M έτσι ώστε $I_{\mathfrak{q}} = I_{\mathfrak{q}|\mathfrak{p}} = \mathrm{Gal}(M/N)$. Αυτό είναι ισοδύναμο ότι ο $\mathfrak{p}$ είναι πλήρως διακλαδιζόμενος με την συνήθη έννοια σε κάθε πεπερασμένη Galois υποεπέκταση F/N. Πράγματι, αν $I_{\mathfrak{q}} = \mathrm{Gal}(M/N)$ τότε έχουμε τον φυσιολογικό επιμορφισμό:

$$\mathrm{Gal}(M/N) \longrightarrow \mathrm{Gal}(F/N)$$
$$\sigma \longmapsto \sigma|_F$$

και η εικόνα του $I_{\mathfrak{q}}$ είναι η $I(\mathfrak{q} \cap F|\mathfrak{p})$. Λόγω της υπόθεσης και του επιμορφισμού παίρνουμε ότι $|I_{\mathfrak{q}\cap F}| = |\mathrm{Gal}(F/N)| = [F : N]$ άρα ο $\mathfrak{p}$ διακλαδίζεται πλήρως στο F. Για το αντίστροφο, παρατηρούμε αρχικά ότι μπορούμε να περιορίσουμε σε οποιαδήποτε πεπερασμένη υποεπέκταση F/N. Εφόσον η κάθε πεπερασμένη υποεπέκταση περιέχεται σε μια πεπερασμένη Galois F'/N, στην οποία ο $\mathfrak{p}$ θα διακλαδίζεται πλήρως με τον πρώτο $\mathfrak{q}'$ να στέκεται από πάνω. Αρα κοιτάμε τον πρώτο $\mathfrak{q}' \cap F$, δηλαδή για κάθε F/N υποεπέκταση έχουμε έναν πρώτο $\mathfrak{q}_F$ τέτοιο ώστε:

$$\mathfrak{p}\mathcal{O}_F = \mathfrak{q}_F^{[F:N]}$$

άρα, $I(\mathfrak{q}_F|\mathfrak{p}) = \mathrm{Gal}(F/N)$. Θέτουμε ως $\mathfrak{q} := \bigcup_F \mathfrak{q}_F$ ο οποίος είναι ο μοναδικός πρώτος του M που στέκεται πάνω από το $\mathfrak{q}_F$. Έχουμε τον φυσιολογικό τοπολογικό ισομορφισμό ομάδων:

$$I(\mathfrak{q}|\mathfrak{p}) \longrightarrow \varprojlim I(\mathfrak{q}_F|\mathfrak{p})$$
$$\sigma \longmapsto (\sigma|_{F_i})_i$$

και από την υπόθεση ότι $I(\mathfrak{q}_F|\mathfrak{p}) = \mathrm{Gal}(F/N)$ μαζί με το γεγονός ότι $\varprojlim \mathrm{Gal}(F/N) \cong \mathrm{Gal}(M/N)$ και την μοναδικότητα του αντιστρόφου ορίου ως προς ισομορφισμό, παίρνουμε ότι $\mathrm{Gal}(M/N) = I(\mathfrak{q}|\mathfrak{p})$. Μπορούμε λοιπόν να χειριστούμε τώρα τους πλήρως διακλαδιζόμενους πρώτους στην επέκταση K_∞/K όπως γίνεται στις παρακάτω προτάσεις.

Πρόταση 4.16. *Κάθε $\mathbb{Z}_p$-επέκταση είναι αδιακλάδιστη έξω από το p, δηλαδή αν λ είναι ένας πρώτος του K που δεν στέκεται πάνω από το p, τότε η επέκταση K_∞/K είναι αδιακλάδιστη στο λ.*

Απόδειξη. Έστω I_λ να είναι η ομάδα αδράνειας του λ. Η ομάδα αδράνειας είναι κλειστή, άρα ως προς τον ισομορφισμό με το $\mathbb{Z}_p$ έχουμε ότι $I_\lambda = 0$ ή $p^n\mathbb{Z}_p$ για κάποιο n. Αν $I_\lambda = 0$ δεν έχουμε κάτι να δείξουμε. Έστω ότι $I_\lambda = p^n Z_p$ για κάποιο n. Η ομάδα αδράνειας ενός αρχιμήδειου πρώτου έχει τάξη 1 ή 2, ενώ εδώ έχουμε άπειρη τάξη άρα αποκλείουμε την περίπτωση το λ να είναι ένας διακλαδιζόμενος αρχιμήδειος πρώτος. Για κάθε m διαλέγουμε μια θέση λ_m έτσι ώστε το λ_m να στέκεται πάνω από το λ_{m-1} και θέτουμε για βάση $\lambda_0 = \lambda$. Θεωρούμε την πλήρωση του κάθε σώματος K_m ως προς το λ_m και παίρνουμε έναν πύργο σωμάτων:

$$K_\lambda = K_{0,\lambda} \subset K_{1,\lambda_1} \subset K_{2,\lambda_2} \subset \cdots$$

όπου θέτουμε

$$\hat{K}_\infty = \bigcup_{m\geq 0} K_{m,\lambda_m}.$$

Παρατηρούμε ότι $I_\lambda \subset \mathrm{Gal}(\hat{K}_\infty/K_\lambda)$. Έστω U οι μονάδες του K_λ. Από την τοπική θεωρία κλάσεων σωμάτων [15] γνωρίζουμε ότι υπάρχει επιμορφισμός $U \to I_\lambda$, δηλαδή επιμορφισμός $U \to p^n Z_p$. Ωστόσο, από το θεώρημα μονάδων της αλγεβρικής θεωρίας αριθμών έχουμε ότι το U είναι ισομορφο με το ευθύ γινόμενο μιας πεπερασμένης ομάδας επί του $\mathbb{Z}_\ell^a$ για κάποιο $a \in \mathbb{Z}$ και πρώτο $\ell \subset \mathbb{Z}$ με $\lambda \mid \ell$. Ξέρουμε ότι το $p^n\mathbb{Z}_p$ δεν έχει στρέψη, άρα έχουμε έναν συνεχή επιμορφισμό $\mathbb{Z}_\ell^a \to p^n Z_p$. Συνδυάζοντάς το με την φυσική προβολή παίρνουμε έναν συνεχή επιμορφισμό:

$$\mathbb{Z}_\ell^a \longrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$$

Το οποίο σημαίνει ότι έχουμε κλειστό υποσύνολο με δείκτη p στο $\mathbb{Z}_\ell^a$, το οποίο είναι άτοπο. Άρα $I_\lambda = 0$. □

Πρόταση 4.17. *Τουλάχιστον ένας πρώτος διακλαδίζεται στην επέκταση K_∞/K και υπάρχει $m \geq 0$ τέτοιο ώστε κάθε πρώτος που διακλαδίζεται στην επέκταση K_∞/K_m να διακλαδίζεται πλήρως.*

Απόδειξη. Η μέγιστη αδιακλάδιστη επέκταση όπως γνωρίζουμε είναι πεπερασμένη ενώ η K_∞/K είναι άπειρη, άρα τουλάχιστον ένας πρώτος θα διακλαδίζεται. Από την προηγούμενη πρόταση μόνο οι πρώτοι πάνω από το p είναι πιθανό να διακλαδίζονται. Έστω ότι αυτοί οι πρώτοι είναι οι $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ με τις αντίστοιχες ομάδες αδράνειας $I_1, \ldots, I_r$. Εφόσον κάθε I_i είναι κλειστό, ισχύει το ίδιο για το $\cap I_i$. Συνεπώς, υπάρχει ένα $m \in \mathbb{Z}$ τέτοιο ώστε

$$\bigcap I_i = p^m \mathbb{Z}_p.$$

Έχουμε ότι $\mathrm{Gal}(K_m/K) \cong \mathbb{Z}/p^m\mathbb{Z} \cong \mathbb{Z}_p/p^m\mathbb{Z}_p$, άρα έχουμε ότι $\mathrm{Gal}(K_\infty/K_m) \cong p^m\mathbb{Z}_p$ και άρα περιέχεται στο I_i για κάθε $i = 1, \ldots, r$. Συνεπώς, δείξαμε ότι τα $\mathfrak{p}_i$ είναι πλήρως διακλαδιζόμενα στην επέκταση K_∞/K_m για κάθε $i = 1, \ldots, r$.

□

Σταθεροποιούμε τώρα ένα m όπως είναι στην πρόταση 4.17.

Πρόταση 4.18. *Για κάθε $n \geq m$ έχουμε ότι $K_{n+1} \cap L_n = K_n$.*

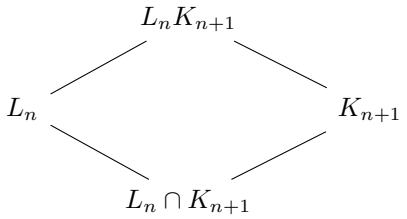
Απόδειξη. Έχουμε ότι $K_n \subseteq L_n \cap K_{n+1}$ άρα αρκεί να δείξουμε ότι η ομάδα $\mathrm{Gal}(L_n \cap K_{n+1}/K_n)$ είναι τετριμμένη. Έχουμε τον φυσιολογικό επιμορφισμό:

$$\mathrm{Gal}(K_\infty/K_n) \longrightarrow \mathrm{Gal}(K_{n+1} \cap L_n/K_n)$$

$$\sigma \longmapsto \sigma|_{K_{n+1} \cap L_n}$$

και ξέρουμε ότι υπάρχει πρώτος $\mathfrak{p}$ που διακλαδίζεται στην επέκταση K_∞/K_n. Καθώς $n \geq m$ αυτός θα διακλαδίζεται πλήρως με έναν μοναδικό πρώτο $\mathfrak{q}$ να στέκεται από πάνω του. Έχουμε ότι $I_\mathfrak{q} = \mathrm{Gal}(K_\infty/K_n)$ και η εικόνα του στον επιμορφισμό είναι η $I(\mathfrak{q} \cap K_{n+1} \cap L_n|\mathfrak{p}) = \mathrm{Gal}(K_{n+1} \cap L_n/K_n)$. Ωστόσο, ο νέος πρώτος $\mathfrak{q} \cap K_{n+1} \cap L_n$ βρίσκεται μέσα στην αδιακλάδιστη επέκταση L_n/K_n, άρα $I_{\mathfrak{q} \cap K_{n+1} \cap L_n} = 1$. □

Προς το παρόν θα θεωρήσουμε ότι $m = 0$. Όπως θα δούμε στην συνέχεια θα μπορούμε να δουλέψουμε και χωρίς αυτήν την υπόθεση, αλλά μέχρι τότε θα μας ευκολύνει στον συμβολισμό. Αυτή η υπόθεση θα ισχύει για τα επόμενα λήμματα μέχρι να αναφέρουμε διαφορετικά. Από την προηγούμενη πρόταση έχουμε τον ισομορφισμό $\mathrm{Gal}(L_nK_{n+1}/K_{n+1}) \cong \mathrm{Gal}(L_n/K_n)$, $\sigma \mapsto \sigma|_{L_n}$ με το διάγραμμα σωμάτων:



Καθώς έχουμε ότι $X_{n+1} = \mathrm{Gal}(L_{n+1}/K_{n+1})$ και $L_nK_{n+1} \subset L_{n+1}$, βλέπουμε ότι η ομάδα $\mathrm{Gal}(L_nK_{n+1}/K_{n+1})$ και άρα το X_n είναι πηλίκο του X_{n+1}. Συνεπώς, έχουμε έναν επιμορφισμό $X_{n+1} \to X_n$. Όμοια, αν πάρουμε το K_∞ αντί για το K_n παραπάνω έχουμε ότι

$$X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$$

και άρα έχουμε

$$\begin{aligned}\varprojlim X_n &= \varprojlim \mathrm{Gal}(L_n/K_n)\\ &\cong \varprojlim \mathrm{Gal}(L_nK_\infty/K_\infty)\\ &\cong \mathrm{Gal}\left(\bigcup (L_nK_\infty)/K_\infty\right)\\ &= \mathrm{Gal}(L/K_\infty)\\ &= X.\end{aligned}$$

Δείξαμε ότι το X είναι το αντίστροφο όριο των ομάδων X_n. Επιπλέον, θέτουμε $\Gamma_n := \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{Gal}(K_n/K)$, όπου η δομή στο Γ_n είναι πολλαπλασιαστική. Έστω $\gamma_n \in \Gamma_n$. Επεκτείνουμε το γ_n σε ένα στοιχείο $\tilde{\gamma}_n \in \mathrm{Gal}(L_n/K)$. Έστω $x_n \in X_n$. Τότε υπάρχει δράση του γ_n στο x_n που δίνεται από την παρακάτω σχέση

$$\gamma_n \cdot x_n = \tilde{\gamma}_n x_n \tilde{\gamma}_n^{-1}.$$

Ωστόσο, πρέπει να δείξουμε ότι η δράση είναι καλά ορισμένη. Αρχικά, έχουμε την ακριβή ακολουθία:

$$0 \longrightarrow \mathrm{Gal}(L_n/K_n) \xhookrightarrow{i} \mathrm{Gal}(L_n/K) \xrightarrow{p} \mathrm{Gal}(K_n/K) \longrightarrow 0$$

δηλαδή

$$\mathrm{Gal}(L_n/K)/X_n \cong \Gamma_n.$$

Άρα για να ανυψώσουμε ένα γ_n σε ένα στοιχείο $\tilde{\gamma}_n$ της $\mathrm{Gal}(L_n/K)$ σημαίνει ότι διαλέγουμε αυτό το στοιχείο ως αντιπρόσωπο της κλάσης $\gamma_n = \tilde{\gamma}_n X_n$. Αν έχουμε $\gamma_n = \tilde{\gamma}_n X_n = \hat{\gamma}_n X_n$ τότε $\tilde{\gamma}_n^{-1}\hat{\gamma}_n \in X_n$. Καθώς η X_n είναι αβελιανή έχουμε

$$\begin{aligned}\tilde{\gamma}_n x_n \tilde{\gamma}_n^{-1} &= \tilde{\gamma}_n \left(\tilde{\gamma}_n^{-1}\hat{\gamma}_n\right)\left(\tilde{\gamma}_n^{-1}\hat{\gamma}_n\right)^{-1} x_n \tilde{\gamma}_n\\ &= \tilde{\gamma}_n \left(\tilde{\gamma}_n^{-1}\hat{\gamma}_n\right) x_n \left(\tilde{\gamma}_n^{-1}\hat{\gamma}_n\right)^{-1} \tilde{\gamma}_n\\ &= \hat{\gamma}_n x_n \hat{\gamma}_n^{-1}.\end{aligned}$$

Άρα πράγματι η δράση είναι καλά ορισμένη. Επιπλέον, έχουμε ότι το X_n ως p-ομάδα είναι ένα $\mathbb{Z}_p$-πρότυπο με φυσιολογικό τρόπο. Έστω $|X_n| = p^{e_n}$, τότε ένα $y = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ θα δρα ως εξής.

$$y \cdot x_n = \left(\sum_{i=0}^{e_n-1} a_i p^i\right) \cdot x_n,$$

εφόσον οι όροι από το $p^{e_n}x_n$ και μετά θα είναι όλοι 0. Άρα με βάση τα προηγούμενα το X_n είναι ένα $\mathbb{Z}_p[\Gamma_n]$-πρότυπο. Για να προχωρήσουμε παρακάτω είναι ιδιαίτερα σημαντικός ο χαρακτηρισμός της άλγεβρας Iwasawa ως πλήρωση ομαδοδακτυλίων.

Θεώρημα 4.19.

$$\Lambda = \mathbb{Z}_p[[T]] \cong \varprojlim \mathbb{Z}_p[\Gamma_n] =: \mathbb{Z}_p[[\Gamma]]$$

με την αντιστοιχία να είναι

$$T \longleftrightarrow (\gamma_n - 1)_n,$$

δηλαδή αντιστοιχούμε έναν τοπολογικό γεννήτορα $\gamma_0 \longleftrightarrow (\gamma_n)_n$ στο $1 + T$.

Απόδειξη. Αρχικά, έχουμε ότι

$$\Gamma = \mathrm{Gal}(K_\infty/K) \cong \varprojlim \mathrm{Gal}(K_\infty/K)/\mathrm{Gal}(K_\infty/K_n) \cong \varprojlim \mathrm{Gal}(K_n/K) \cong \varprojlim \Gamma_n.$$

Αν κοιτάξουμε τώρα σε πεπερασμένο επίπεδο, καθώς $\Gamma_n \cong \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ έχουμε ότι για έναν γεννήτορα $\gamma_n \in \Gamma_n$ ισχύει ότι $\gamma_n^{p^n} = 1$. Άρα απλά στέλνοντας το γ_n σε ένα U έχουμε τον ισομορφισμό

$$\mathbb{Z}_p[\Gamma_n] \cong \frac{\mathbb{Z}_p[U]}{(U^{p^n} - 1)}.$$

Ωστόσο αυτός ο ισομορφισμός δεν είναι συμβατός με το αντίστροφο σύστημα που φτιάχνουν τα $\mathbb{Z}_p[\Gamma_n]$. Για να το διορθώσουμε αυτό κάνουμε την αλλαγή μεταβλητής $U = T + 1$. Έτσι έχουμε

$$\mathbb{Z}_p[\Gamma_n] \cong \frac{\mathbb{Z}_p[T]}{((1+T)^{p^n} - 1)}$$

και παρατηρούμε ότι το $h_n = (1+T)^{p^n} - 1$ είναι distinguished πολυώνυμο. Επιπλέον, γνωρίζουμε ότι το $\mathbb{Z}_p[[T]]$ είναι η (p, T)-αδική πλήρωση του $\mathbb{Z}_p[T]$, δηλαδή

$$\mathbb{Z}_p[[T]] \cong \varprojlim \frac{\mathbb{Z}_p[T]}{(p, T)^n}.$$

Έχουμε ότι

$$\varprojlim \frac{\mathbb{Z}_p[[T]]}{(h_n)} \cong \mathbb{Z}_p[[T]]$$

καθώς

$$\begin{aligned} h_{n+1} &= (1+T)^{p^{n+1}} - 1 \\ &= \left((1+T)^{p^n} - 1 + 1\right)^p - 1 \\ &= (h_n + 1)^p - 1 \\ &= h_n^p + p h_n^{p-1} + \cdots + p h_n. \end{aligned}$$

Άρα επαγωγικά βλέπουμε ότι το h_{n+1} βρίσκεται στο ιδεώδες $(p, T)^{n+1}$. Επιπλέον, έχουμε

$$\frac{\mathbb{Z}_p[[T]]}{(h_n)} \cong \frac{\mathbb{Z}_p[T]}{(h_n)} \cong \mathbb{Z}_p[\Gamma_n]$$

καθώς το h_n είναι distinguished και μπορούμε σε ένα $f \in \mathbb{Z}_p[[T]]$ να εφαρμόσουμε τον αλγόριθμο διαίρεσης. Έχοντας ότι τα h_n είναι συμβατά ως προς το αντίστροφο όριο, συνδυάζοντας τα παραπάνω έπεται το θεώρημα. □

Καθώς $X \cong \varprojlim X_n$ και $\Lambda \cong \varprojlim \mathbb{Z}_p[\Gamma_n]$, μπορούμε να γράφουμε τα στοιχεία του X ως $(x_0, x_1, \ldots, x_n, \ldots)$ με $x_i \in X_i$ και το Λ να δρα στο X «κατά συντεταγμένη», έτσι ώστε το X να γίνεται ένα Λ-πρότυπο. Όμοια με πριν, ορίζουμε

$$\gamma \cdot x = \tilde{\gamma} x \tilde{\gamma}^{-1},$$

όπου $\tilde{\gamma}$ είναι μια επέκταση του γ στο $\mathrm{Gal}(L/K_m)$, για το m που σταθεροποιήσαμε προηγουμένως. Ωστόσο, εξακολουθούμε να είμαστε στην υπόθεση όπου $m = 0$. Έχοντας $G/X \cong \Gamma$ και ότι η X είναι αβελιανή ως αντίστροφο όριο αβελιανών ομάδων, με όμοιο επιχείρημα με πριν παίρνουμε ότι η παραπάνω δράση είναι καλά ορισμένη.

Θεωρούμε ξανά τους $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ να είναι οι πρώτοι που διακλαδίζονται στην επέκταση K_∞/K και στέκονται αναγκαστικά πάνω από το p. Σταθεροποιούμε έναν πρώτο $\mathfrak{q}_i$ του L που στέκεται πάνω από το $\mathfrak{p}_i$. Ως συνήθως, θεωρούμε $I_i = I(\mathfrak{q}_i|\mathfrak{p}_i) \subset G$ την ομάδα αδράνειας. Καθώς κάθε L_n/K_n είναι αδιακλάδιστη, θα είναι αδιακλάδιστη και η επέκταση L/K_∞ και άρα έχουμε $I_i \cap X = 1$. Συνεπώς έχουμε μια εμφύτευση $I_i \hookrightarrow G/X \cong \Gamma$. Καθώς είμαστε στην υπόθεση όπου $m = 0$, δηλαδή η επέκταση K_∞/K διακλαδίζεται πλήρως στο $\mathfrak{p}_i$ και άρα $I_i = \Gamma$ έχουμε ότι αυτή η εμφύτευση είναι και επιμορφισμός. Άρα η G είναι το ημιευθύ γινόμενο των Γ, I_i, οπότε έχουμε

$$G = I_i X = X I_i$$

για κάθε $i = 1, \ldots, s$. Έστω $\sigma_i \in I_i$ να είναι το στοιχείο που απεικονίζεται στον τοπολογικό γεννήτορα γ_0 της Γ. Καθώς $G = XI_1$ έχουμε ότι $I_i \subseteq XI_1$ για τα $i = 1, \ldots, s$. Συνεπώς, υπάρχει $a_i \in X$ τέτοιο ώστε

$$\sigma_i = a_i \sigma_1$$

Λήμμα 4.20.

$$[G, G] = (\gamma_0 - 1) \cdot X = TX.$$

Απόδειξη. Ταυτίζουμε το Γ με το I_1 και ορίζουμε την δράση του Γ στο X μέσω αυτής της ταύτισης, δηλαδή

$$\gamma \cdot x = \gamma x \gamma^{-1}.$$

Έστω $g_1, g_2 \in G$. Καθώς $G = \Gamma X$ έχουμε στοιχεία $\gamma_1, \gamma_2 \in \Gamma$ και $x_1, x_2 \in X$ έτσι ώστε $g_1 = \gamma_1 x_1$ και $g_2 = \gamma_2 x_2$. Έχουμε

$$\begin{aligned} g_1 g_2 g_1^{-1} g_2^{-1} &= \gamma_1 x_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} \\ &= (\gamma_1 \cdot x_1)\, \gamma_1 \gamma_2 x_2 x_1^{-1} \gamma_1^{-1} x_2^{-1} \gamma_2^{-1} \\ &= (\gamma_1 \cdot x_1)\left((\gamma_1 \gamma_2) \cdot (x_2 x_1^{-1})\right)\left(\gamma_2 \cdot x_2^{-1}\right), \end{aligned}$$

όπου χρησιμοποιήσαμε ότι η Γ είναι αβελιανή. Επιπλέον, παρατηρούμε ότι

$$\begin{aligned} ((1-\gamma_2)\gamma_1 \cdot x_1)\left((\gamma_1 - 1)\gamma_2 \cdot x_2\right) &= \left((1-\gamma_2) \cdot \gamma_1 x_1 \gamma_1^{-1}\right)\left((\gamma_1 - 1) \cdot \gamma_2 x_2 \gamma_2^{-1}\right) \\ &= \left(\gamma_1 x_1 \gamma_1^{-1}\right)\left(\gamma_2 \gamma_1 x_1^{-1} \gamma_1^{-1} \gamma_2^{-1}\right) \\ &\quad \left(\gamma_1 \gamma_2 x_2 \gamma_2^{-1} \gamma_1^{-1}\right)\left(\gamma_2 x_2^{-1} \gamma_2^{-1}\right) \\ &= (\gamma_1 \cdot x_1)\left((\gamma_1 \gamma_2) \cdot (x_2 x_1^{-1})\right)\left(\gamma_2 \cdot x_2^{-1}\right), \end{aligned}$$

όπου χρησιμοποιήσαμε ότι οι Γ και X είναι αβελιανές. Έχουμε

$$g_1 g_2 g_1^{-1} g_2^{-1} = ((1-\gamma_2)\gamma_1 \cdot x_1)\left((\gamma_1 - 1)\gamma_2 \cdot x_2\right).$$

Ειδικότερα, αν θέσουμε $\gamma_2 = e$ και $\gamma_1 = \gamma_0$ θα έχουμε ότι $(\gamma_0 - 1) \cdot x_2 \in [G, G]$. Συνεπώς,

$$(\gamma_0 - 1) \cdot X \subseteq [G, G].$$

Έστω τώρα $\gamma \in \Gamma$ να είναι τυχόν. Καθώς το γ_0 είναι τοπολογικός γεννήτορας, υπάρχει $c \in \mathbb{Z}_p$ έτσι ώστε $\gamma = \gamma_0^c$. Συνεπώς,

$$\begin{aligned} 1 - \gamma &= 1 - \gamma_0^c \\ &= 1 - (1+T)^c \\ &= 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda, \end{aligned}$$

όπου χρησιμοποιήσαμε ότι το γ_0 αντιστοιχεί στο $1 + T$. Άρα έχουμε ότι

$$(1-\gamma_2)\gamma_1 \cdot x_1 \in (\gamma_0 - 1) \cdot X$$

και

$$(1-\gamma_1)\gamma_2 \cdot x_2 \in (\gamma_0 - 1) \cdot X$$

Συνεπώς, έχουμε ότι $[G, G] \subseteq (\gamma_0 - 1) \cdot X$. □

Για $n \geq 0$ θέτουμε

$$\nu_n = 1 + \gamma_0 + \cdots + \gamma_0^{p^n-1}$$

και παρατηρούμε ότι

$$\begin{aligned}\nu_n &= \frac{\gamma_0^{p^n} - 1}{\gamma_0 - 1} \\ &= \frac{(1+T)^{p^n} - 1}{T}.\end{aligned}$$

Έστω Y_0 να ειναι το $\mathbb{Z}_p$-υποπρότυπο του X που παράγεται από τα $\{a_i : 2 \leq i \leq s\}$ και το TX. Σημειώνουμε ότι δεν περιέχουμε το a_1. Θέτουμε $Y_n = \nu_n \cdot Y_0$. Έχουμε το ακόλουθο λήμμα που είναι ιδιαίτερα σημαντικό για την απόδειξη του θεωρήματος Iwasawa, καθώς μπορεί να συσχετίζει πληροφορία μεταξύ του X και των X_n.

Λήμμα 4.21. *Για $n \geq 0$ έχουμε*

$$X_n \cong X/Y_n.$$

Απόδειξη. Ξεκινάμε με την περίπτωση που $n = 0$. Έχουμε $K \subset L_0 \subset L$ και ότι το L_0 είναι η μέγιστη αβελιανή αδιακλάδιστη p-επέκταση του K. Καθώς L/K είναι επίσης p-επέκταση, με την έννοια ότι η G είναι άπειρη p-ομάδα, ισχύει ότι η L_0/K είναι η μέγιστη αβελιανή αδιακλάδιστη p-υποεπέκταση της L/K. Συνεπώς, έχουμε ότι η $\mathrm{Gal}(L/L_0)$ παράγεται από την $[G, G]$ και όλες τις ομάδες αδράνειας $I_i, i = 1, \ldots, s$. Ειδικότερα, έχουμε ότι η $\mathrm{Gal}(L/L_0)$ είναι η κλειστή θήκη της υποομάδας που παράγεται από τα $(\gamma_0 \cdot X), I_1$ και $\{a_i : 2 \leq i \leq s\}$. Συνεπώς, έχουμε

$$\begin{aligned}X_0 &= \mathrm{Gal}(L_0/K) \\ &= G/Gal(L/L_0) \\ &= XI_1/\overline{\langle (\gamma_0 - 1) \cdot X, a_2, \ldots, a_s, I_1 \rangle} \\ &\cong X/\overline{\langle (\gamma_0 - 1) \cdot X, a_2, \ldots, a_s \rangle} \\ &= X/Y_0.\end{aligned}$$

Άρα έχουμε το ζητούμενο για $n = 0$. Έστω τώρα $n \geq 1$. Ουσιαστικά θα μεταφέρουμε την προηγούμενη απόδειξη στην γενική περίπτωση. Αντικαθιστούμε το K με K_0 και άρα την θέση του γ_0 την παίρνει το $\gamma_0^{p^n}$, εφόσον $\mathrm{Gal}(K_\infty/K_n) \cong \Gamma^{p^n}$. Ειδικότερα, αυτό αλλάζει τα σ_i σε $\sigma_i^{p^n}$. Έχουμε ότι

$$\begin{aligned}\sigma_i^{k+1} &= (a_i\sigma_1)^{k+1} \\ &= a_i\sigma_1 a_i \sigma_1^{-1}\sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^k a_i \sigma_1^{-k}\sigma_1^{k+1} \\ &= (1 + \sigma_1 + \cdots + \sigma_1^k) \cdot a_i \sigma_1^{k+1}.\end{aligned}$$

Συνεπώς

$$\sigma_i^{p^n} = (\nu_n a_i) \cdot \sigma_1^{p^n}.$$

Αυτό μας δείχνει ότι πρέπει να αλλάξουμε στο παραπάνω επιχείρημα το a_i με το $\nu_n \cdot a_i$. Είναι ξεκάθαρο ότι πρέπει να αλλάξουμε το $(\gamma_0 - 1) \cdot X$ με το $(\gamma_0^{p^n} - 1) \cdot X = \nu_n(\gamma_0 - 1) \cdot X$. Ουσιαστικά, εδώ φαίνεται πώς θα έπρεπε να προχωρήσουμε σε μια γενική απόδειξη χωρίς την απλούστευση στην περίπτωση $n = 0$. Οπότε, το Y_0 γίνεται Y_n και τελειώνει η απόδειξη. □

Πριν προχωρήσουμε στο επόμενο λήμμα χρειαζόμαστε το γνωστό λήμμα του Nakayama, την απόδειξη του οποίου μπορεί να βρει κανείς στην πρόταση 2.6 του [11]. Υπενθυμίζουμε ότι μια μορφή του λέει το εξής.

Λήμμα 4.22 (Nakayama's Lemma)**.** *Έστω R τυχόν δακτύλιος και και M ένα πεπερασμένα παραγόμενο R-πρότυπο. Υποθέτουμε ότι ένα ιδεώδες I του R περιέχεται στο ιδεώδες Jacobson του R. Τότε αν $IM = M$ έπεται ότι $M = 0$.*

Λήμμα 4.23. *Έστω M ένα συμπαγές Λ-πρότυπο. Αν το $M/(p,T)M$ είναι πεπερασμένα παραγόμενο, τότε το M είναι πεπερασμένα παραγόμενο Λ-πρότυπο. Ειδικότερα, αν το $M/(p,T)M$ είναι πεπερασμένο, τότε το M είναι πεπερασμένα παραγόμενο Λ-πρότυπο.*

Απόδειξη. Έστω U μια περιοχή του 0 στο M. Υπενθυμίζουμε ότι $(p,T)^n \to 0$ στο Λ. Συνεπώς, για οποιοδήποτε $m \in M$ υπάρχει περιοχή U_m έτσι ώστε $(p,T)^n U_m \subseteq U$ για αρκετά μεγάλο n. Τώρα χρησιμοποιούμε την συμπάγεια του M για να διαλέξουμε ένα πεπερασμένο κάλυμμα για το M. Συνεπώς, παίρνοντας το N να είναι το μέγιστο n που χρειάζεται για αυτό το πεπερασμένο κάλυμμα παίρνουμε ότι $(p,T)^N M \subset U$. Καθώς το U ήταν τυχαία περιοχή του 0, έχουμε ότι $\bigcap((p,T)^n M) = 0$. Έστω ότι τα $m_1, \ldots, m_n$ παράγουν το $M/(p,T)M$. Θέτουμε $N = \Lambda m_1 + \cdots \Lambda m_n \subseteq M$. Παρατηρούμε ότι το N είναι συμπαγές καθώς είναι η εικόνα του Λ, άρα είναι κλειστό. Συνεπώς, το M/N είναι ένα συμπαγές Λ-πρότυπο. Εφόσον τα m_i παράγουν το $M/(p,T)M$ αυτό μας δίνει ότι $N + (p,T)M = M$. Συνεπώς, έχουμε

$$(p,T)(M/N) = (N + (p,T)M)/N = M/N.$$

Άρα,

$$(p,T)^n(M/N) = (M/N)$$

για κάθε $n \geq 0$. Εφόσον το (p,T) είναι το μοναδικό μέγιστο ιδεώδες όπως έχουμε δείξει, από το λήμμα του Nakayama παίρνουμε ότι $M/N = 0$, δηλαδή τα $m_1, \ldots, m_n$ παράγουν το M. □

Πόρισμα 4.24. *Το Λ-πρότυπο $X = \mathrm{Gal}(L/K_\infty)$ είναι πεπερασμένα παραγόμενο.*

Απόδειξη. Υπενθυμίζουμε ότι

$$\nu_1 = \frac{(1+T)^p - 1}{T}$$

Είναι προφανές ότι $\nu_1 \in (p,T)$. Συνεπώς, έχουμε ότι το $Y_0/(p,T)Y_0$ έναι πηλίκο του $Y_0/\nu_1 \cdot Y_0 = Y_0/Y_1 \subset X/Y_1 = X_1$. Ξέρουμε ότι το X_1 είναι πεπερασμένο σύνολο και άρα είναι και το $Y_0/(p,T)Y_0$ πεπερασμένο. Εφαρμόζοντας το προηγούμενο λήμμα παίρνουμε ότι το Y_0 είναι πεπερασμένα παραγόμενο. Καθώς τώρα το $X/Y_0 = X_0$ είναι πεπερασμένο, το ίδιο το X θα είναι πεπερασμένα παραγόμενο ως Λ-πρότυπο. □

Όλα τα παραπάνω αποτελέσματα έχουν γίνει υπό την υπόθεση ότι $m = 0$, δηλαδή η επέκταση K_∞/K είναι πλήρως διακλαδιζόμενη σε όποιο πρώτο διακλαδίζεται. Τώρα θα σταματήσουμε να είμαστε κάτω από αυτή την υπόθεση. Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση και K_m να είναι όπως στην πρόταση 4.17. Υπενθυμίζουμε ότι οι επεκτάσεις K_∞/K και K_∞/K_m αντιστοιχούν στο ίδιο X. Άρα έχουμε ότι το X είναι πεπερασμένα παραγόμενο Λ-πρότυπο από το πόρισμα 4.24. Για $n \geq m$, αντικαθιστούμε το ν_n με το $\nu_{n,m}$ που ορίζουμε ως εξής:

$$\begin{aligned}\nu_{n,m} &= \frac{\nu_n}{\nu_m} \\ &= 1 + \gamma_0^{p^m} + \gamma_0^{2p^m} + \cdots + \gamma_0^{p^n - p^m}.\end{aligned}$$

Αυτό δουλεύει καθώς $\mathrm{Gal}(K_\infty/K_m) \cong \Gamma^{p^m}$ η οποία παράγεται από το $\gamma_0^{p^m}$. Άρα με τις κατάλληλες αντικαταστάσεις διορθώνουμε το λήμμα 4.21 και παίρνουμε το πιο ισχυρό:

Λήμμα 4.25. *Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση. Το X είναι πεπερασμένα παραγόμενο Λ-πρότυπο και υπάρχει $m \geq 0$ τέτοιο ώστε*

$$X_n \cong X/\nu_{n,m} \cdot Y_m$$

για κάθε $n \geq m$, όπου το Y_m είναι αυτό που έχει οριστεί προηγουμένως.

Είμαστε τώρα σε θέση να εφαρμόσουμε το θεώρημα δομής για τα πεπερασμένα παραγόμενα Λ-πρότυπα στο X και στο Y_m. Παρατηρούμε ότι παίρνουμε το ίδιο αποτέλεσμα από το θεώρημα είτε χρησιμοποιήσουμε το X ή το Y_m, καθώς το X/Y_m είναι πεπερασμένο και το θεώρημα δομής είναι σε όρους ψευδο-ισομορφισμού. Συνεπώς, έχουμε

$$X \sim Y_m \sim \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus \Lambda/(f_j(T)^{m_j})\right). \tag{4.4}$$

Και το επόμενο μας βήμα είναι να υπολογίσουμε το $M/\nu_{n,m}M$ για κάθε όρο M του ευθέους αθροίσματος παραπάνω στην σχέση 4.4. Κάνοντας το, θα πάρουμε τα φράγματα που θέλουμε για την τάξη $|X_n|$.

Περίπτωση 1: $M = \Lambda$.
Παρατηρούμε ότι το $\nu_{n,m}$ όχι μόνο δεν είναι αντιστρέψιμο στο Λ, αλλά είναι distinguished πολυώνυμο. Επομένως από το λήμμα 4.12 παίρνουμε ότι το $\Lambda/(\nu_{n,m})$ έχει άπειρη τάξη. Ωστόσο, έχουμε ήδη ότι το $Y_m/\nu_{n,m}Y_m$ είναι πεπερασμένο. Άρα αναγκαστικά $r = 0$.

Περίπτωση 2: $M = \Lambda/(p^k)$ για κάποιο $k > 0$.
Σε αυτή τη περίπτωση έχουμε να εξετάσουμε το $\Lambda/(p^k, \nu_{n,m})$. Εφόσον το $\nu_{n,m}$ είναι distinguished πολυώνυμο, μπορούμε να εφαρμόσουμε τον αλγόριθμο διαίρεσης ώστε να καταλήξουμε στο ότι τα στοιχεία του $\Lambda/(p^k, \nu_{n,m})$ είναι ακριβώς τα πολυώνυμα modulo p^k βαθμού μικρότερου του $\deg \nu_{n,m} = p^n - p^m$. Συνεπώς,

$$|M/\nu_{n,m}M| = (p^k)^{p^n - p^m} = p^{kp^n + c}$$

όπου $c = -kp^m$, μια σταθερά που εξαρτάται από το σώμα K.

Περίπτωση 3: $M = \Lambda/(f(T)^r)$.
Έστω $g(T) = f(T)^r$. Υποθέτουμε ότι το g έχει βαθμό d. Καθώς το f είναι distinguished πολυώνυμο, θα είναι και το g. Άρα έχουμε ότι

$$T^k \equiv p \cdot (\text{πολυώνυμο}) (\text{mod}\, g)$$

για $k \geq d$. Θα χρησιμοποιούμε τον όρο «πολυώνυμο στις παρακάτω πράξεις αρκετές φορές», ωστόσο δεν σημαίνει ότι θα είναι το ίδιο πολυώνυμο κάθε φορά. Έστω $p^n \geq d$. Έχουμε

$$\begin{aligned}(1+T)^{p^n} &= 1 + p \cdot (\text{πολυώνυμο}) + T^{p^n} \\ &\equiv 1 + p \cdot (\text{πολυώνυμο}) (\text{mod}\, g).\end{aligned}$$

Ειδικότερα, έχουμε ότι

$$\begin{aligned}(1+T)^{p^{n+1}} &= \left((1+T)^{p^n}\right)^p \\ &\equiv (1 + p \cdot (\text{πολυώνυμο}))^p \,(\text{mod}\, g) \\ &\equiv 1 + p^2 \cdot (\text{πολυώνυμο}) (\text{mod}\, g)\end{aligned}$$

Θέτουμε $P_n(T) = (1+T)^{p^n} - 1$. Κάνοντας τις πράξεις έχουμε

$$\begin{aligned}
P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\
&= \left((1+T)^{p^{n+1}} - 1\right)\left(1 + (1+T)^{p^{n+1}} + \cdots + (1+T)^{p^{n+1}(p-1)}\right) \\
&= P_{n+1}(T)\left(1 + (1+T)^{p^{n+1}} + \cdots + (1+T)^{p^{n+1}(p-1)}\right) \\
&\equiv P_{n+1}(T)(1 + \cdots + 1 + p^2 \cdot (\text{πολυώνυμο}) \ ) \pmod{g} \\
&\equiv P_{n+1}(T)(p + p^2 \cdot (\text{πολυώνυμο}) \ ) \pmod{g} \\
&\equiv p(1 + p \cdot (\text{πολυώνυμο}))P_{n+1}(T) \pmod{g}.
\end{aligned}$$

Εφόσον το $1 + p \cdot (\text{πολυώνυμο})$ είναι αναγκαστικά αντιστρέψιμο στο Λ, έχουμε ότι το $\frac{P_{n+2}(T)}{P_{n+1}(T)}$ δρα στο $\Lambda/(g)$ ως $p \cdot U$ για ένα $U \in \Lambda^\times$, με την προϋπόθεση ότι $p^n \geq d$. Υποθέτουμε τώρα ότι έχουμε $n_0 > m, p^{n_0} \geq d$ και $n \geq n_0$. Παρατηρούμε ότι

$$\frac{\nu_{n+2,m}}{\nu_{n+1,m}} = \frac{\nu_{n+2}}{\nu_{n+1}} = \frac{P_{n+2}}{P_{n+1}}.$$

Συνεπώς,

$$\begin{aligned}
\nu_{n+2,m}M &= \frac{P_{n+2}}{P_{n+1}}\nu_{n+1,m}M \\
&= p\nu_{n+1,m}M.
\end{aligned}$$

Οπότε έχουμε

$$|M/\nu_{n+2,m}M| = |M/pM| \cdot |pM/p\nu_{n+1,m}M|$$

Καθώς το g είναι distinguished πολυώνυμο έχουμε $\gcd(p, g) = 1$. Ειδικότερα, αυτό σημαίνει ότι ο πολλαπλασιασμός με p είναι μια 1-1 απεικόνιση. Άρα

$$|pM/p\nu_{n+1,m}M| = |M/\nu_{n+1,m}M|.$$

Επιπλέον, ισχύει ότι

$$M/pM \cong \Lambda/(p, g) = \Lambda/(p, T^d)$$

και άρα $|M/pM| = p^d$. Συνεπώς, σε λίγα βήματα έχουμε

$$\begin{aligned}
|M/\nu_{n,m}M| &= |M/pM| \cdot |pM/p\nu_{n-1,m}M| \\
&= p^d \cdot |M/\nu_{n-1,m}M| \\
&= p^d \cdot p^d \cdot |pM/p\nu_{n-2,m}M| \\
&= \cdots \\
&= p^{d(n-n_0-1)}|M/\nu_{n_0+1,m}M|
\end{aligned}$$

για τα $n \geq n_0 + 1$.
Οπότε, αν το $|M/\nu_{n,m}M|$ είναι πεπερασμένο για κάθε n παίρνουμε ότι $|M/\nu_{n,m}M| = p^{dn+c}$ για τα $n \geq n_0 + 1$ και c μια σταθερά που εξαρτάται από το σώμα K. Αν το $M/\nu_{n,m}M$ ήταν άπειρο για οποιοδήποτε n, τότε το M δεν θα μπορούσε να προκύψει όπως είδαμε στην περίπτωση 1. Άρα έχουμε δείξει το ακόλουθο αποτέλεσμα.

Πρόταση 4.26. *Υποθέτουμε ότι*

$$N = \Lambda^r \oplus \left(\bigoplus \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus \Lambda/(f_j(T))\right),$$

όπου κάθε f_j είναι distinguished. Έστω $\mu = \sum \mu_i$ και $\lambda = \sum \deg f_j$. Αν το $N/\nu_{n,m}N$ είναι πεπερασμένο για κάθε n, τότε $r = 0$ και υπάρχουν n_0 και c έτσι ώστε

$$|N/\nu_{n,m}N| = p^{\mu p^n + \lambda n + c}$$

για κάθε $n \geq n_0$.

Ξέρουμε ότι το Y_m είναι ψευδο-ισόμορφο με ένα κατάλληλο N όπως αυτό δίνεται στην παραπάνω πρόταση. Επιπλέον, ξέρουμε την τάξη του $N/\nu_{n,m}N$ για όλα τα $n \geq n_0$. Άρα μας μένει να συσχετίσουμε την τάξη αυτή στην τάξη του $Y_m/\nu_{n,m}Y_m$. Το πρόβλημα εδώ είναι ότι τα άκρα της ακριβής ακολουθίας που έχουμε στον ορισμό του ψευδο-ισομορφισμού μπορεί να διαφέρουν καθώς αλλάζει το n. Ξέρουμε ότι από το προηγούμενο αποτέλεσμα η τάξη της $|Y_m/\nu_{n,m}Y_m|$ έχει την μορφή που θέλουμε, αλλά καθώς αλλάζουν τα άκρα δεν έχουμε δείξει προς το παρόν ότι αυτό δεν θα διαφοροποιείται. Οπότε, αρκεί να δείξουμε ότι για αρκετά μεγάλο n οι τάξεις των άκρων στις ακριβείς ακολουθίες θα παραμείνουν σταθερές. Το πετυχαίνουμε αυτό στο επόμενο λήμμα, με μια τυπική εφαρμογή του λήμματος του φιδιού.

Λήμμα 4.27. *Έστω M και N να είναι Λ-πρότυπα με $M \sim N$ και το $M/\nu_{n,m}M$ να έχει πεπερασμένη τάξη για κάθε $n \geq m$. Για κάποιο σταθερό a και κάποιο n_0 έχουμε*

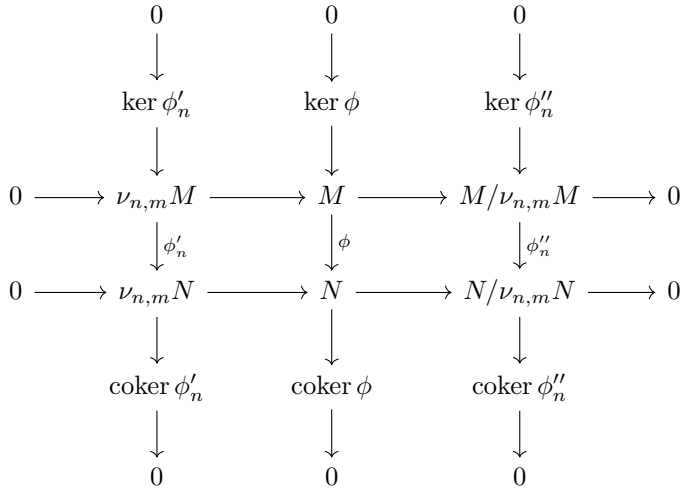
$$|M/\nu_{n,m}M| = p^a |N/\nu_{n,m}N|$$

για κάθε $n \geq n_0$.

Απόδειξη. Εφόσον υποθέτουμε ότι $M \sim N$ έχουμε την ακριβή ακολουθία

$$0 \longrightarrow \ker\phi \longrightarrow M \xrightarrow{\phi} N \longrightarrow \operatorname{coker}\phi \longrightarrow 0$$

με τα $\ker\phi$ και $\operatorname{coker}\phi$ να είναι πεπερασμένα. Χρησιμοποιώντας αυτήν την ακριβή ακολουθία παίρνουμε το παρακάτω μεταθετικό διάγραμμα



Ο στόχος μας είναι να δείξουμε ότι για αρκετά μεγάλο n οι τάξεις $|\ker\phi''_n|$ και $|\operatorname{coker}\phi''_n|$ μένουν σταθερά. Το αποδεικνύουμε αυτό με το να δείξουμε ότι σαν ακολουθίες είναι φθίνουσες και φραγμένες. Είναι ξεκάθαρο ότι $|\operatorname{coker}\pi''_n| \leq |\operatorname{coker}\phi|$ καθώς παίρνουμε τους αντιπροσώπους του $\operatorname{coker}\phi''_n$ από αυτούς του $\operatorname{coker}\phi$. Για να δούμε ότι το $|\ker\phi''_n|$ είναι φραγμένο, εφαρμόζουμε το λήμμα του φιδιού για να πάρουμε την μακριά ακριβή ακολουθία

$$0 \longrightarrow \ker \phi'_n \longrightarrow \ker \phi \longrightarrow \ker \phi''_n \longrightarrow$$

$$\operatorname{coker} \phi'_n \longrightarrow \operatorname{coker} \phi \longrightarrow \operatorname{coker} \phi''_n \longrightarrow 0$$

Από την οποία παίρνουμε ότι

$$\begin{aligned} |\ker \phi''_n| &\leq |\ker \phi| \cdot |\operatorname{coker} \phi'_n| \\ &\leq |\ker \phi| \cdot |\operatorname{coker} \phi|, \end{aligned}$$

όπου χρησιμοποιήσαμε ότι $|\operatorname{coker} \phi'_n| \leq |\operatorname{coker} \phi|$, το οποίο ισχύει εφόσον για να πάρουμε τους αντιπροσώπους του $\operatorname{coker} \phi'_n$ πολλαπλασιάζουμε τους αντιπροσώπους του $\operatorname{coker} \phi$ με $\nu_{n,m}$. Άρα το $|\ker \phi''_n|$ είναι πράγματι φραγμένο.

Θα δείξουμε τώρα ότι αυτά φθίνουν. Έστω $n' \geq n \geq 0$. Τότε έχουμε $|\operatorname{coker} \phi''_{n'}| \leq |\operatorname{coker} \phi''_n|$ καθώς

$$\nu_{n',m} N = \nu_{n,m} \left(\frac{\nu_{n',m}}{\nu_{n,m}} \right) N \subseteq \nu_{n,m} N.$$

Άρα, για αρκετά μεγάλο n έχουμε ότι το $|\operatorname{coker} \phi''_n|$ είναι σταθερό. Μένει να δείξουμε το ίδιο για το $|\ker \phi''_n|$. Από το λήμμα του φιδιού έχουμε ότι

$$|\ker \phi'_n| \cdot |\ker \phi''_n| \cdot |\operatorname{coker} \phi| = |\ker \phi| \cdot |\operatorname{coker} \phi'_n| \cdot |\operatorname{coker} \phi''_n|.$$

Συνεπώς, αρκεί να δείξουμε ότι για μεγάλο n τα $|\ker \phi'_n|$ και $|\operatorname{coker} \phi'_n|$ είναι σταθερά. Από το μεταθετικό διάγραμμα έχουμε ότι $\ker \phi'_n \subset \ker \phi$, άρα εύκολα παίρνουμε ότι το $|\ker \phi'_n|$ είναι φραγμένο. Για να δούμε ότι φθίνει, παρατηρούμε ότι $\nu_{n',m} M \subseteq \nu_{n,m} M$ και από αυτό έπεται ότι $\ker \phi'_{n'} \subseteq \ker \phi'_n$.

Θα ασχοληθούμε τώρα με το $|\operatorname{coker} \phi'_n|$. Έχουμε όπως αναφέραμε πριν ότι $|\operatorname{coker} \phi'_{n'}| \leq |\operatorname{coker} \phi|$, άρα πρέπει να δείξουμε ότι το $|\operatorname{coker} \phi'_n|$ φθίνει. Έστω $\nu_{n',m} y \in \nu_{n',m} N$. Σταθεροποιούμε ένα σύνολο αντιπροσώπων του $\operatorname{coker} \phi'_n$ και έστω $z \in \nu_{n,m} N$ να είναι ο αντιπρόσωπος του $\nu_{n,m} y$ στο $\operatorname{coker} \phi'_n$. Παρατηρούμε ότι

$$\nu_{n,m} y - z = \phi(\nu_{n,m} x)$$

για κάποιο $x \in M$ καθώς αυτό θα είναι αναγκαστικά μέσα στην εικόνα $\operatorname{im}(\phi'_n)$ η οποία εμφυτεύεται στην $\operatorname{im}(\phi)$. Συνεπώς, έχουμε

$$\left(\frac{\nu_{n',m}}{\nu_{n,m}} \right) \nu_{n,m} y - \left(\frac{\nu_{n',m}}{\nu_{n,m}} \right) z = \left(\frac{\nu_{n',m}}{\nu_{n,m}} \right) \phi(\nu_{n,m} x),$$

δηλαδή

$$\begin{aligned} \nu_{n',m} y - \left(\frac{\nu_{n',m}}{\nu_{n,m}} \right) z &= \phi(\nu_{n',m} x) \\ &= \phi'_{n'}(\nu_{n',m} x). \end{aligned}$$

Άρα με το να πολλαπλασιάσουμε τους αντιπροσώπους του $\operatorname{coker} \phi'_n$ με το $\frac{\nu_{n',m}}{\nu_{n,m}}$ παίρνουμε αντιπροσώπους του $\operatorname{coker} \phi'_{n'}$, το οποίο αποδεικνύει ότι $|\operatorname{coker} \phi'_{n'}| \leq |\operatorname{coker} \phi'_n|$.

Συνοψίζοντας, έχουμε την ακριβή ακολουθία

$$0 \longrightarrow \ker \phi''_n \longrightarrow M/\nu_{n,m} M \longrightarrow N/\nu_{n,m} N \longrightarrow \operatorname{coker} \phi''_n \longrightarrow 0$$

και n_0 έτσι ώστε για τα $n \geq n_0$ οι όροι $|\ker \phi''_n|, |\operatorname{coker} \phi''_n|$ να είναι σταθεροί, άρα έχουμε το επιθυμητό αποτέλεσμα.

□

Είναι πλέον απλό να ολοκληρώσουμε την απόδειξη του θεωρήματος του Iwasawa, δηλαδή του θεωρήματος 4.1. Έχουμε δείξει ότι υπάρχουν ακέραιοι $n_0, \nu, \lambda \geq 0$, και $\mu \geq 0$ έτσι ώστε

$$\begin{aligned} p^{e_n} &= |X_n| \\ &= |X/Y_m| \cdot |Y_m/\nu_{n,m}Y_m| \\ &= p^b \cdot |N/\nu_{n,m}N| \\ &= p^{\lambda n + \mu p^n + \nu} \end{aligned}$$

για κάθε $n \geq n_0$. □

Αξίζει να σημειωθεί ότι λόγω της ασυμπτωτικής φύσης που έχει το αποτέλεσμα δεν μπορεί να λειτουργήσει αυτός ο τύπος για την ακριβή εύρεση της τάξης της ομάδας κλάσεων ιδεωδών. Αυτό είναι γενικότερα ένα δύσκολο πρόβλημα υπολογιστικά και ο αλγόριθμος που χρησιμοποιείται σήμερα για τον υπολογισμό των μεγάλων τάξεων υποθέτει την ορθότητα της γενικευμένης υπόθεσης του Riemann [10]. Από όλα τα παραπάνω επιχειρήματα που κάναμε, το n_0 αρχικά εξαρτάται από ποιο βήμα και μετά ανεβαίνοντας τον πύργο K_∞/K τα ιδεώδη που διακλαδίζονται να διακλαδίζονται πλήρως, δηλαδή από ποιο m ξεκινάει να συμβαίνει αυτό για την επέκταση K_∞/K_m. Επιπλέον, εξαρτάται από ποιο n και πάνω ο πυρήνας και ο συνπυρήνας διατηρούν σταθερή τάξη στον ομομορφισμό που έχουμε από το θεώρημα δομής.

Κλείνουμε την ενότητα με κάποιες εφαρμογές από την δουλειά που έχουμε κάνει. Υπενθυμίζουμε ότι $X_n \cong A_n$ όπου A_n είναι η p-Sylow υποομάδα της ομάδας κλάσεων του K_n. Θα εξακολουθούμε να χρησιμοποιούμε το X_n σαν συμβολισμό μαζί με ότι το h_n είναι η τάξη της ομάδας κλάσεων του K_n. Συγκεκριμένα, η τάξη του A_n είναι το p-μέρος του h_n. Χρησιμοποιώντας το λήμμα 4.22 του Nakayama έχουμε το εξής αποτέλεσμα.

Πρόταση 4.28. *Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση στην οποία ακριβώς ένας πρώτος διακλαδίζεται. Επιπλέον, υποθέτουμε ότι αυτός διακλαδίζεται πλήρως. Τότε έχουμε*

$$X_n \cong X/((1+T)^{p^n} - 1)X$$

και $p \nmid h_0$ αν και μόνο αν $p \nmid h_n$ για κάθε $n \geq 0$.

Απόδειξη. Έχουμε ότι για την επέκταση K_∞/K ισχύει η προϋπόθεση $m = 0$ που είχαμε κάνει όταν αποδεικνύαμε το λήμμα 4.21. Συγκεκριμένα $s = 1$, το πλήθος των πρώτων, και $Y_0 = TX$. Συνεπώς,

$$\begin{aligned} Y_n &= \nu_n TX \\ &= \left(\frac{(1+T)^{p^n} - 1}{T} \right) TX \end{aligned}$$

το οποίο μας δίνει το πρώτο αποτέλεσμα. Υποθέτουμε ότι $p \nmid h_0$. Ειδικότερα, αυτό μας δίνει ότι $X_0 = 0$, δηλαδή $X/TX = 0$. Ωστόσο, αυτό σημαίνει ότι

$$\frac{X}{TX} \supseteq \frac{X}{(p,T)} = 0,$$

δηλαδή

$$(p,T)X = X$$

και άρα από το λήμμα του Nakayama παίρνουμε ότι $X = 0$. □

Εδώ παρατηρούμε ότι δεν μπορούμε να χρησιμοποιήσουμε το θεώρημα 4.1 για να καταλήξουμε στο αποτέλεσμα σχετικά με την διαιρετότητα του h_n καθώς το θεώρημα 4.1 ισχύει μόνο για τα n μεγαλύτερα από κάποιο n_0 και όχι για όλα τα $n \geq 0$.

Υπενθυμίζουμε ότι για A μια πεπερασμένη αβελιανή ομάδα έχουμε όρισει το p-rank(A) να είναι η διάσταση του A/pA ως $\mathbb{F}_p$-διανυσματικού χώρου, δηλαδή

$$p\text{-rank}(A) = \dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA)$$

Λήμμα 4.29. *Έστω το Λ-πρότυπο N που δίνεται ως εξής*

$$N = \left(\bigoplus_{i=1}^{s} \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T))\right),$$

όπου τα f_j είναι distinguished πολυώνυμα. Θέτουμε $\mu = \sum \mu_i$. Τότε $\mu = 0$ αν και μόνο αν το p-rank$(N/\nu_{n,m}N)$ είναι φραγμένο καθώς $n \longrightarrow \infty$.

Απόδειξη. Το $\nu_{n,m}$ είναι distinguished πολυώνυμο βαθμού $p^n - p^m$. Συνεπώς, μπορούμε να πάρουμε μεγάλο n έτσι ώστε να έχουμε ότι ο βαθμός του $\nu_{n,m}$ θα είναι μεγαλύτερος από το μέγιστο των βαθμών των f_j. Για αυτό το n έχουμε

$$\begin{aligned}
N/(p,\nu_{n,m})N &= \left(\bigoplus_{i=1}^{s} \frac{\Lambda/(p^{\mu_i})}{(p,\nu_{n,m})/(p^{\mu_i})}\right) \oplus \left(\bigoplus_{j=1}^{t} \frac{\Lambda/(f_j(T))}{(p,\nu_{n,m})/(f_j(T))}\right) \\
&= \left(\bigoplus_{i=1}^{s} \Lambda/(p,\nu_{n,m})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p,f_j,\nu_{n,m})\right) \\
&= \left(\bigoplus_{i=1}^{s} \Lambda/(p,T^{p^n-p^m})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(p,T^{\deg f_j})\right) \\
&\cong (\mathbb{Z}/p\mathbb{Z})^{s(p^n-p^m)+\lambda},
\end{aligned}$$

όπου $\lambda = \sum \deg f_j$. Από την τελευταία σχέση είναι ξεκάθαρο ότι το p-rank είναι φραγμένο αν και μόνο αν $s = 0$, δηλαδή αν και μόνο αν $\mu = 0$. □

Πρόταση 4.30. *Θεωρούμε το μ όπως είναι στο θεώρημα 4.1. Τότε $\mu = 0$ αν και μόνο αν το p-rank(X_n) είναι φραγμένο καθώς $n \longrightarrow \infty$.*

Απόδειξη. Έχουμε ότι το $\mu = 0$ αν και μόνο αν το p-rank$(N/\nu_{n,m}N)$ είναι φραγμένο, από το προηγούμενο λήμμα όπου το N είναι όπως παραπάνω. Υπενθυμίζουμε ότι έχουμε την ακριβή ακολουθία

$$0 \longrightarrow \ker \phi_n'' \longrightarrow Y_m/\nu_{n,m}Y_m \xrightarrow{\phi_n''} N/\nu_{n,m}N \longrightarrow \operatorname{coker} \phi_n'' \longrightarrow 0$$

όπου ξέρουμε ότι τα $|\ker \phi_n''|$ και $|\operatorname{coker} \phi_n''|$ είναι φραγμένα ανεξαρτήτως του n για αρκετά μεγάλο n. Από αυτό έπεται ότι $\mu = 0$ αν και μόνο αν το p-rank$(Y_m/\nu_{n,m}Y_m)$ είναι φραγμένο. Ωστόσο, ξέρουμε ότι $X_n \cong X/\nu_{n,m}Y_m$ και το $X/Y_m \cong X_m$ είναι πεπερασμένο και ανεξάρτητο του n. Άρα το X_n διαφέρει από το $Y_m/\nu_{n,m}Y_m$ κατά μια πεπερασμένη ομάδα που με φραγμένη τάξη που δεν εξαρτάται από το n. Συνεπώς, έπεται το αποτέλεσμα. □

Η Κύρια Εικασία Iwasawa

5.1 Εισαγωγή

Σε αυτή την ενότητα θα δώσουμε τους απαραίτητους ορισμούς για να μπορέσουμε να διατυπώσουμε και να καταλάβουμε την κύρια εικασία του Iwasawa. Θα την διατυπώσουμε με όρους πλήρως πραγματικών σωμάτων, ωστόσο ως εικασία αποδείχθηκε για πρώτη φορά το 1984 από τους A. Wiles και B. Mazur μόνο για το $\mathbb{Q}$ και τις αβελιανές του επεκτάσεις [3]. Στην συνέχεια το 1990 ο Wiles την απέδειξε για όλα τα πλήρως πραγματικά σώματα [4].

Έστω F ένα πλήρως πραγματικό σώμα και $F \subset F_1 \subset \cdots \subset F_\infty$ να είναι η κυκλοτομική $\mathbb{Z}_p$-επέκταση του F. Έστω $\gamma_0 \in \mathrm{Gal}(F_\infty/F)$ να είναι το στοιχείο που αντιστοιχεί στο $1 \in \mathbb{Z}_p$ μέσα από τον ισομορφισμό $\mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$, έτσι το γ_0 να είναι ένας τοπολογικός γεννήτορας του $\mathrm{Gal}(F_\infty/F)$. Παρατηρούμε ότι εδώ το F_∞, άρα και κάθε F_n, διακλαδίζεται πλήρως στο p. Άρα $I_\mathfrak{q} = \mathrm{Gal}(F_\infty/F)$, δηλαδή η ομάδα αδράνειας του μοναδικού πρώτου $\mathfrak{q}$ πάνω από το p είναι ολόκληρη η ομάδα Galois.

Έστω χ ένας p-αδικός Artin χαρακτήρας του F, δηλαδή ένας συνεχής ομομορφισμός ομάδων με πεπερασμένη εικόνα

$$\chi : G_F = \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \overline{\mathbb{Q}}_p^\times,$$

όπου F^{sep} είναι η διαχωρίσιμη θήκη του F. Καθώς ο χ είναι συνεχής, ο πυρήνας $\ker\chi$ θα είναι κλειστή υποομάδα, δηλαδή επιδέχεται την αντιστοιχία Galois και άρα μπορούμε να ορίσουμε όπως στους χαρακτήρες Dirichlet το σώμα F^χ που αντιστοιχεί στον χαρακτήρα χ να είναι το σταθερό σώμα του $\ker\chi$. Δηλαδή, ο χαρακτήρας παραγοντοποιείται μέσα από

$$\chi : \mathrm{Gal}(F^\chi/F) \longrightarrow \langle\zeta_n\rangle \subseteq \overline{\mathbb{Q}}_p^\times.$$

Ακολουθώντας τον Wiles [4] λέμε ότι ο χ είναι τύπου S αν $F^\chi \cap F_\infty = F$ και τύπου W αν $F^\chi \subset F_\infty$. Στο βιβλίο του Washington [1] αυτά αναφέρονται ως τύπου 1 και 2 αντίστοιχα. Στο εξής θα υποθέτουμε ότι το F^χ είναι και αυτό πλήρως πραγματικό.

Υποθέτουμε επιπλέον ότι ο χ είναι τύπου S. Θέτουμε $F_n^\chi = F_n F^\chi$, έτσι ώστε

$$F_\infty^\chi = F_\infty F^\chi = \bigcup_n F_n^\chi.$$

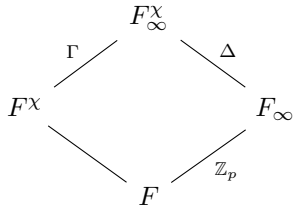
Το γεγονός ότι ο χ είναι τύπου S μας δίνει τους ισομορφισμούς

$$\Gamma = \mathrm{Gal}(F_\infty^\chi/F^\chi) \longrightarrow \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$$

και

$$\Delta = \mathrm{Gal}(F_\infty^\chi/F_\infty) \longrightarrow \mathrm{Gal}(F^\chi/F)$$

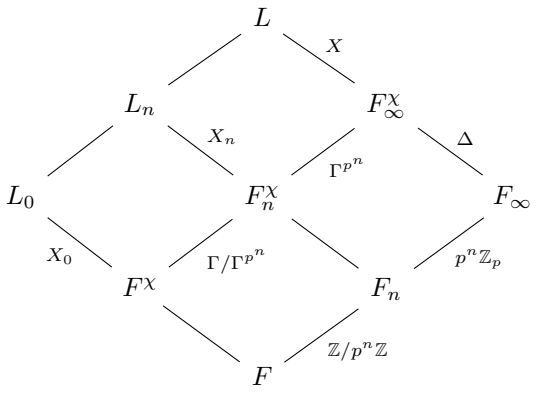
και όπως κάναμε στα προηγούμενα κεφάλαια, παίρνουμε όμοιους ισομορφισμούς αντικαθιστώντας τα F_∞^χ και F_∞ με τα F_n^χ και F_n αντίστοιχα. Σκεφτόμαστε πλέον το γ_0 σαν στοιχείο του Γ. Έχουμε το ακόλουθο διάγραμμα σωμάτων με τις αντίστοιχες ομάδες



Όπως στο κεφάλαιο 4 ορίζουμε ως L_n να είναι η μέγιστη αδιακλάδιστη αβελιανή p-επέκταση του F_n^χ. Θέτουμε $X_n = \mathrm{Gal}(L_n/F_n^\chi)$, οπότε το X_n είναι ισόμορφο με την p-Sylow υποομάδα της ομάδας κλάσεων του F_n^χ. Έστω $L = \cup L_n F_\infty^\chi$ και παρατηρούμε ότι

$$\begin{aligned} X &= \mathrm{Gal}(L/F_\infty^\chi) \\ &\cong \varprojlim \mathrm{Gal}(L_n F_\infty^\chi / F_\infty^\chi) \\ &\cong \varprojlim \mathrm{Gal}(L_n/F_n^\chi) \\ &= \varprojlim X_n \end{aligned}$$

όμοια με την δουλειά στο κεφάλαιο 4. Έχουμε πλέον το ακόλουθο διάγραμμα σωμάτων με τις αντίστοιχες ομάδες:



Όπως προηγουμένως, έχουμε ότι $\mathrm{Gal}(F_\infty^\chi/F) \cong \Delta \times \Gamma$ και δρα στο X με συζυγίες. Καθώς το X είναι pro-p ομάδα, έχουμε μια φυσιολογική δράση του $\mathbb{Z}_p$ στο X. Συνεπώς, το X είναι ένα $\mathbb{Z}_p[[\Delta \times \Gamma]]$-πρότυπο, άρα και ένα $\mathbb{Z}_p[[\Gamma]]$-πρότυπο. Χρησιμοποιούμε πάλι το γεγονός ότι $\mathbb{Z}_p[[\Gamma]] \cong \Lambda = \mathbb{Z}_p[[T]]$ μέσα από την απεικόνιση $\gamma_0 \longmapsto 1+T$. Υπενθυμίζουμε ότι στο κεφάλαιο 4 είδαμε το ακόλουθο

$$X \sim \left(\bigoplus_i \Lambda/(p^{\mu_i}) \right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j}) \right) \tag{5.1}$$

με τα f_j να είναι ανάγωγα και distinguished πολυώνυμα στο $\mathbb{Z}_p[T]$.

Θέτουμε $V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p$. Με αυτό έχουμε ότι

$$V \cong \bigoplus_j \overline{\mathbb{Q}}_p[T]/(f_j(T)^{m_j})$$

καθώς με το να πάρουμε το τανυστικό γινόμενο με το $\overline{\mathbb{Q}}_p$ μηδενίζουμε τον πυρήνα, τον συνπυρήνα και τα $\Lambda/(p^{\mu_i})$ στην εξίσωση 5.1. Άρα το V είναι ένας διανυσματικός χώρος πεπερασμένης

διάστασης. Θέτουμε

$$f_X(T) = \prod_j f_j(T)^{m_j}.$$

Καθώς $T \longleftrightarrow \gamma_0 - 1$ μέσα από τον ισομορφισμό $\Lambda \cong \mathbb{Z}_p[[\Gamma]]$, έχουμε ότι το $f_X(T)$ είναι το χαρακτηριστικό πολυώνυμο της δράσης του $\gamma_0 - 1$ στο V. Μπορούμε να πάρουμε επιπλέον πληροφορία με την δουλειά που κάναμε με τα ορθογώνια ταυτοδύναμα στοιχεία. Ο διανυσματικός χώρος V είναι ένα $\overline{\mathbb{Q}}_p[\Delta]$-πρότυπο, άρα έχουμε

$$V = \bigoplus_{\psi \in \Delta^\wedge} \varepsilon_\psi V.$$

Υπενθυμίζουμε ότι μπορούμε να δούμε το χ σαν χαρακτήρα του $\mathrm{Gal}(F^\chi/F) \cong \Delta$. Ενδιαφερόμαστε για το

$$V^\chi := \varepsilon_\chi V = \{v \in V : \sigma v = \chi(\sigma) v \ \forall \sigma \in \Delta\}.$$

Είναι ξεκάθαρο ότι το V^χ παραμένει ένα Γ-πρότυπο, εφόσον το γ_0 δρα σαν $1+T$ όπως πριν. Θέτουμε $f_\chi(T)$ να είναι το χαρακτηριστικό πολυώνυμο της δράσης του $\gamma_0 - 1$ στο V^χ. Παρατηρούμε ότι $f_\chi(T) \mid f_X(T)$. Το χαρακτηριστικό πολυώνυμο μας δίνει μόνο την μισή πληροφορία που χρειαζόμαστε για την διατύπωση της κύριας εικασίας. Πριν προχωρήσουμε στο δεύτερο μισό, αξίζει να σημειωθεί ότι όταν πήραμε το τανυστικό γινόμενο με το $\overline{\mathbb{Q}}_p$ χάσαμε όλη τη πληροφορία που περιείχε το $\mu = \sum \mu_i$ στην εξίσωση 5.1. Θα επιστρέψουμε σε αυτό και θα δούμε πώς θα αναδιατυπώσουμε το παραπάνω επιχείρημα για να διατηρηθεί αυτή η πληροφορία.

Πρέπει τώρα να επιστρέψουμε στις p-αδικές L-συναρτήσεις. Για το σώμα $\mathbb{Q}$, είδαμε στο κεφάλαιο 3 την παρεμβολή που κάνουν με τις κλασικές L-συναρτήσεις. Έστω ψ ένας χαρακτήρας ενός πλήρως πραγματικού σώματος, έτσι ώστε το F^ψ να είναι και αυτό πλήρως πραγματικό. Οι Deligne και Ribet [6] απέδειξαν την ύπαρξη μιας p-αδικής L-συνάρτησης $\mathcal{L}_p(s, \psi)$ που αντιστοιχεί στο ψ, γενικεύοντας εκείνη στην περίπτωση του σώματος $\mathbb{Q}$ με τις ίδιες ιδιότητες παρεμβολής. Ορίζουμε

$$H_\psi(T) = \begin{cases} \psi(\gamma_0)(1+T) - 1, & \psi \text{ είναι τύπου } W \text{ ή τετριμμένο,} \\ 1, & \text{διαφορετικά.} \end{cases}$$

Οι Deligne και Ribet [6] απέδειξαν επίσης ότι υπάρχει $G_\psi(T) \in \mathcal{O}_\psi[[T]]$ έτσι ώστε

$$\mathcal{L}_p(1-s, \psi) = \frac{G_\psi((1+p)^s - 1)}{H_\psi((1+p)^s - 1)},$$

όπου $\mathcal{O}_\psi := \mathbb{Z}_p[\psi]$ ο δακτύλιος πάνω από το $\mathbb{Z}_p$ που παράγεται από τις τιμές που παίρνει ο χαρακτήρας ψ. Θα χρησιμοποιούμε τον συμβολισμό Λ_ψ για το $\mathcal{O}_\psi[[T]]$. Επιπλέον, αν ρ είναι ένας χαρακτήρας τύπου W τότε

$$G_{\psi\rho}(T) = G_\psi(\rho(\gamma_0)(1+T) - 1).$$

Έστω χ ένας περιττός χαρακτήρας και θέτουμε $\psi = \chi^{-1}\omega$, όπου ω είναι ο χαρακτήρας Teichmüller. Καθώς ο ψ είναι άρτιος χαρακτήρας έχουμε ότι υπάρχει για αυτόν η αντίστοιχη p-αδική L-συνάρτηση μαζί με το G_ψ. Από το θεώρημα προπαρασκευής του Weierstrass για το $G_\psi((1+p)(1+T)^{-1} - 1)$ έχουμε ότι

$$G_\psi((1+p)(1+T)^{-1} - 1) = \pi^{\mu_\chi^{\mathrm{an}}} g_\psi(T) u_\psi(T),$$

όπου π είναι ένας uniformizer του $\mathcal{O}_\psi$, το $g_\psi(T)$ είναι ένα distinguished πολυώνυμο και το $u_\psi(T)$ είναι αντιστρέψιμο στο Λ_ψ. Το an που προσθέσαμε στον συμβολισμό στο μ_χ είναι για να το ξεχωρίσουμε ως το «αναλυτικό» μ-αναλλοίωτο. Παρατηρούμε ότι αν το χ είναι τύπου S, τότε $H_\psi(T) = 1$ εκτός αν $\chi = \omega$.

Θεώρημα 5.1 (Κύρια Εικασία της Θεωρίας Iwasawa). *Για χ περιττό χαρακτήρα τύπου S και p έναν περιττό πρώτο έχουμε*

$$f_\chi(T) = g_{\chi^{-1}\omega}(T).$$

Για την περίπτωση όπου $p = 2$ μπορεί να συμβουλευτεί κανείς το [4]. Να σημειωθεί ότι δεν χρειαζόμαστε το χ να είναι τύπου S στην περίπτωση των αβελιανών επεκτάσεων του $\mathbb{Q}$.

Όπως αναφέραμε πριν, καθώς φτιάξαμε έναν διανυσματικό χώρο V από το X παίρνοντας το τανυστικό γινόμενο με το $\overline{\mathbb{Q}}_p$, χάσαμε την πληροφορία που περιέχουν τα μ_χ και μ_χ^{an} της κύριας εικασίας. Θα αναφέρουμε τώρα μια διαφορετική προσέγγιση με την οποία θα διατηρήσουμε αυτή τη πληροφορία. Υποθέτουμε ότι για τον χαρακτήρα χ εκτός από το να είναι περιττός και τύπου S θέλουμε να έχει τάξη σχετικά πρώτη με το p. Γράφουμε ως X^χ για να συμβολίσουμε το $(X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi)^\chi$ για το οποίο ισχύει ότι

$$\begin{aligned}(X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi)^\chi &= \{x \in X \otimes_{\mathbb{Z}_p} \mathcal{O}_\chi : \ \sigma x = \chi(\sigma)x \ \forall\ \sigma \in \Delta\} \\ &\cong X \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi,\end{aligned}$$

όπου βλέπουμε το $\mathcal{O}_\chi$ σαν ένα $\mathbb{Z}_p[\Delta]$-πρότυπο μέσα από τον ομομορφισμό δακτυλίων που επάγεται από το χ. Για να είναι καλά ορισμένο αυτό πρέπει να πάρουμε το τανυστικό γινόμενο με το $\mathbb{Z}_p[\chi]$, διαφορετικά ο όρος $\chi(\sigma)x$ δεν έχει νόημα. Έχουμε ότι το X^χ είναι ένα πεπερασμένα παραγόμενο Λ_χ-πρότυπο στρέψης και έχει χαρακτηριστικό πολυώνυμο της μορφής $\pi^{\mu_\chi} f_\chi(T)$.

Θεώρημα 5.2 (μ-αναλλοίωτη εικασία). *Έστω p ένας περιττός πρώτος και χ ένας περιττός χαρακτήρας τύπου S με τάξη σχετικά πρώτη ως προς το p. Τότε*

$$\mu_\chi = \mu_\chi^{\text{an}}.$$

Η ισχυρή αυτή διατύπωση της μ-αναλλοίωτης εικασίας επιπλέον μας λέει ότι αυτές οι αναλλοίωτες είναι 0 για τις κυκλοτομικές $\mathbb{Z}_p$-επεκτάσεις. Για τις αβελιανές επεκτάσεις, είναι γνωστή αυτή η ισχυρή έκδοση της εικασίας, και αποδεικνύεται εύκολα ως το θεώρημα 7.15 στο [1]. Αντιθέτως, υπάρχουν άλλες μη-κυκλοτομικές $\mathbb{Z}_p$-επεκτάσεις όπου οι μ-αναλλοίωτες δεν είναι 0. Ο Iwasawa κατασκεύασε μια τέτοια μη-κυκλοτομική επέκταση με $\mu > 0$ στο [5].

Υπάρχει ωστόσο ένας πιο κομψός τρόπος να διατυπωθεί η κύρια εικασία, έτσι ώστε να περιέχεται το νόημα των θεωρημάτων 5.1 και 5.2 σε μια έκφραση. Έστω M ένα πρότυπο έτσι ώστε

$$M \sim \left(\bigoplus_i \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j})\right)$$

με τα $f_j(T)$ να είναι ανάγωγα και distinguished. Το ιδεώδες που παράγεται από το χαρακτηριστικό πολυώνυμο

$$\text{char}_\Lambda(M) = \left(p^{\sum \mu_i} \prod f_j(T)_j^m\right)$$

λέγεται το *χαρακτηριστικό ιδεώδες* του M. Η κύρια εικασία μπορεί πλέον να διατυπωθεί ως την ισότητα των ακόλουθων ιδεωδών στον δακτύλιο Λ_χ:

$$\text{char}_{\Lambda_\chi}(X^\chi) = \left(G_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1)\right).$$

Να σημειωθεί ότι το $u_{\chi^{-1}\omega}(T)$ που προκύπτει όταν εφαρμόζουμε το θεώρημα προπαρασκευής του Weierstrass είναι ένα αντιστρέψιμο στοιχείο και άρα δεν παίζει ρόλο στην παραπάνω ισότητα.

Συνοψίζοντας, η κύρια εικασία μας δίνει την επιπλέον πληροφορία για τις p-αδικές L-συναρτήσεις, ότι εκτός από την μια αλγεβρική κατασκευή τους από τον Iwasawa με την χρήση των Stickelberger στοιχείων, όπως γίνεται στο θεώρημα 7.10 στο [1], έχουμε ότι δεν είναι και τίποτα παραπάνω από χαρακτηριστικές δυναμοσειρές συγκεκριμένων δράσεων Galois που εμφανίζονται μέσα στην θεωρία των $\mathbb{Z}_p$-επεκτάσεων.

5.2 Σύνδεση με Ομάδες Κλάσεων

Σε αυτήν την τελευταία ενότητα θα δώσουμε τους αναγκαίους ορισμούς ώστε να περιγράψουμε μια εφαρμογή της κύριας εικασίας στα μεγέθη των τάξεων των ομάδων κλάσεων ιδεωδών. Έστω p ένας περιττός πρώτος και F μια αβελιανή φανταστική επέκταση του $\mathbb{Q}$ βαθμού σχετικά πρώτου με το p. Έστω $\chi : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow \mathcal{O}_\chi^\times$ να είναι ένας περιττός χαρακτήρας. Θέτουμε $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Θα βλέπουμε τον χ ως χαρακτήρα του $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Έστω $g = [\mathcal{O}_\chi : \mathbb{Z}_p]$. Γράφουμε A_F για την p-Sylow υποομάδα της ομάδας κλάσεων του F. Ως συνήθως, γράφουμε A_F^χ για την χ-ισοτυπική συνιστώσα του A_F, δηλαδή

$$A_F^\chi = A_F \otimes_{\mathbb{Z}_p[\Delta]} \mathcal{O}_\chi.$$

Στόχος σε αυτή την ενότητα θα είναι με την χρήση της κύριας εικασίας να αποδειχτεί το παρακάτω αποτέλεσμα.

Θεώρημα 5.3. *Υποθέτουμε ότι $\chi \neq \omega$, τότε*

$$|A_F^\chi| = |\mathcal{O}_\chi/(\mathcal{L}_p(0, \chi^{-1}\omega))|.$$

Ειδικότερα,

$$\nu_p(|A_F^\chi|) = g \cdot \nu_p(L(0, \chi^{-1}))$$

για κάποιο $g \in \mathbb{N}$, όπου $\nu_p(a)$ είναι η p-αδική εκτίμηση του a.

Για ευκολία, θα θεωρήσουμε ότι $\chi(p) \neq 1$. Αν και το θεώρημα ισχύει για την περίπτωση που $\chi(p) = 1$, είναι αρκετά πιο δύσκολο να αποδειχθεί και πρέπει να ανατρέξει κανείς στο [3].

Ξεκινάμε με την περίπτωση που $F = \mathbb{Q}^\chi$. Για να φτάσουμε στο αποτέλεσμα, θα αποδείξουμε κάτι ελάχιστα πιο γενικό. Έστω K/E μια αβελιανή επέκταση σωμάτων αριθμών με $[K : E]$ να είναι σχετικά πρώτο ως προς το p και το χ να παραγοντοποιείται μέσα από το $\mathrm{Gal}(E/\mathbb{Q})$. Δείχνουμε ότι η φυσιολογική απεικόνιση

$$A_E^\chi \longrightarrow A_K^\chi$$

είναι ισομορφισμός. Έχοντας αυτό το αποτέλεσμα είναι εύκολο να δείξουμε την περίπτωση που $F = \mathbb{Q}^\chi$ με το να θέσουμε $K = F$ και $E = \mathbb{Q}^\chi$. Ξεκινάμε με το ακόλουθο λήμμα από την αλγεβρική θεωρία αριθμών.

Λήμμα 5.4. *Έστω K/E μια Galois επέκταση σωμάτων αριθμών με $[K : E] = n$ και $\gcd(n, h_E) = 1$. Τότε η φυσιολογική απεικόνιση $C_E \longrightarrow C_K$ είναι μια εμφύτευση.*

Απόδειξη. Η φυσιολογική απεικόνιση μεταξύ των ομάδων κλάσεων $C_E \longrightarrow C_K$ προκύπτει από την απεικόνιση

$$I_E \longrightarrow I_K$$
$$\mathfrak{a} \longmapsto \mathfrak{a}\mathcal{O}_K,$$

όπου I_E είναι τα κλασματικά ιδεώδη του $\mathcal{O}_E$ και όμοια για το I_K. Έστω $\mathfrak{a} \in I_E$ να ανήκει στον πυρήνα, δηλαδή να γίνεται κύριο στο I_K. Άρα υπάρχει $a \in K$ τέτοιο ώστε $\mathfrak{a}\mathcal{O}_K = (a)$. Υπενθυμίζουμε ότι αν απεικονίσουμε το $\mathfrak{a}$ μέσα στο I_K και πίσω στο I_E μέσω της απεικόνισης νόρμας, παίρνουμε ότι $\mathrm{Nm}(\mathfrak{a}\mathcal{O}_K) = \mathfrak{a}^{[K:E]}$. Επιπλέον, καθώς το $\mathfrak{a}\mathcal{O}_K$ είναι κύριο, έχουμε $\mathrm{Nm}(\mathfrak{a}\mathcal{O}_K) = (\mathrm{Nm}(a))$. Συνεπώς, έχουμε ότι $\mathfrak{a}^{[K:E]} = (\mathrm{Nm}(a))$, δηλαδή το $\mathfrak{a}^{[K:E]}$ είναι 0 στην ομάδα κλάσεων του E. Ωστόσο, έχουμε ότι η τάξη του $\mathfrak{a}$ διαιρεί το $[K : E]$ καθώς και το h_E. Εφόσον αυτά τα δύο τα θεωρήσαμε σχετικά πρώτα, έπεται ότι η τάξη του $\mathfrak{a}$ είναι 1 και άρα η απεικόνιση είναι εμφύτευση. □

Χρησιμοποιώντας αυτό το λήμμα βλέπουμε ότι το A_E^χ εμφυτεύεται μέσα στο A_K^χ. Καθώς το χ παραγοντοποιείται μέσα από την ομάδα $\mathrm{Gal}(E/\mathbb{Q})$ έπεται ότι είναι τετριμμένο στην $\mathrm{Gal}(K/E)$. Ειδικότερα, από τον ορισμό του A_K^χ βλέπουμε ότι ένα $\sigma \in \mathrm{Gal}(K/E)$ διατηρεί τα ιδεώδη στο A_K^χ αναλλοίωτα. Πιο συγκεκριμένα, για κάθε πρώτο ιδεώδες $\mathfrak{p}$ στο A_K^χ, έχουμε ότι $\sigma\mathfrak{p} = \mathfrak{p}$

για κάθε $\sigma \in \mathrm{Gal}(K/E)$. Ωστόσο, ξέρουμε ότι η $\mathrm{Gal}(K/E)$ μεταθέτει τους πρώτους $\mathfrak{p}$ που στέκονται πάνω από έναν ίδιο πρώτο $\mathfrak{q}$ του E. Άρα, μπορεί να υπάρχει μόνο ένας πρώτος πάνω από το $\mathfrak{q}$ για κάθε πρώτο ιδεώδες $\mathfrak{q} \in A_E^\chi$. Αυτό μας δείχνει ότι η παραπάνω απεικόνιση είναι επιμορφισμός και άρα ισομορφισμός όπως αναφέραμε.

Έστω L_n, L, X_n και X να είναι όπως στην προηγούμενη ενότητα. Συγκεκριμένα, ο στόχος μας είναι να προσδιορίσουμε την p-αδική εκτίμηση του $|X_0^\chi|$. Από την επιλογή μας για το χ έχουμε ότι $X_0^\chi = (X/TX)^\chi = X^\chi/TX^\chi$. Υπενθυμίζουμε ότι το X^χ είναι ένα πεπερασμένα παραγόμενο Λ_χ-πρότυπο στρέψης. Θέτουμε π να έιναι ένας uniformizer του $\mathcal{O}_\chi$. Από τα προηγούμενα κεφάλαια έχουμε ότι

$$X^\chi \sim \left(\bigoplus_i \Lambda_\chi/(\pi^{\mu_{\chi,i}})\right) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j})\right),$$

όπου θέσαμε $\mu_\chi = \sum \mu_{\chi,i}$ και τα $f_{\chi,j}$ είναι ανάγωγα και distinguished πολυώνυμα. Καθώς υποθέτουμε ότι ο χ είναι περιττός χαρακτήρας, έχουμε ότι ο παραπάνω ψευδο-ισομορφισμός είναι μια εμφύτευση με πεπερασμένο συνπυρήνα C. Για μια απόδειξη, μπορεί να ανατρέξει κανείς στην πρόταση 13.28 στο [1]. Συνεπώς, έχουμε το διάγραμμα

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X^\chi & \longrightarrow & \left(\bigoplus_i \Lambda_\chi/(\pi^{\mu_{\chi,i}})\right) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j})\right) & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle T^{(1)}} & & \downarrow{\scriptstyle T^{(2)}} & & \downarrow{\scriptstyle T^{(3)}} & & \\
0 & \longrightarrow & X^\chi & \longrightarrow & \left(\bigoplus_i \Lambda_\chi/(\pi^{\mu_{\chi,i}})\right) \oplus \left(\bigoplus_j \Lambda_\chi/(f_{\chi,j}(T)^{m_j})\right) & \longrightarrow & C & \longrightarrow & 0
\end{array}$$

όπου με $T^{(i)}$ εννοούμε σε κάθε περίπτωση πολλαπλασιασμό με T.

Λήμμα 5.5. *Ο πυρήνας της απεικόνισης $T^{(2)}$ είναι 0.*

Απόδειξη. Υποθέτουμε ότι $\ker T^{(2)} \neq 0$. Τότε θα ισχύει ότι $T \mid \prod_j f_{\chi,j}(T)^{m_j}$. Τότε, από την κύρια εικασία επάγεται ότι

$$T \mid G_{\chi^{-1}\omega}((1+p)(1+T)^{-1} - 1),$$

δηλαδή έχουμε

$$\begin{aligned}
0 &= G_{\chi^{-1}\omega}((1+p)-1) \\
&= \mathcal{L}_p(0, \chi^{-1}\omega) \\
&= (1-\chi^{-1}(p))L(0,\chi^{-1}),
\end{aligned}$$

όπου έχουμε χρησιμοποιήσει ότι $\chi \neq \omega$ για να συμπεράνουμε ότι $H_{\chi^{-1}\omega} = 1$. Ωστόσο, έχουμε υποθέσει ότι $\chi(p) \neq 1$ από υπόθεση και $L(0,\chi^{-1}) \neq 0$, εφόσον ο χ είναι περιττός χαρακτήρας. Συνεπώς, ο πυρήνας είναι αναγκαστικά τετριμμένος. □

Μπορούμε τώρα να εφαρμόσουμε το λήμμα του φιδιού καθώς και ότι $\ker T^{(2)} = 0$ για να πάρουμε την ακριβή ακολουθία

$$0 \longrightarrow \ker T^{(3)} \longrightarrow \mathrm{coker}\, T^{(1)} \longrightarrow \mathrm{coker}\, T^{(2)} \longrightarrow \mathrm{coker}\, T^{(3)} \longrightarrow 0$$

Έχουμε επιπλέον την ακριβή ακολουθία

$$0 \longrightarrow C[T] \longrightarrow C \xrightarrow{\cdot T} C \longrightarrow C/TC \longrightarrow 0$$

όπου $C[T] = \{c \in C : \ Tc = 0\}$. Χρησιμοποιούμε τώρα το γεγονός ότι αν έχουμε μια ακριβή ακολουθία πεπερασμένων ομάδων

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow D \longrightarrow 0$$

ισχύει ότι $|A| \cdot |B| \cdot |C|^{-1} \cdot |D|^{-1} = 1$, για να συμπεράνουμε ότι $|C[T]| = |C/TC|$. Παρατηρούμε ότι $C[T] = \ker T^{(3)}$ και $C/TC = \operatorname{coker} T^{(3)}$ παίρνουμε ότι $|\operatorname{coker} T^{(1)}| = |\operatorname{coker} T^{(2)}|$. Συνεπώς, έχουμε τις ακόλουθες ισότητες.

$$\begin{aligned}
|A_F^\chi| &= |X_0^\chi| \\
&= |X^\chi / TX^\chi| \\
&= |\operatorname{coker} T^{(1)}| \\
&= |\operatorname{coker} T^{(2)}| \\
&= \left| \bigoplus_i \Lambda_\chi / (\pi^{\mu_{\chi,i}}, T) \right| \cdot \left| \bigoplus_j \Lambda_\chi / (f_{\chi,j}(T)^{m_j}, T) \right| \\
&= |\Lambda_\chi / (f_\chi(T), T)| \qquad (5.2) \\
&= |\mathcal{O}_\chi / f_\chi(0)| \\
&= |\mathcal{O}_\chi / G_{\chi^{-1}\omega}(p)| \qquad (5.3) \\
&= |\mathcal{O}_\chi / \mathcal{L}_p(0, \chi^{-1}\omega)|,
\end{aligned}$$

όπου χρησιμοποιήσαμε στην ισότητα (5.2) ότι $\mu_\chi = 0$ από την κύρια εικασία καθώς βρισκόμαστε σε αβελιανή επέκταση. Επιπλέον, χρησιμοποιήσαμε την κύρια εικασία και στην ισότητα (5.3). Ειδικότερα, έχουμε ότι

$$|\mathcal{O}_\chi / \mathcal{L}_p(0, \chi^{-1}\omega)| = |\mathcal{O}_\chi / \left(L(0, \chi^{-1})(1 - \chi^{-1}(p)) \right)|.$$

Συνεπώς,

$$\nu_p(|A_F^\chi|) = \nu_p \left(\left| \mathcal{O}_\chi / \left(L(0, \chi^{-1})(1 - \chi^{-1}(p)) \right) \right| \right) = g \cdot \nu_p(L(0, \chi^{-1}))$$

όπως αναφέραμε.

Βιβλιογραφία

[1] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Second Edition, Springer (1991).

[2] J. Antoniadis and A. Kontogeorgis, *Algebraic Number Theory [Undergraduate textbook]*, Kallipos, Open Academic Editions, `https://dx.doi.org/10.57713/kallipos-8`, (2021).

[3] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76, 179-330 (1984).

[4] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Math. (2) 131 no. 3, 493-540 (1990).

[5] K. Iwasawa, *On the* μ*-invariants of* $\mathbb{Z}_\ell$*-extensions*, Number theory, Algebraic Geometry, and Commutative Algebra (in honor of Y. Akizuki), Kinokuniya: Tokyo, 1-11 (1973).

[6] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. 59, 227-286 (1980).

[7] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. 34, 151-162 (1976).

[8] J. Brown, *Iwasawa theory course notes*, Ohio State University, winter semester (2006).

[9] F. Q. Gouvêa, *P-adic numbers: An introduction*, Springer (2020).

[10] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, (2022), Online; accessed 5 December 2022.

[11] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*, Perseus Books, Cambridge, Mass. (1969).

[12] J.W.S Cassels and A. Frolich, *Algebraic Number Theory*, Academic Press Inc., Washington, D.C. (1967).

[13] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics 110, Springer-Verlag (1986).

[14] J.S. Milne, *Algebraic Number Theory*, `http://www.jmilne.org`.

[15] J.S. Milne, *Class Field Theory*, `http://www.jmilne.org`.