Γιάννη Α. Αντωνιάδη
Τμήμα Μαθηματικών, Πανεπιστήμιο Κρήτης

Θεωρία Αριθμών II

L-σειρές

Έκδοση ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ"
Πανεπιστήμιο Κρήτης
Ηράκλειο, 1999

Στο γυιό μας τον πρωτότοκο,

τον Αντώνη.

Περιεχόμενα

Εισαγωγή

Πρώτος ο Euler, κατά τον 18^o αιώνα, όρισε την ζήτα συνάρτηση και έκανε χρήση των ιδιοτήτων της για να δώσει μία επιπλέον, αλλά εντελώς διαφορετική, απόδειξη του γνωστού Θεωρήματος του Ευκλείδη ότι υπάρχουν άπειροι πρώτοι αριθμοί.

Η ανάπτυξη της μιγαδικής ανάλυσης κατά τον 19^o αιώνα έδωσε νέα ώθηση στη χρήση αναλυτικών μεθόδων για την απόδειξη αποτελεσμάτων της Θεωρίας των Αριθμών. Ο Dirichlet όριζει τις ομώνυμες L-σειρές και αποδεικνύει, μεταξύ άλλων, ότι σε κάθε αριθμητική πρόοδο $\{a+kn|(a,n)=1, k\in\mathbb{Z}\}$ υπάρχουν άπειροι πρώτοι αριθμοί. Ο Kummer αποδεικνύει σημαντικά αποτελέσματα σχετικά με την εικασία του Fermat. Η ζήτα συνάρτηση μελετάται από τον Riemann για μιγαδική μεταβλητή και, έκτοτε, αποκαλείται προς τιμή του **ζήτα συνάρτηση του Riemann**. Ακολουθεί ο ορισμός της **ζήτα συνάρτησης του Dedekind** αλγεβρικού σώματος αριθμών καθώς και των **αβελιανών L-σειρών**.

Στις αρχές του $20^{ου}$ αιώνα ορίζονται οι **L-σειρές του Artin**, οι οποίες αποτελούν γενίκευση αυτών του Dirichlet και της ζήτα συνάρτησης του Dedekind. Ένα μεγάλο μέρος της **Θεωρίας Κλάσεων Σωμάτων** (Class Field Theory) στηρίζεται στις ιδιότητες αυτών των σειρών. Τόση είναι η επιρροή αυτών των ιδεών στις μέρες μας, ώστε ο G. Harder να παρατηρήσει:

"Η ζήτα συνάρτηση γνωρίζει τα πάντα για το αλγεβρικό σώμα αριθμών. Δεν έχουμε παρά να την πείσουμε να μας τα αποκαλύψει."

(Δες [34], σελίδα 113.)

Κύριος σκοπός του βιβλίου είναι μία εισαγωγή στον φανταστικό αυτόν κλάδο της Θεωρίας των Αριθμών. Το περιεχόμενό του ποικίλλει, ως προς τον βαθμό δυσκολίας, ανάλογα με το κεφάλαιο.

Στο πρώτο κεφάλαιο μελετούμε ιδιότητες της ζήτα συνάρτησης του Riemann και των L-σειρών του Dirichlet. Για την κατανόησή των απαιτούνται αποκλειστικά γνώσεις μιγαδικής ανάλυσης.

Στη συνέχεια, στο δεύτερο κεφάλαιο, μελετούμε την κατανομή των ακεραίων ιδεωδών αλγεβρικού σώματος αριθμών σε κλάσεις ιδεωδών, ορίζουμε την ζήτα συνάρτηση του Dedekind αλγεβρικού σώματος αριθμών και μελετούμε τον αριθμό κλάσεων ιδεωδών τετραγωνικών σωμάτων αριθμών.

Στο τρίτο κεφάλαιο μελετούμε τον αριθμό κλάσεων ιδεωδών αβελιανών επεκτάσεων του σώματος των ρητών αριθμών (κυκλοτομικών σωμάτων).

Στο τέταρτο κεφάλαιο μελετούμε θεωρήματα πυκνότητας πρώτων ιδεωδών. Κύρια εργαλεία προσέγγισης του θέματος αυτού αποτελούν οι ιδιότητες των **αβελιανών L-σειρών** και κορωνίδα αποτελεί η απόδειξη του θεωρήματος του Čebotarev, το οποίο γενικεύει το θεώρημα του Dirichlet για αριθμητικές προόδους. Η κατανόηση του περιεχομένου του δεύτερου, τρίτου και τέταρτου κεφαλαίου προϋποθέτει γνώσεις ενός, μεταπτυχιακού επιπέδου, μαθήματος αλγεβρικής θεωρίας αριθμών, όπως, παραδείγματος χάρη, αυτές περιγράφονται στις σημειώσεις [2].

Στο πέμπτο κεφάλαιο γίνεται μικρή εισαγωγή στη **Θεωρία Κλάσεων Σωμάτων**.

Στο έκτο κεφάλαιο μελετώνται οι ιδιότητες των **L-σειρών του Artin (μη-αβελιανές L-σειρές)**. Στο κεφάλαιο αυτό απαιτούνται, πέραν των άλλων, και γνώσεις θεωρίας παραστάσεων πεπερασμένων ομάδων. Εν συντομία αναφέρονται ορισμοί και ιδιότητες. Για μία πλήρη ανάπτυξη της απαιτούμενης θεωρίας παραπέμπουμε στο [3].

Το κεφάλαιο αυτό κλείνει με μία μικρή αναφορά στις εικασίες του Stark.

Προκειμένου να κρατηθεί ο όγκος του βιβλίου σε ανεκτά όρια δεν συμπεριλάβαμε άλλες ζήτα συναρτήσεις και L-σειρές, όπως αυτές των αλγεβρικών σωμάτων συναρτήσεων μιάς μεταβλητής με σώμα σταθερών ένα πεπερασμένο σώμα, L-σειρές των modular συναρτήσεων, κ.λ.π., ούτε αναφερθήκαμε στη σημασία που έχουν οι L-σειρές ελλειπτικών καμπυλών για την μελέτη της αριθμητικής αυτών των καμπυλών.

Όλα αυτά θα αποτελέσουν, ελπίζουμε, το περιεχόμενο ενός άλλου βιβλίου.

Το περιεχόμενο του παρόντος βιβλίου έχει διδαχθεί είτε σαν μεταπτυχιακό μάθημα είτε σαν μάθημα μελέτης σε μεταπτυχιακούς φοιτητές του Τμήματός μας. Τα σχόλια και οι παρατηρήσεις τους ήταν για μένα πολύ χρήσιμα.

Το βιβλίο εκδίδεται μέσω του προγράμματος ΕΠΕΑΕΚ "ΠΡΟΜΗΘΕΑΣ" του Πανεπιστημίου Κρήτης. Θερμές ευχαριστίες χρωστώ στον υπεύθυνο του προγράμματος Αν. Καθηγητή κύριο Γιώργο Τζιρίτα. Τέλος θα ήθελα να ευχαριστήσω τον πτυχιούχο Μαθηματικό Παντελή Στουπά καθώς και τον μεταπτυχιακό φοιτητή του Τμήματος Επιστήμης Υπολογιστών David J. M^{c}Clurkin για την εξαιρετικά επιμελημένη ηλεκτρονική επεξεργασία του κειμένου.

Γιάννης Α. Αντωνιάδης, Καθηγητής

Ηράκλειο, Οκτώβριος 1999

Κεφάλαιο 1

Ζήτα συναρτήσεις και L-σειρές

1.1 Χαρακτήρες πεπερασμένων αβελιανών ομάδων

Ορισμός 1.1.1 *Έστω G μία πεπερασμένη ομάδα. Κάθε ομομορφισμός ομάδων*

$$\chi : G \longrightarrow \mathbb{C}^*$$

θα λέγεται **χαρακτήρας** *της G.*

Το γινόμενο δύο χαρακτήρων χ και χ' της G ορίζεται ως εξής:

$$\left(\chi \cdot \chi'\right)(g) := \chi(g)\chi'(g) \quad \text{για κάθε στοιχείο } g \text{ της } G.$$

Ο αντίστροφος ενός χαρακτήρα χ της ομάδας G ορίζεται

$$\chi^{-1}(g) := \chi(g)^{-1} \quad \text{για κάθε στοιχείο } g \text{ της } G.$$

Θεωρούμε το σύνολο

$$\widehat{G} = \{\chi \mid \chi \text{ χαρακτήρας της } G\}.$$

Προφανώς το σύνολο $\widehat{G}$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό χαρακτήρων.

Θεώρημα 1.1.2 *Αν G είναι πεπερασμένη αβελιανή ομάδα τότε $\widehat{G} \cong G$. Ιδιαίτερα ισχύει: $[\widehat{G} : 1] = [G : 1]$.*

Απόδειξη: Η ομάδα G αναλύεται σε ευθύ άθροισμα κυκλικών ομάδων. Αν $g_1, g_2, \ldots, g_k$ οι γεννήτορες αυτών των κυκλικών ομάδων τάξεων $n_1, n_2, \ldots, n_k$ αντίστοιχα, τότε κάθε $g \in G$ γράφεται στην μορφή

$$g = g_1^{r_1} g_2^{r_2} \ldots g_k^{r_k}, \quad r_1, r_2, \ldots, r_k \in \mathbb{Z}$$

Αν $\chi \in \widehat{G}$ και $\chi(g_i) = \xi_i \ (i = 1, 2, \dots, k)$ τότε

$$\xi_i^{n_i} \ = \ \chi(g_i)^{n_i} \ = \ \chi(g_i^{n_i}) \ = \ \chi(e) \ = \ 1$$

και

$$\chi(g) \ = \ \chi\left(g_1^{r_1} g_2^{r_2} \dots g_k^{r_k}\right) \ = \ \chi(g_1)^{r_1} \chi(g_2)^{r_2} \dots \chi(g_k)^{r_k} \ = \ \xi_1^{r_1} \xi_2^{r_2} \dots \xi_k^{r_k}$$

δηλαδή ξ_i n_i-ρίζες της μονάδας και ο χ ορίζεται μέσω των ξ_i.

Αντίστροφα, αν $\xi_1, \xi_2, \dots, \xi_k \in \mathbb{C}^*$ με $\xi_i^{n_i} = 1$, $i = 1, 2, \dots, k$ τότε η $\chi : G \to \mathbb{C}^*$

$$\chi\left(g_1^{r_1} g_2^{r_2} \dots g_k^{r_k}\right) \ := \ \xi_1^{r_1} \xi_2^{r_2} \dots \xi_k^{r_k}$$

είναι χαρακτήρας. Υπάρχει λοιπόν μία αμφιμονοσήμαντη αντιστοιχία ανάμεσα στους χαρακτήρες χ της G και στις k-άδες $(\xi_1, \xi_2, \dots, \xi_k)$ με $\xi_i^{n_i} = 1$ όπου το γινόμενο των χαρακτήρων αντιστοιχεί στο γινόμενο των ξ_i. Συνεπώς

$$\begin{aligned} \widehat{G} \ &\cong \ \left\{(\xi_1, \xi_2, \dots, \xi_k) \in \mathbb{C}^* \ \middle| \ \xi_1^{n_1} = \xi_2^{n_2} = \dots = \xi_k^{n_k} = 1\right\} \\ &\cong \ \mathbb{Z}\diagup_{n_1\mathbb{Z}} \times \mathbb{Z}\diagup_{n_2\mathbb{Z}} \times \dots \times \mathbb{Z}\diagup_{n_k\mathbb{Z}} \cong G. \quad \square \end{aligned}$$

Παρατήρηση: Αν G πεπερασμένη τότε $\chi(g)$ είναι ρίζα της μονάδας, δηλαδή για κάθε $g \in G$ έχουμε ότι $|\chi(g)| = 1 \Rightarrow \chi(g)\overline{\chi(g)} = 1$, οπότε μπορούμε να ορίσουμε τον **συζυγή** χαρακτήρα $\overline{\chi}$ του χ ως εξής:

$$\overline{\chi}(g) \ := \ \overline{\chi(g)} \quad \forall\, g \in G.$$

Ορισμός 1.1.3 *Έστω $N \in \mathbb{N}\setminus\{0\}$. Κάθε χαρακτήρας της $\mathbb{Z}_N^* = \left\{n (mod N) \ \middle| \ (n, N) = 1\right\}$ θα λέγεται* **χαρακτήρας Dirichlet mod** N.

Από τον ορισμό έχουμε ότι ο χ ορίζεται μόνο στα n για τα οποία $(n, N) = 1$. Επεκτείνομε λοιπόν τον ορισμό ως εξής:

$$\chi(n) \ := \ \begin{cases} \chi\left(n \bmod N\right), & \text{όταν } (n, N) = 1 \\ 0, & \text{όταν } (n, N) > 1 \end{cases}$$

και θα το ονομάζουμε και πάλι χαρακτήρα του Dirichlet.

Ώστε **χαρακτήρας του Dirichlet mod** N είναι μία συνάρτηση $\chi : \mathbb{Z} \to \mathbb{C}$ με τις εξής ιδιότητες:

1. $\chi(n) = 0 \iff (n, N) > 0$
2. χ πολλαπλασιαστική, δηλαδή $\chi(mn) = \chi(m)\chi(n) \quad \forall\, m, n \in \mathbb{Z}$
3. $\chi(n)$ εξαρτάται μόνο από $n \bmod N$

Από το Θεώρημα 1.1.2 έχουμε ότι $\exists!\ \varphi(N) = N \prod_{p|N} \left(1 - \frac{1}{p}\right)$ χαρακτήρες του Dirichlet $\bmod N$.

Παραδείγματα:

1. $\forall N \in \mathbb{N} \setminus \{0\}$ ο **κύριος** χαρακτήρας $\bmod N$ ορίζεται ως εξής:

$$\chi_0(n) := \begin{cases} 1, & \text{όταν } (n, N) = 1 \\ 0, & \text{όταν } (n, N) > 1 \end{cases}$$

2. Για $N = 2$ έχουμε $\varphi(N) = 1$, συνεπώς ο χ_o είναι **μοναδικός** χαρακτήρας $\bmod 2$.
   Για $N = 3, 4, 6$ έχουμε ότι $\varphi(N) = 2$ οπότε υπάρχει ακόμη ένας εκτός του κυρίου π.χ.
   για $N = 3$

n	0	1	2	3	4	5	6	...
$\varepsilon_3(n)$	0	1	-1	0	1	-1	0	...

   για $N = 4$

n	0	1	2	3	4	5	6	...
$\varepsilon_4(n)$	0	1	0	-1	0	1	0	...

   για $N = 5$, $\varphi(N) = 5\left(1 - \frac{1}{5}\right) = 4$ υπάρχουν ακόμα 3 χαρακτήρες

$n \pmod 5$	0	1	2	3	4
$\chi(n)$	0	1	i	$-i$	-1
	0	1	-1	-1	1
	0	1	$-i$	i	-1

3. Αν $p \in \mathbb{P}$ το σύμβολο του Legendre (Kronecker) είναι χαρακτήρας Dirichlet $\bmod p$

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & \text{όταν } p \text{ διαιρεί το } n \\ 1, & \text{όταν } p \text{ δεν διαιρεί το } n \text{ και } n \text{ τετραγωνικό υπόλοιπο } \bmod p \\ -1, & \text{όταν } p \text{ δεν διαιρεί το } n \text{ και } n \text{ όχι τετραγωνικό υπόλοιπο } \bmod p \end{cases}$$

Θεώρημα 1.1.4 *Αν χ χαρακτήρας Dirichlet mod N τότε ισχύει η*

$$S := \sum_{n \bmod N} \chi(n) = \begin{cases} \varphi(N), & \text{για } \chi = \chi_o \\ 0, & \text{για } \chi \neq \chi_o \end{cases} \tag{1.1}$$

Απόδειξη: Αν $\chi = \chi_o$, προφανώς $S = \varphi(N)$. Αν $\chi \neq \chi_o$ τότε $\exists\, n_o \bmod N$, $(n_o, N) = 1$, τέτοιο ώστε $\chi(n_o) \neq 1$. Όταν το n διατρέχει ένα πλήρες σύστημα αντιπροσώπων **πρώτων** κλάσεων υπολοίπων $\bmod N$ το ίδιο κάνει και το nn_o (δηλαδή $(n, N) = 1 \Leftrightarrow (nn_o, N) = 1$). Συνεπώς

$$S = \sum_{n \bmod N} \chi(n_o n) = \chi(n_o) S$$

άρα, επειδή $\chi(n_o) \neq 1$, έχομε ότι $S = 0$. □

Πόρισμα 1.1.5 *Αν χ_1, χ_2 είναι χαρακτήρες του Dirichlet mod N τότε*

$$\frac{1}{\varphi(N)} \sum_{n (mod\, N)} \chi_1(n)\overline{\chi_2}(n) = \begin{cases} 1, & \text{όταν } \chi_1 = \chi_2 \\ 0, & \text{όταν } \chi_1 \neq \chi_2 \end{cases} \tag{1.2}$$

Απόδειξη: Εφαρμόζουμε το θεώρημα για τον χαρακτήρα $\chi := \chi_1\overline{\chi_2}$. □

Εάν τώρα αθροίσουμε ως πρός τους χαρακτήρες, έχουμε το ακόλουθο θεώρημα.

Θεώρημα 1.1.6 *Για κάθε ακέραιο n ισχύει*

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(N), & \text{όταν } n \equiv 1\, (mod\, N) \\ 0, & \text{όταν } n \not\equiv 1\, (mod\, N) \end{cases}$$

όπου το χ στην άθροιση διατρέχει όλους τους χαρακτήρες Dirichlet mod N.

Απόδειξη: Αν $n \equiv 1 \pmod N$ τότε για όλους τους χαρακτήρες Dirichlet $\bmod N$ χ ισχύει ότι $\chi(n) = 1$. Το πλήθος αυτών είναι $\varphi(N)$. Επομένως, όταν $n \equiv 1 \pmod N$ έχουμε το ζητούμενο.

Αν τώρα $(n, N) > 1$ το θεώρημα ισχύει διότι για όλους τους χαρακτήρες Dirichlet $\bmod N$ θα ισχύει $\chi(n) = 0$. Έστω λοιπόν $n \not\equiv 1 \pmod N$, $(n, N) = 1$ και χ_1 ένας χαρακτήρας του Dirichlet $\bmod N$ τέτοιος ώστε $\chi_1(n) \neq 1$. Υπάρχει τέτοιος χαρακτήρας διότι οι χαρακτήρες χ με $\chi(n) = 1$ είναι χαρακτήρες της ομάδας πηλίκων $\left(\mathbb{Z}/N\mathbb{Z}\right)^* \Big/ \langle n \rangle$ της οποίας η τάξη είναι μικρότερη της τάξης της $\left(\mathbb{Z}/N\mathbb{Z}\right)^*$. Έχουμε λοιπόν:

$$\big(1 - \chi_1(n)\big) \sum_{\chi} \chi(n) = \sum_{\chi} [\chi(n) - \chi_1\chi(n)] = \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0.$$

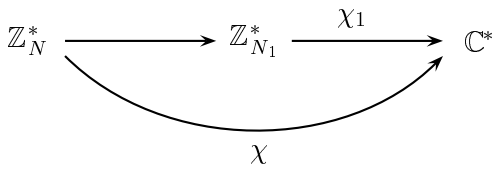
Λόγω της σχέσης $\chi_1(n) \neq 1$ έπεται ότι $\sum_\chi \chi(n) = 0$. □

Πόρισμα 1.1.7 *Αν $a, b \in \mathbb{Z}$, $(b, N) = 1$, τότε ισχύει:*

$$\frac{1}{\varphi(N)} \sum_\chi \chi(a)\overline{\chi}(b) = \begin{cases} 1, & \text{όταν } a \equiv b \,(mod\, N) \\ 0, & \text{όταν } a \not\equiv b \,(mod\, N) \end{cases}$$

Απόδειξη: Εφαρμόζουμε το θεώρημα για $n,\ nb \equiv a \pmod N$. □

Έστω τώρα $N_1 \,|\, N$, $N_1 \neq N$ και χ_1 ένας χαρακτήρας $\bmod N_1$. Η σύνθεση



όπου η πρώτη απεικόνιση είναι η αναγωγή $\bmod N_1$, ορίζει ένα **χαρακτήρα** $\bmod N$. Ο χ θα λέμε ότι **επάγεται** από τον χ_1 και θα λέγεται **μή πρωταρχικός**, αλλιώς θα λέγεται **πρωταρχικός**.

Σημείωση: Ο κύριος χαρακτήρας $\chi_0 \pmod N$ για $N > 1$ δεν είναι **ποτέ πρωταρχικός** διότι επάγεται από τον τετριμμένο χαρακτήρα $\bmod 1$.

Για κάθε χαρακτήρα του Dirichlet $\chi \pmod N$ υπάρχει **ελάχιστος** φυσικός N_1 τέτοιος ώστε ο χ επάγεται από τον $\chi_1 \pmod{N_1}$ όπου ο χ_1 είναι πρωταρχικός $\bmod N_1$. Τον φυσικό αυτόν τον N_1 θα τον ονομάζομε **οδηγό του χαρακτήρα** χ.

Ενδιαφερόμαστε προπαντός για **πραγματικούς χαρακτήρες** ($\chi = \overline{\chi}$) δηλαδή τέτοιους που παίρνουν τιμές πραγματικούς αριθμούς. Επειδή οι τιμές τους είναι ρίζες της μονάδας ή μηδέν οι χαρακτήρες αυτοί παίρνουν τιμές $0, -1, +1$. Το επόμενο θεώρημα θα μας δώσει όλους τους **πρωταρχικούς πραγματικούς χαρακτήρες**. Πρώτα όμως δίνουμε τον παρακάτω ορισμό.

Ορισμός 1.1.8 *Έστω D ακέραιος. Ο D θα λέγεται* **θεμελιώδης διακρίνουσα** *όταν ισχύουν:*

- *ο $D \equiv 1 \,(mod\, 4)$ και δεν διαιρείται με το τετράγωνο ακεραίου μεγαλύτερου του ένα (square free), ή*
- *ο $D \equiv 0 \,(mod\, 4)$, ο $\dfrac{D}{4}$ είναι square free και $\dfrac{D}{4} = 2$ ή $3 \,(mod\, 4)$.*

Έστω D θεμελιώδης διακρίνουσα. **Ορίζουμε** τη συνάρτηση $\chi_D : \mathbb{N} \longrightarrow \mathbb{Z}$ ως εξής:

1. $\chi_D(p) = \left(\dfrac{D}{p}\right)$, όπου $p \in \mathbb{P} \setminus \{2\}$

2. $\chi_D(2) = \begin{cases} 0, & \text{όταν } D \equiv 0 \pmod 4 \\ 1, & \text{όταν } D \equiv 1 \pmod 8 \\ -1, & \text{όταν } D \equiv 5 \pmod 8 \end{cases}$

3. $\chi_D\left(p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}\right) = \chi_D(p_1)^{n_1} \chi_D(p_2)^{n_2} \cdots \chi_D(p_k)^{n_k}$

Ισχύει λοιπόν το ακόλουθο

Θεώρημα 1.1.9 *Έστω D θεμελιώδης διακρίνουσα. Η συνάρτηση*

$$n \longmapsto \chi_D(n)$$

είναι **περιοδική** *mod $|D|$ και ορίζει έναν* **πρωταρχικό** *χαρακτήρα του Dirichlet mod $|D|$, όπου*

$$\chi_D(-1) = \begin{cases} 1, & \text{όταν } D > 0 \\ -1, & \text{όταν } D < 0 \end{cases}$$

Κάθε **πρωταρχικός πραγματικός χαρακτήρας** *του Dirichlet είναι χαρακτήρας της μορφής χ_D.*

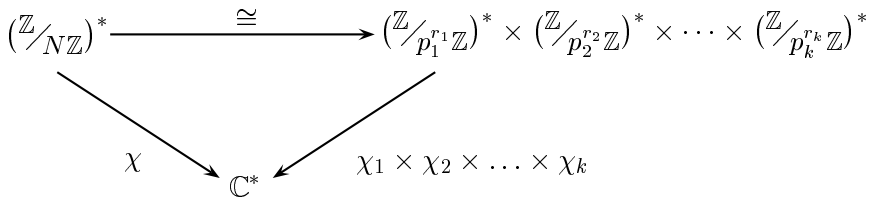
Απόδειξη: Έστω $N = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ η ανάλυση του N σε γινόμενο πρώτων παραγόντων. Για κάθε κλάση $a \bmod N$ ορίζουμε τις "συνιστώσες" a_i

$$\left\{ \begin{array}{rcl} a_i & \equiv & a \bmod p_i^{r_i} \\ a_i & \equiv & 1 \bmod \dfrac{N}{p_i^{r_i}} \end{array} \right\} \quad \text{Θεώρημα υπολοίπων του Κινέζου}$$

Επομένως έχουμε $a \equiv a_1 a_2 \dots a_k \pmod N$.

Ορίζουμε $\chi_i(a) := \chi(a_i)$ όπου χ κάποιος χαρακτήρας Dirichlet $(\bmod N)$. Προφανώς η χ_i είναι χαρακτήρας του Dirichlet $\bmod p_i^{r_i}$ και $\chi(a) = \chi(a_1)\chi(a_2)\dots\chi(a_k) = \chi_1(a)\,\chi_2(a)\dots\chi_k(a) = (\chi_1\chi_2\dots\chi_k)(a)$, συνεπώς $\chi = \chi_1\chi_2\dots\chi_k$. Η παραπάνω ανάλυση είναι **μοναδική**. Πράγματι αν $\chi = \chi_1'\chi_2'\dots\chi_k'$ τότε $\chi_i(a) = \chi(a_i) = \chi_1'(a_i)\chi_2'(a_i)\dots\chi_k'(a_i) = \chi_i'(a_i) = \chi_i'(a)$ διότι $\chi_j'(a_i) = 1$ για κάθε $i \neq j$ καθ' όσον $a_i \equiv 1 \bmod p_j^{r_j}$ $(j \neq i)$. Συνεπώς $\chi_i = \chi_i'$.

Έχουμε λοιπόν το ακόλουθο αντιμεταθετικό διάγραμμα:



Επομένως ο χ είναι **πρωταρχικός** χαρακτήρας $\bmod N$ ακριβώς τότε όταν όλοι οι χ_i είναι **πρωταρχικοί** $\bmod p_i^{r_i}$. Για την ταξινόμηση όλων αυτών των χαρακτήρων αρκεί να εξετάσουμε την περίπτωση $N = p^r$, $p \in \mathbb{P}$.

1. Έστω $p \in \mathbb{P}$ με $p \neq 2$. Είναι γνωστό ότι η ομάδα $(\mathbb{Z}/p^r\mathbb{Z})^*$ είναι κυκλική. Έστω x ένας γεννήτορας της ομάδας αυτής (πρωταρχική ρίζα $\bmod p^r$!). Αν ο χαρακτήρας χ είναι πραγματικός και $\chi \neq \chi_0$ τότε θα πρέπει $\chi(x) = -1$ και συνεπώς υπάρχει το πολύ ένας τέτοιος χαρακτήρας. Από την άλλη μεριά η απεικόνιση $n \mapsto \left(\frac{n}{p}\right)$ είναι ένας πραγματικός χαρακτήρας $(\bmod p^r)$ διάφορος του χ_0 ο οποίος έχει οδηγό το p. Ώστε, για κάθε πρώτο $p \neq 2$, υπάρχει **ακριβώς ένας πραγματικός πρωταρχικός** χαρακτήρας $\chi \pmod p$. Αυτός είναι ο $\chi_p(n) = \left(\frac{n}{p}\right)$. **Δεν υπάρχει** πραγματικός πρωταρχικός χαρακτήρας $\bmod p^r$ για $r > 1$.

2. Εάν $p = 2$ τότε για $r = 1$ η ομάδα $(\mathbb{Z}/2\mathbb{Z})^*$ είναι τετριμμένη, δηλαδή έχει μόνο τον χαρακτήρα $\chi = \chi_0$.
   Για $r = 2$ έχουμε $(\mathbb{Z}/2^r\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z}$, συνεπώς ο ε_4 είναι ο μοναδικός χαρακτήρας διαφορετικός από τον χ_0 ο οποίος είναι πρωταρχικός.
   Για $r = 3$ έχουμε $(\mathbb{Z}/2^r\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ και υπάρχουν ακριβώς 2 χαρακτήρες οι οποίοι δίνονται από τον παρακάτω πίνακα.

$n \pmod 8$	0	1	2	3	4	5	6	7	...
$\varepsilon_8'(n)$	0	1	0	-1	0	-1	0	1	...
$\varepsilon_8''(n)$	0	1	0	1	0	-1	0	-1	...

   ε_8' και ε_8'' είναι πραγματικοί πρωταρχικοί χαρακτήρες. (Αν $\chi(3) = \alpha$ και $\chi(5) = \beta$ τότε $\chi(7) = \chi(3 \cdot 5) = \alpha\beta$, $\alpha, \beta \in \{-1, +1\}$ και από τις τέσσερις δυνατότητες που έχουμε οι δύο μάς δίνουν τους μη-πρωταρχικούς χαρακτήρες χ_0 και ε_4). Για $r > 3$ ισχύει ότι

αν $n \equiv 1 \pmod 8$ τότε $n \equiv k^2 \bmod 2^r$ όπου $k \in \mathbb{Z}$. (Δες [38], σελίδα 241, Proposition A11.) Οπότε για χ πραγματικό έχουμε ότι

$$\chi(n) = \chi\left(k^2\right) = \chi^2(k) = (\pm 1)^2 = 1,$$

δηλαδή ο χ **δεν** μπορεί να είναι πρωταρχικός. Επομένως υπάρχει μοναδικός πραγματικός πρωταρχικός χαρακτήρας $\varepsilon_4 \bmod 4$ και υπάρχουν δύο πραγματικοί πρωτεύοντες χαρακτήρες ε_8' και $\varepsilon_8'' \bmod 8$.

Για $r \neq 2, 3$ **δεν** υπάρχουν πραγματικοί πρωταρχικοί χαρακτήρες $\bmod 2^r$.

Όλοι λοιπόν οι πραγματικοί πρωταρχικοί χαρακτήρες έχουν οδηγό της μορφής:

$$\begin{aligned} & 1 \text{ ή } 4 \text{ ή } 8 \quad \textbf{επί} \text{ γινόμενο περιττών πρώτων} \\ = \; & 1 \text{ ή } 4 \text{ ή } 8 \quad \textbf{επί} \text{ κάποιον περιττό ``square free'' ακέραιο.} \end{aligned}$$

Κάνοντας τώρα χρήση του τετραγωνικού νόμου αντιστροφής έχουμε $\chi_{p'}(n) = \left(\dfrac{n}{p}\right)$ για $p' = (-1)^{\frac{p-1}{2}} p,\ p \neq 2$ και

$$\begin{aligned} \varepsilon_4(n) &= \left(\frac{-4}{n}\right) = \chi_{-4}(n) \\ \varepsilon_8'(n) &= \left(\frac{8}{n}\right) = \chi_8(n) \\ \varepsilon_8''(n) &= \left(\frac{-8}{n}\right) = \chi_{-8}(n). \end{aligned}$$

Από την άλλη μεριά το γινόμενο δύο θεμελιωδών δικρινουσών D_1 και D_2 με $(D_1, D_2) = 1$ είναι επίσης θεμελιώδης διακρίνουσα και ισχύει $\chi_{D_1 D_2} = \chi_{D_1} \cdot \chi_{D_2}$. Αποδείχτηκε δηλαδή ότι οι πραγματικοί **πρωταρχικοί** χαρακτήρες είναι ακριβώς οι χ_D όπου το D γινόμενο πρώτων μεταξύ τους αριθμών από το σύνολο

$$\Big\{-4, +8, -8,\ p \text{ πρώτος } \big(\text{αν } p \equiv 1 \pmod 4\big), -p\ \big(\text{αν } p \equiv 3 \pmod 4\big)\Big\}.$$

Από την άλλη μεριά κάθε θεμελιώδης διακρίνουσα είναι αυτής της μορφής, δηλαδή

$$D = m,\ -4m,\ 8m,\ -8m$$

και m square free, $m \equiv 1 \pmod 4$.

Απομένει να αποδείξομε την τελική έκφραση του θεωρήματος. Αρκεί να το δούμε για διακρίνουσα -4, $+8$, -8, p ($p \equiv 1 \pmod 4$), $-p$ ($p \equiv 3 \pmod 4$). Πράγματι:

$$\begin{aligned}
\chi_{-4}(-1) &= \varepsilon_4(-1) = -1 = \operatorname{sign}(-4) \\
\chi_{8}(-1) &= \varepsilon'_8(-1) = 1 = \operatorname{sign}(8) \\
\chi_{-8}(-1) &= \varepsilon''_8(-1) = -1 = \operatorname{sign}(-8) \\
\chi_{p'}(-1) &= \left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}
\end{aligned}$$

το οποίο είναι ίσο με $\operatorname{sign}(p')$.

□

1.2 Σειρές του Dirichlet (γενικότητες)

Οι σειρές του Dirichlet παίζουν στην αναλυτική θεωρία αριθμών, τόσο σημαντικό ρόλο όσο οι δυναμοσειρές στη θεωρία μιγαδικών συναρτήσεων. Στη θεωρία των δυναμοσειρών παίρνει κανείς την συνάρτηση $z \mapsto z^n$ ($n \in \mathbb{N}$) και προσπαθεί οποιαδήποτε άλλη συνάρτηση να την παραστήσει σαν άπειρο γραμμικό συνδυασμό τέτοιων. Στις σειρές Dirichlet παίρνουμε την εκθετική συνάρτηση

$$z \longmapsto e^{-\lambda z} \quad (\lambda \in \mathbb{R})$$

και, αφού το $\mathbb{R}$ είναι υπεραριθμήσιμο, περιοριζόμαστε σε μία ακολουθία

$$\left\{ z \to e^{-\lambda_n z} \right\}_{n \in \mathbb{N}}$$

όπου λ_n ακολουθία πραγματικών αριθμών με $\lambda_1 < \lambda_2 < \cdots < \lambda_n \to \infty$. Η μιγαδική μεταβλητή θα συμβολίζεται με $s = \sigma + it$.

Ορισμός 1.2.1 *Μία* **σειρά Dirichlet** *είναι μία σειρά της μορφής*

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$$

όπου $\{\lambda_n\}$ *ακολουθία πραγματικών αριθμών με* $\lambda_1 < \lambda_2 < \ldots < \lambda_n \to \infty$, a_n *αυθαίρετοι μιγαδικοί αριθμοί και* $s = \sigma + it \in \mathbb{C}$.

Παραδείγματα:

1. Έστω ότι $\lambda_n = n$ για κάθε φυσικό αριθμό n. Σ΄ αυτήν την περίπτωση δέν οδηγούμαστε σε καμμία καινούργια θεωρία διότι η αντικατάσταση $z = e^{-s}$ δίνει την μορφή $\sum a_n z^n$ δηλαδή σ΄ αυτήν τη περίπτωση, η θεωρία των σειρών Dirichlet ταυτίζεται με τη θεωρία των δυναμοσειρών.

2. Έστω $\lambda_n = \log n$, οπότε η σειρά γράφεται $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. Αυτή τη μορφή θα χρειαστούμε και μ΄ αυτή θα ασχοληθούμε παρακάτω. Από εδώ και πέρα θα τη λέμε **συνήθη σειρά Dirichlet**.

   Το πρώτο πρόβλημα που θα εξετάσουμε, είναι το **πότε** και **πού συγκλίνει** μία σειρά Dirichlet.

   Για τις δυναμοσειρές γνωρίζουμε παραδείγματος χάριν την ύπαρξη της ακτίνας σύγκλισης οπότε για $\lambda_n = n$ και $z = e^{-s}$ που είχαμε στο παράδειγμα (1) μπορούμε να βγάλουμε το εξής συμπέρασμα: υπάρχει $\sigma_0 = log\left(\frac{1}{R}\right) \in \mathbb{R}$ τέτοιο ώστε η σειρά του Dirichlet **συγκλίνει** για κάθε $s = \sigma + it \in \mathbb{C}$ με $\mathrm{Re}(\sigma) > \sigma_0$, **αποκλίνει** για κάθε $s \in \mathbb{C}$ με $\mathrm{Re}(\sigma) < \sigma_0$ ενώ **δεν** μπορούμε να πούμε τίποτα για $\sigma = \sigma_0$. Σκοπός μας τώρα είναι να το αποδείξομε για όλες τις σειρές του Dirichlet. Αν και η απόδειξη είναι ίδια στην γενική περίπτωση εμείς εδώ θα περιοριστούμε, από εδώ και κάτω, στις **συνήθεις σειρές Dirichlet**.

Θεώρημα 1.2.2 *Αν η σειρά Dirichlet* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *συγκλίνει για* $s = s_0$, *τότε* **συγκλίνει για όλα τα** s **με** $\mathbf{Re}(s) > \mathbf{Re}(s_0)$ *και μάλιστα* **ομοιόμορφα σε συμπαγή υποσύνολα του ημιεπιπέδου** $\mathbf{Re}(s) > \mathbf{Re}(s_0)$.

Απόδειξη: Θα αποδείξομε κάτι γενικότερο, ότι δηλαδή σε **κάθε** τόπο της μορφής

$$\left|\arg(s - s_0)\right| \leq \frac{\pi}{2} - \theta < \frac{\pi}{2}$$

έχουμε ομοιόμορφη σύγκλιση, οπότε τελειώνουμε αφού κάθε συμπαγές υποσύνολο του ημιεπιπέδου $\mathrm{Re}(s) > \mathrm{Re}(s_0)$ περιέχεται σε κάποιο τέτοιο τόπο. Κατ΄ αρχήν, χωρίς περιορισμό της γενικότητας, μπορούμε να υποθέσουμε ότι $s_0 = 0$. $\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^{s_0}} \cdot \frac{1}{n^{s-s_0}} = \sum_{n=1}^{\infty} \frac{b_n}{n^{s-s_0}}\right.$ οπότε σύγκλιση της αρχικής σειράς για $s = s_0$ είναι ισοδύναμη με τη σύγκλιση της τελευταίας για $s - s_0 = 0$.$\left.\right)$

Αφού λοιπόν εξ υποθέσεως συγκλίνει για $s_0 = 0$ έχουμε ότι η $\sum_{n=1}^{\infty} a_n$ **συγκλίνει**, δηλαδή

$$\forall\, \varepsilon > 0 \;\; \exists\, N_0 \in \mathbb{N} \;\text{ τέτοιος ώστε }\; |A(M,N)| \le \varepsilon \;\text{ για όλα τα }\; N > M \ge N_0$$

όπου

$$A(M,N) := \sum_{n=M}^{N} a_n, \quad A(N) := \sum_{n=1}^{N} a_n \quad \text{και} \quad A(M,M-1) := 0.$$

Επομένως για $N > M \ge N_0$ ισχύει

$$\begin{aligned}
\sum_{n=M}^{N} a_n e^{-\lambda_n s} &= \sum_{n=M}^{N} \Big[\, A(M,n) - A(M,n-1) \,\Big]\, e^{-\lambda_n s} \\
&= A(M,M)e^{-\lambda_M s} - A(M,M)e^{-\lambda_{M+1} s} \\
&\quad + A(M,M+1)e^{-\lambda_{M+1} s} - A(M,M+1)e^{-\lambda_{M+2} s} \\
&\quad \vdots \\
&\quad + A(M,N-1)e^{-\lambda_{N-1} s} - A(M,N-1)e^{-\lambda_N s} \\
&\quad + A(M,N)e^{-\lambda_N s} \\
&= \sum_{n=M}^{N-1} A(M,n)\left[e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right] + A(M,N)e^{-\lambda_N s}.
\end{aligned}$$

Η παραπάνω διαδικασία είναι το λεγόμενο λήμμα του Abel. Τώρα

$$\begin{aligned}
\left|e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right| &= \left|\, s \int_{\lambda_n}^{\lambda_{n+1}} e^{-su}du \,\right| \\
\le\; |s| \int_{\lambda_n}^{\lambda_{n+1}} \left|e^{-su}\right| du &= |s| \int_{\lambda_n}^{\lambda_{n+1}} e^{-\sigma u}du \\
= \frac{|s|}{\sigma}\left(e^{-\lambda_n \sigma} - e^{-\lambda_{n+1}\sigma}\right).&
\end{aligned}$$

Για s μέσα στην περιοχή που ορίσαμε, έχουμε:

$$\frac{|s|}{\sigma} = \frac{1}{\cos|\arg s|} \le \frac{1}{\cos\left(\frac{\pi}{2} - \theta\right)} = \frac{1}{\sin\theta}$$

οπότε, για $\sigma > 0$, έχουμε

$$\begin{aligned}
\left|\sum_{n=M}^{N} a_n e^{-\lambda_n s}\right| &\le \sum_{n=M}^{N-1} \left|A(M,n)\right| \cdot \left|e^{-\lambda_n s} - e^{-\lambda_{n+1} s}\right| + \left|A(M,N)\right| \cdot \left|e^{-\lambda_N s}\right| \\
&\le \frac{1}{\sin\theta}\,\varepsilon \sum_{n=M}^{N-1} \left(e^{-\lambda_n \sigma} - e^{-\lambda_{n+1}\sigma}\right) + \varepsilon e^{-\lambda_N \sigma} \\
&\le \frac{1}{\sin\theta}\,\varepsilon e^{-\lambda_M \sigma} + \varepsilon e^{-\lambda_N \sigma} < \left(\frac{1}{\sin\theta} + 1\right) e^{-\lambda_{N_0}\sigma}\,\varepsilon,
\end{aligned}$$

δηλαδή αποδείξαμε την αλήθεια του θεωρήματος. □

Το θεώρημα αυτό μάς δίνει ότι μία σειρά του Dirichlet συγκλίνει σε κάποιο ημιεπίπεδο. Πράγματι αν

$$U = \left\{\sigma \in \mathbb{R} \;\middle|\; \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ συγκλίνει}\right\} \text{ και}$$

$$L = \left\{\sigma \in \mathbb{R} \;\middle|\; \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ αποκλίνει } \forall s : \mathrm{Re}(s) = \sigma\right\}$$

τότε κάθε στοιχείο του U είναι μεγαλύτερο από κάθε στοιχείο του L και η ταξινόμηση αυτή ορίζει έναν πραγματικό σ_0 τέτοιο ώστε να έχουμε σύγκλιση για κάθε $\sigma > \sigma_0$ και απόκλιση για κάθε $\sigma < \sigma_0$.

Αν $U = \emptyset$ τότε $\sigma_0 = +\infty$

Αν $L = \emptyset$ τότε $\sigma_0 = -\infty$

Ορισμός 1.2.3 *Το σημείο σ_0 θα λέγεται* **σημείο αρχής της σύγκλισης**. *Η ευθεία $\sigma = \sigma_0$ είναι η* **γραμμή σύγκλισης** *και το ημιεπίπεδο $\sigma > \sigma_0$ είναι το* **ημιεπίπεδο σύγκλισης της σειράς Dirichlet**.

Άσκηση: Να δειχθεί ότι η σειρά $\displaystyle\sum_{n=1}^{\infty} \frac{n!}{n^s}$ δεν συγκλίνει πουθενά, δηλαδή το σημείο αρχής της σύγκλισης σ_0 είναι στο $+\infty$, ενώ η σειρά $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n!n^s}$ συγκλίνει παντού, δηλαδή $\sigma_0 = -\infty$.

Συνδυάζοντας τώρα το θεώρημα 1.2.2 και το γνωστό θεώρημα του Weierstrass για σειρές συναρτήσεων (δες [1], σελίδα 176).

Θεώρημα 1.2.4 *Κάθε σειρά Dirichlet παριστά στο ημιεπίπεδο σύγκλισής της μία* **ολόμορφη συνάρτηση του** s *της οποίας οι διαδοχικές παράγωγοι λαμβάνονται παραγωγίζοντας τη σειρά* **κατά όρους**.

Φυσιολογικά τίθεται το ερώτημα στη συνέχεια για την εύρεση του σ_0 και τη συμπεριφορά της συνάρτησης (όριο σύγκλισης της σειράς Dirichlet στο $\sigma > \sigma_0$) στη γραμμή σύγκλισης $\sigma = \sigma_0$. Έχουμε το ανάλογο της ακτίνας σύγκλισης των δυναμοσειρών;
Θα αποδείξουμε το ακόλουθο

Θεώρημα 1.2.5 *Έστω $\displaystyle\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$ μία σειρά του Dirichlet και έστω ότι η $\displaystyle\sum_{n=1}^{\infty} a_n$ αποκλίνει. Τότε*

$$\sigma_0 = \limsup_{N\to\infty} \frac{\log|A(N)|}{\lambda_N}$$

$$\left(A(N) := \sum_{n=1}^{N} a_n \right).$$

Παράδειγμα: Αν $\sum_{n=1}^{\infty} a_n$ συγκλίνει τότε το θεώρημα ισχύει και πάλι αρκεί να αντικαταστήσουμε το $A(N)$ με το $\sum_{N}^{\infty} a_n$. Επίσης μπορούμε πάντα να μεταφέρουμε τη σειρά έτσι ώστε $\sigma_0 > 0$, δηλαδή η σειρά $\sum_{n=1}^{\infty} a_n$ να αποκλίνει.

Απόδειξη: Για λόγους ευκολίας θα αποδείξουμε το θεώρημα για **συνήθεις** σειρές Dirichlet, δηλαδή για $\lambda_N = \log N$. Για την απόδειξη της γενικής περίπτωσης παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο βιβλίο του T. M. Apostol [5], σελίδα 161. Θα πρέπει λοιπόν να δείξουμε ότι

$$\sigma_0 \;=\; \gamma \;:=\; \limsup_{N\to\infty} \frac{\log|A(N)|}{\log N} \;=\; \inf\{\alpha \;\mid\; \alpha > 0,\; A(N) = O(N^{\alpha})\}$$

(Ο συμβολισμός $A(N) = O\left(N^{\alpha}\right)$ σημαίνει ότι υπάρχει $B > 0$ τ.ω $|A(N)| \le BN^{\alpha}$ για όλα τα N). Έστω $\sigma > \sigma_0$. Τότε η σειρά $\sum a_n n^{-\sigma}$ συγκλίνει. Άρα θα έχουμε ότι

$$\left| \sum_{n=1}^{N} a_n n^{-\sigma} \right| < C$$

για **όλα** τα $N \in \mathbb{N}$ και κατάλληλη σταθερά C. Όπως και πιο μπροστά, κάνοντας χρήση του λήμματος του Abel, έχουμε

$$\begin{aligned}
|A(N)| &= \left| \sum_{n=1}^{N-1} \left(a_n n^{-\sigma}\right) n^{\sigma} \right| \\
&= \left| \sum_{n=1}^{N-1} \left(\sum_{m=1}^{n} a_m m^{-\sigma} \right) \left(\; n^{\sigma} - (n+1)^{\sigma} \; \right) + \left(\sum_{n=1}^{N} a_n n^{-\sigma} \right) N^{\sigma} \right| \\
&\overset{(\sigma>0)}{\le} \sum_{n=1}^{N-1} \left| \sum_{m=1}^{n} a_m m^{-\sigma} \right| \left(\; (n+1)^{\sigma} - n^{\sigma} \; \right) + \left| \sum_{n=1}^{N} a_n n^{-\sigma} \right| N^{\sigma} \\
&< C \sum_{n=1}^{N-1} \left(\; (n+1)^{\sigma} - n^{\sigma} \; \right) + CN^{\sigma} \;<\; 2CN^{\sigma}.
\end{aligned}$$

Αν τώρα $\gamma := \inf\left\{\alpha \;\mid\; \exists N_0 \in \mathbb{N} \text{ τ.ω. } \forall N \ge N_0 \;\; \dfrac{\log|A(N)|}{\log N} < \alpha\right\}$ τότε ο γ θα είναι, εξ ορισμού, μικρότερος είτε ίσος προς τον σ και, αφού αυτό ισχύει για όλα τα σ με $\sigma > \sigma_0$, θα έχουμε ότι $\gamma \le \sigma_0$. Έστω τώρα $\sigma > \gamma$. Εφαρμόζοντας ξανά το λήμμα του Abel βρίσκουμε

$$\sum_{n=1}^{N} a_n n^{-\sigma} \;=\; \sum_{n=1}^{N-1} A(n) \left(\; n^{-\sigma} - (n+1)^{-\sigma} \; \right) + A(N) N^{-\sigma}. \tag{1.3}$$

Διαλέγουμε α με $\gamma < \alpha < \sigma$ και μία σταθερά C με $\big|\, A(N) \,\big| \leq CN^{\alpha}$ για κάθε N, οπότε έχουμε:

$$\begin{aligned} \Big|A(n)\big(n^{-\sigma} - (n+1)^{-\sigma}\big)\Big| &\overset{(\sigma>0)}{\leq} Cn^{\alpha}\big(n^{-\sigma} - (n+1)^{-\sigma}\big) \\ &= Cn^{\alpha}\sigma \int_{n}^{n+1} x^{-\sigma-1}dx \\ &< C\sigma n^{\alpha-\sigma-1} \end{aligned}$$

και $\big|A(N)N^{-\sigma}\big| \leq CN^{\alpha-\sigma} \to 0$ καθώς $N \to \infty$. Η σύγκλιση της σειράς $\displaystyle\sum_{n=1}^{\infty} n^{\alpha-\sigma-1}$ μας δίνει ένα **πεπερασμένο** όριο καθώς $N \to \infty$. Επομένως το δεξί μέλος της (1.3) συγκλίνει, όταν $N \to \infty$, συνεπώς και η σειρά $\displaystyle\sum_{n=1}^{\infty} a_n n^{-\sigma}$ συγκλίνει άρα $\sigma \geq \sigma_0$ και (αφού ισχύει για κάθε $\sigma > \gamma$) έπεται ότι $\gamma \geq \sigma_0$, δηλαδή τελικά $\gamma = \sigma_0$. □

Παραδείγματα:

1. Έστω $\zeta(s) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s}$ η περίφημη ζήτα συνάρτηση του Riemann. Έχουμε

$$a_n = 1,\ A(N) = N \implies \sigma_0 = \gamma = 1$$

δηλαδή η σειρά συγκλίνει για $\sigma > 1$.

2. Έστω τώρα η $\psi(s) := 1 - \dfrac{1}{2^s} + \dfrac{1}{3^s} - \cdots$ εδώ

$$a_n = (-1)^{n-1},\ A(N) := \begin{cases} 1, & \text{όταν } N \text{ είναι περιττός} \\ 0, & \text{όταν } N \text{ είναι άρτιος} \end{cases}$$

συνεπώς $\sigma_0 = \gamma = 0$ δηλαδή η σειρά συγκλίνει για $\sigma > 0$ και ορίζει στο ημιεπίπεδο αυτό μία **ολόμορφη** συνάρτηση. Για $\sigma > 1$ όμως είναι προφανές ότι

$$\psi(s) \;=\; \zeta(s) - 2\left(\frac{1}{2^s} + \frac{1}{4^s} + \ldots\right) \;=\; \big(1 - 2^{1-s}\big)\zeta(s),$$

δηλαδή έχουμε μία μέθοδο να επεκτείνουμε την $\zeta(s)$ μερόμορφα στο ημιεπίπεδο $\sigma > 0$, όπου οι πιθανοί πόλοι βρίσκονται το πολύ στα σημεία

$$s = 1,\ 1 \pm \frac{2\pi i}{\log 2},\ 1 \pm \frac{4\pi i}{\log 2}, \ldots$$

όπου μηδενίζεται ο $1 - 2^{1-s}$.

Σημαντική διαφορά από τις δυναμοσειρές.

Ο τύπος $R = \liminf|a_n|^{-\frac{1}{n}}$ δίνει αμέσως ότι οι $\sum a_n z^n$ και $\sum|a_n|z^n$ έχουν την **ίδια** ακτίνα σύγκλισης και μάλιστα όπου συγκλίνει η σειρά μέσα στον ανοικτό δίσκο σύγκλισης εκεί συγκλίνει και **απόλυτα**.

Στο παράδειγμα μας όμως η $\psi(s)$ συγκλίνει για $\sigma > 0$, ενώ συγκλίνει απόλυτα για $\sigma > 1$.

Στην περίπτωση της **συνήθους** σειράς Dirichlet ισχύει το

Θεώρημα 1.2.6 *Έστω ότι η σειρά Dirichlet* $\sum_{n=1}^{\infty} a_n n^{-s}$ *έχει σημείο αρχής σύγκλισης* σ_0 *ενώ η* $\sum_{n=1}^{\infty}|a_n|n^{-s}$ *το* σ_1. *Τότε ισχύει:*

$$\sigma_1 \leq \sigma_0 + 1, \ \ \delta\eta\lambda\alpha\delta\acute{\eta} \ 0 \leq \sigma_1 - \sigma_0 \leq 1.$$

Απόδειξη: Αρκεί να δείξουμε ότι αν η $\sum \frac{a_n}{n^s}$ συγκλίνει για κάποια τιμή s_0 τότε θα συγκλίνει **απόλυτα** για **όλα** τα s με $\sigma > \sigma_0 + 1$. Έστω A ένα άνω φράγμα των αριθμών $\left|\frac{a_n}{n^{s_0}}\right|$. (Υπάρχει τέτοιο αφού εξ υποθέσεως για $s = s_0$ η σειρά $\sum \frac{a_n}{n^{s_0}}$ συγκλίνει). Επομένως

$$\left|\frac{a_n}{n^s}\right| = \left|\frac{a_n}{n^{s_0}}\right| \cdot \left|\frac{1}{n^{s-s_0}}\right| \leq \frac{A}{n^{\sigma-\sigma_0}}$$

για $\sigma > \sigma_0 + 1 \Longrightarrow \sigma - \sigma_0 > 1 \Longrightarrow \sum \frac{1}{n^{\sigma-\sigma_0}}$ **συγκλίνει**, άρα και η σειρά $\sum\left|\frac{a_n}{n^s}\right|$ **συγκλίνει**. □

Το θεώρημα ισχύει μόνο για συνήθεις σειρές Dirichlet (αντιπαραδείγματα θα βρείτε παραδείγματος χάριν στο [10], σελίδα 115).

Υπάρχει και άλλη πολύ πιο σπουδαία διαφορά των σειρών Dirichlet από αυτή των δυναμοσειρών.

Στις δυναμοσειρές, αν η $\sum a_n z^n$ παριστά μια συνάρτηση η οποία επεκτείνεται **ολόμορφα** στον ανοικτό δίσκο $|z| < r$ τότε αυτή συγκλίνει σ΄ αυτόν τον δίσκο. Αυτό **δεν** ισχύει για σειρές Dirichlet (μπορεί να δει κανείς ότι $\psi(s)$ η οποία ορίζεται για $\sigma > 0$ επεκτείνεται ολόμορφα σ'ολο το μιγαδικό επίπεδο, αλλά η σειρά $\psi(s) = \sum_{n=0}^{\infty}(-1)^n \frac{1}{n^s}$ συγκλίνει **μόνο** για $\sigma > 0$.

Ισχύει όμως, σαν ειδική περίπτωση, το παρακάτω θεώρημα.

Θεώρημα 1.2.7 (Θεώρημα του Landau) *Έστω* $\sigma_0 \in \mathbb{R}$ *το αρχικό σημείο σύγκλισης της σειράς* $\sum_{n=1}^{\infty} a_n n^{-s}$ *και έστω ότι* $a_n \in \mathbb{R}$ *για κάθε* $n \in \mathbb{N}$ *και* $a_n \geq 0$. *Τότε η συνάρτηση* $f(s)$

που ορίζεται από τη σειρά Dirichlet

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \gamma\iota\alpha \ \sigma > \sigma_0$$

έχει ανωμαλία στο $\sigma = \sigma_0$.

Απόδειξη: Αφού $a_n \geq 0$ έχουμε $\sigma_1 = \sigma_0$ (για τον ορισμό του σ_1 δες προηγούμενο θεώρημα). Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\sigma_0 = 0$. Αν $f(s)$ ολόμορφη στο $s = 0$ τότε αυτή θα ήταν ολόμορφη σε κάποιο δίσκο $|s| < \varepsilon$ και (αφού για $\sigma > \sigma_0 = 0$ είναι ολόμορφη (δες Θεώρημα 1.2.4) το ανάπτυγμα Taylor της $f(s)$ στο σημείο $s = 1$ θα είχε ακτίνα σύγκλισης $R > 1$. Θα υπήρχε λοιπόν ένα $s \in \mathbb{R}$, $s < 0$ για το οποίο, το ανάπτυγμα Taylor

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} f^{(\nu)}(1)$$

θα συνέκλινε. Αλλά για $\sigma > 0$, $f(s) = \sum_{n=1}^{\infty} a_n e^{-s \log n}$, οπότε από Θεώρημα 1.2.4, έχουμε

$$f^{(\nu)}(s) \ = \ \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n^s}$$

και για $s = 1$

$$f^{(\nu)}(1) \ = \ \sum_{n=1}^{\infty} a_n \frac{(-\log n)^\nu}{n}$$

Το ανάπτυγμα Taylor λοιπόν της f για $s = 1$ είναι:

$$\sum_{\nu=0}^{\infty} \frac{(s-1)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{a_n(-\log n)^\nu}{n} \ = \ \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu}{\nu!} \sum_{n=1}^{\infty} \frac{a_n(\log n)^\nu}{n}.$$

Της διπλοσειράς όλοι οι όροι είναι μη-αρνητικοί, αν $s < 0$ (έχουμε δηλαδή απόλυτη σύγκλιση!) οπότε μπορούμε να αλλάξουμε τη σειρά πρόσθεσης, συνεπώς η προηγούμενη σχέση μπορεί να πάρει τη μορφή

$$\sum_{n=1}^{\infty} \frac{a_n}{n} \ \sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!}$$

Έχουμε λοιπόν σύγκλιση αυτής της σεράς για κάποιο $s < 0$. Επίσης έχουμε ότι

$$\sum_{\nu=0}^{\infty} \frac{(1-s)^\nu (\log n)^\nu}{\nu!} \ = \ e^{(1-s)\log n} \ = \ n^{1-s}.$$

Επομένως η σειρά $\sum_{n=1}^{\infty} a_n n^{-s}$ συγκλίνει για κάποιο $s < 0$ το οποίο είναι άτοπο, διότι $\sigma_0 = 0$, δηλαδή θα πρέπει η $f(s)$ να έχει **ανωμαλία** στο $s = 0$. □

Θα κλείσουμε αυτήν την παράγραφο με ένα θεώρημα **μοναδικότητας των συντελεστών** μιας σειράς Dirichlet. Συγκεκριμένα θα αποδείξουμε το

Θεώρημα 1.2.8 *Αν οι σειρές Dirichlet*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \textit{και} \quad \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

συγκλίνουν σε κάποιο κοινό ημιεπίπεδο και οι συναρτήσεις που ορίζουν, έστω $f_1(s)$ και $f_2(s)$, συμπίπτουν σε κάποιο μη-κενό, **ανοικτό** *σύνολο που περιέχεται στο ημιεπίπεδο κοινής σύγκλισης, τότε $a_n = b_n$ για όλα τα $n \geq 1$.*

Απόδειξη: Θεωρούμε τη σειρά Dirichlet

$$\sum_{n=1}^{\infty} \frac{(a_n - b_n)}{n^s}$$

Αυτή συγκλίνει στο ημιεπίπεδο $\sigma > \sigma_0$ όπου και ορίζει ολόμορφη συνάρτηση, έστω $f(s)$. Η συνάρτηση αυτή μηδενίζεται σε κάποιο ανοικτό σύνολο που περιέχεται στο ημιεπίπεδο $\sigma > \sigma_0$. Επομένως $f(s) \equiv 0$ στο $\sigma > \sigma_0$. Έστω M ο ελάχιστος φυσικός τέτοιος ώστε $a_M \neq b_M$ και έστω $c_n = a_n - b_n$. Για $\sigma > \sigma_0$ έχουμε λοιπόν

$$\sum_{n=1}^{\infty} \frac{c_n}{n^\sigma} = \sum_{n=M}^{\infty} \frac{c_n}{n^\sigma} = 0 \qquad \text{ή} \qquad \frac{c_M}{M^\sigma} = -\sum_{n=M+1}^{\infty} \frac{c_n}{n^\sigma}.$$

Επομένως

$$|c_M| \leq \sum_{n=M+1}^{\infty} |c_n| \left(\frac{M}{n}\right)^\sigma, \qquad \sigma > \sigma_0 + 1$$

Αν τώρα πάρουμε το σ τέτοιο ώστε $\sigma > \sigma_0 + 2$ τότε, λόγω **ομοιόμορφης σύγκλισης**, αν $\sigma \to \infty$ έπεται ότι $c_M = 0$ το οποίο είναι άτοπο. Συνεπώς δεν υπάρχει τέτοιο M και επομένως ισχύει $a_n = b_n$ για κάθε $n \geq 1$. □

Σημείωση: Η έννοια της σειράς του Dirichlet είναι ειδική περίπτωση της έννοιας του μετασχηματισμού Laplace ως προς κάποιο μέτρο μ. Αυτό είναι εξορισμού η συνάρτηση

$$\int_0^\infty e^{-zt} d\mu(t).$$

Η περίπτωση των σειρών Dirichlet που θεωρούμε εδώ είναι για μ ένα **διακριτό** (discrete) μέτρο.

1.3 Σειρές του Dirichlet (τυπικές ιδιότητες)

Η πρόσθεση σειρών Dirichlet ορίζεται τελείως φυσιολογικά σαν η σειρά που έχει συντελεστές το άθροισμα των αντιστοίχων συντελεστών. Τί γίνεται όμως με το γινόμενο; Έστω

$$f(s)=\sum_{n=1}^{\infty}a_n n^{-s} \quad \text{και} \quad g(s)=\sum_{m=1}^{\infty}b_m m^{-s}$$

δύο συναρτήσεις οι οποίες ορίζονται σε κάποιο **ανοικτό** σύνολο U μέσω της **απόλυτης σύγκλισης** των σειρών Dirichlet που τις ορίζουν. Στο U λοιπόν έχουμε

$$\begin{aligned} f(s)g(s) &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}a_n b_m n^{-s}m^{-s} \\ &= \sum_{n,m=1}^{\infty}a_n b_m (nm)^{-s} \;=\; \sum_{k=1}^{\infty}c_k k^{-s} \\ \text{όπου} \qquad c_k &= \sum_{\substack{n,m>1\\ mn=k}}^{\infty}a_n b_m \;=\; \sum_{n|k}a_n b_{\frac{k}{n}} \end{aligned}$$

Η παραπάνω έκφραση των συντελεστών c_k που είναι πολλαπλασιαστική, σε αντίθεση με τις δυναμοσειρές που είναι προσθετική, είναι αυτή για την οποία οι σειρές Dirichlet έχουν μεγίστη σημασία για τη Θεωρία των Αριθμών.

Εύκολα αποδεικνύεται ότι η σειρά $\displaystyle\sum_{k=1}^{\infty}c_k k^{-s}$ συγκλίνει όταν τουλάχιστον μία από αυτές συγκλίνει απλά και η άλλη απόλυτα.

Παραδείγματα:

1. Έστω $d(n)$ το πλήθος των θετικών διαιρετών του φυσικού αριθμού n. Τότε, για $\sigma>1$,

$$\sum_{n=1}^{\infty}\frac{d(n)}{n^s} \;=\; \zeta(s)^2 \quad \text{διότι} \quad d(n)=\sum_{d|n}1\times 1$$

2. Έστω $\tau(n)$ το άθροισμα των θετικών διαιρετών του n ή γενικότερα

$$\sigma_k(n) \;=\; \sum_{d|n}d^k \;=\; 1\times d^k$$

τότε ισχύει

$$\sum_{n=1}^{\infty}\frac{\sigma_k(n)}{n^s} \;=\; \zeta(s)\,\zeta(s-k) \qquad (\sigma>k+1).$$

Και στα δύο παραδείγματα οι συναρτήσεις μέσω των οποίων ορίζονται οι συντελεστές των σειρών είναι **πολλαπλασιαστικές**. Ξαναθυμίζουμε τον ορισμό.

Ορισμός 1.3.1 *Η συνάρτηση* $f : \mathbb{N} \to \mathbb{C}$ *θα λέγεται* **πολλαπλασιστική** *συνάρτηση όταν*

$$f(mn) \;=\; f(m)f(n)$$

για όλους τους φυσικούς m, n *πρώτους μεταξύ τους και υπάρχει τουλάχιστο ένας φυσικός* n_0 *τέτοιος ώστε* $f(n_0) \neq 0$. *Επιπλέον θα λέγεται* **πλήρως πολλαπλασιαστική** *συνάρτηση όταν απαλείψουμε τον περιορισμό* $(m, n) = 1$.

Στα 1737 ο Euler ανακάλυψε και απέδειξε το παρακάτω θεώρημα.

Θεώρημα 1.3.2 (Γινόμενο Euler) *Αν* f **πολλαπλασιαστική** *και* $\displaystyle\sum_{n=1}^{\infty} f(n)$ **απολύτως συγκλίνουσα** *τότε*

$$\sum_{n=1}^{\infty} f(n) \;=\; \prod_{p\in\mathbb{P}} \{1 + f(p) + f(p^2) + \cdots\}$$

και το απειρογινόμενο συγκλίνει απολύτως. Αν f **πλήρως πολλαπλασιαστική** *τότε*

$$\sum_{n=1}^{\infty} f(n) \;=\; \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)}.$$

Απόδειξη: Κατ' αρχήν ορίζουμε

$$P(x) \;:=\; \prod_{p\leq x} \{1 + f(p) + f(p^2) + \cdots\}.$$

Το $P(x)$ είναι πεπερασμένο γινόμενο απόλυτα συγκλινουσών σειρών, συνεπώς μπορούμε να πολλαπλασιάσουμε ή να αλλάξουμε τη σειρά των όρων, χωρίς να αλλάξει το άθροισμα. Θα έχουμε δηλαδή γινόμενα της μορφής

$$f(p_1^{\alpha_1})f(p_2^{\alpha_2})\cdots f(p_\nu^{\alpha_\nu}) \;=\; f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_\nu^{\alpha_\nu}).$$

Το θεμελιώδες θεώρημα της αριθμητικής μας δίνει

$$P(x) \;=\; \sum_{n\,\in\, A} f(n)$$

όπου $A = \{n \in \mathbb{N} \;\big|\; \text{οι πρώτοι παράγοντες του } n \text{ είναι όλοι} \leq x\}$. Επομένως

$$\sum_{n=1}^{\infty} f(n) \;-\; P(x) \;=\; \sum_{n\,\in\, B} f(n)$$

όπου $B = \{n \in \mathbb{N} \;\big|\; \exists\, p \in \mathbb{P},\ p|n, \text{ τέτοιος ώστε } p > x\}$. Άρα

$$\left|\sum_{n=1}^{\infty} f(n) \;-\; P(x)\right| \;\leq\; \sum_{n\,\in\, B} |f(n)| \;\leq\; \sum_{n>x} |f(n)|.$$

Τώρα αφού η $\sum_{n=1}^{\infty}|f(n)|$ συγκλίνει, έπεται ότι για $x\to\infty$ το $\sum_{n>x}^{\infty}|f(n)|\to 0$. Επίσης είναι γνωστό ότι:

$$\prod(1+a_n)\ \text{ συγκλίνει απόλυτα} \quad\Longleftrightarrow\quad \sum|a_n|\ \text{ συγκλίνει}$$

(δες [1], σελίδα 192).

Επίσης έχουμε ότι

$$\sum_{p\le x}|f(p)+f(p^2)+\dots|\ \le\ \sum_{p\le x}\Big(|f(p)|+|f(p^2)|+\dots\Big)\ \le\ \sum_{n=2}^{\infty}|f(n)|.$$

Αφού όλα τα μερικά αθροίσματα είναι πεπερασμένα, η σειρά θετικών όρων

$$\sum_{p\in\mathbb{P}}|f(p)+f(p^2)+\cdots|$$

συγκλίνει, οπότε και το αντίστοιχο απειρογινόμενο συγκλίνει απόλυτα. Τώρα αν η f είναι πλήρως πολλαπλασιαστική τότε $f(p^n)=f(p)^n$ για κάθε πρώτο p και έχουμε συγκλίνουσες γεωμετρικές σειρές με άθροισμα $\dfrac{1}{1-f(p)}$. □

Θεώρημα 1.3.3 *Αν υποθέσουμε ότι η σειρά Dirichlet* $\displaystyle\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ *συγκλίνει* **απόλυτα** *για* $\sigma>\sigma_0$, *όπου* f **πολλαπλασιαστική** *συνάρτηση, τότε*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\ =\ \prod_{p\in\mathbb{P}}\left\{1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\cdots\right\},\quad \text{για } \sigma>\sigma_0.$$

Αν f **πλήρως πολλαπλασιαστική** *συνάρτηση, τότε*

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\ =\ \prod_{p\in\mathbb{P}}\frac{1}{1-f(p)\,p^{-s}},\quad \text{για } \sigma>\sigma_0$$

Το παραπάνω θεώρημα ειναι άμεση συνέπεια του θεωρήματος 1.3.2 για $g(n)=\dfrac{f(n)}{n^s}$.

Παραδείγματα:

1. $\zeta(s)\ =\ \displaystyle\sum_{n=1}^{\infty}\frac{1}{n^s}\ =\ \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}},\quad \text{για } \sigma>1$

2. $\displaystyle\sum_{n=1}^{\infty}\frac{d(n)}{n^s}\ =\ \zeta(s)^2\ =\ \prod_{p\in\mathbb{P}}(1-p^{-s})^{-2}$

1.4 Οι L-σειρές του Dirichlet

Στη συνέχεια θα συνδέσουμε τη θεωρία των σειρών του Dirichlet με την θεωρία των χαρακτήρων πεπερασμένων ομάδων που αναπτύξαμε στην πρώτη παράγραφο.

Έστω $N \in \mathbb{N}$ και χ ένας χαρακτήρας Dirichlet $mod\, N$. Η **L-σειρά Dirichlet** ορίζεται ως εξής:

$$L(s/\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \tag{1.4}$$

Αφού $\left|\chi(n)\right| \leq 1$ για κάθε φυσικό αριθμό n, συνεπάγεται ότι $\left|\dfrac{\chi(n)}{n^s}\right| \leq \dfrac{1}{n^\sigma}$, άρα η $L(s/\chi)$ συγκλίνει απόλυτα για $\sigma > 1$.

Αφού χ πολλαπλασιαστική συνάρτηση θα έχουμε ότι

$$L(s/\chi) = \prod_{p\in\mathbb{P}} \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \cdots\right)$$

και μάλιστα, αφού χ πλήρως πολλαπλασιστική,

$$L(s/\chi) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad (\sigma > 1) \tag{1.5}$$

Ιδιαίτερα για $\chi = \chi_0$ έχουμε

$$\begin{aligned} L(s/\chi_0) &= \prod_{p\in\mathbb{P}} \left(1 - \chi_0(p)p^{-s}\right)^{-1} \\ &= \prod_{p\nmid N} \left(1 - p^{-s}\right)^{-1} \\ &= \prod_{p|N} \left(1 - p^{-s}\right) \prod_{p\in\mathbb{P}} \left(1 - p^{-s}\right)^{-1} \\ &= \zeta(s) \prod_{p|N} \left(1 - p^{-s}\right), \end{aligned}$$

δηλαδή η L-σειρά Dirichlet για $\chi = \chi_0$ είναι ίση με τη ζήτα συνάρτηση του Riemann πολλαπλασιασμένη με σταθερά που εξαρτάται **μόνο** από το N.

Αν δεχτούμε σαν γνωστή την ιδιότητα της ζήτα συνάρτησης του Riemann, ότι επεκτείνεται μερόμορφα σ΄ όλο το μιγαδικό επίπεδο και μάλιστα έχει μοναδικό απλό πόλο στη θέση $s = 1$ και υπόλοιπο ίσο με 1, κάτι το οποίο θα αποδείξουμε σε επόμενη παράγραφο, τότε το συμπέρασμα για την $L(s/\chi_0)$ είναι ότι επεκτείνεται μερόμορφα σ'ολο το μιγαδικό επίπεδο με μοναδικό πόλο στη θέση $s = 1$ και υπόλοιπο ίσο προς

$$\prod_{p|N} \left(1 - p^{-1}\right) = \frac{\varphi(N)}{N}.$$

Αν τώρα $\chi \neq \chi_0$ και $x \to \infty$ τότε

$$\begin{aligned}\left|\sum_{n=1}^{x}\chi(n)\right| &= \left|\sum_{n=1}^{N\left[\frac{x}{N}\right]}\chi(n)+\sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\ &= \left|\left[\frac{x}{N}\right]\sum_{n(modN)}\chi(n)+\sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\ &= \left|\sum_{n=N\left[\frac{x}{N}\right]+1}^{x}\chi(n)\right| \\ &\leq \left|x-N\left[\frac{x}{N}\right]\right| \leq N = O(1)\end{aligned}$$

οπότε, από θεώρημα 1.2.5, έχουμε ότι $\sigma_0 \leq 0$. Επειδή η σειρά αποκλίνει για $\sigma_0 < 0$ θα έχουμε κατ' ανάγκη $\sigma_0 = 0$.

Επομένως για $\chi \neq \chi_0$ και $\sigma > 0$ η $L(s/\chi)$ είναι μία ολόμορφη συνάρτηση. Για $\chi \neq \chi_0$ μπορεί να αποδειχθεί ότι η $L(s,\chi)$ επιδέχεται **ολόμορφη επέκταση** σ' όλο το μιγαδικό επίπεδο (δες [44], σελίδα 51).

Η πιο σημαντική ίσως ιδιότητα των L-σειρών του Dirichlet περιέχεται στο:

Θεώρημα 1.4.1 *Αν $\chi \neq \chi_0$ τότε*

$$L(1/\chi) \neq 0.$$

Απόδειξη: Έστω

$$F(s) := \prod_{\chi} L(s/\chi) \tag{1.6}$$

όπου το χ διατρέχει όλους τους χαρακτήρες Dirichlet $\bmod N$. Λόγω του γινομένου Euler (1.5) για $\sigma > 1$ ισχύει:

$$\begin{aligned}\log F(s) &= \sum_{\chi}\sum_{p\in\mathbb{P}}\log\left(1-\chi(p)p^{-s}\right)^{-1} \\ &= \sum_{\chi}\sum_{p\in\mathbb{P}}\sum_{r=1}^{\infty}\frac{1}{r}\,\frac{\chi(p)^r}{p^{rs}} \\ &= \sum_{\chi}\chi(p)^r\sum_{p\in\mathbb{P}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}} \\ &= \varphi(N)\sum_{\substack{p\in\mathbb{P}\\ p^r\equiv 1 \bmod N}}\sum_{r=1}^{\infty}\frac{1}{rp^{rs}}\end{aligned}$$

διότι

$$\sum_{\chi} \chi(n) \;:=\; \begin{cases} \varphi(N), & \text{όταν } n \equiv 1 \,(\mathrm{mod}\, N) \\ 0, & \text{όταν } n \not\equiv 1 \,(\mathrm{mod}\, N). \end{cases}$$

Ιδιαίτερα για $s \in \mathbb{R}$ και $s > 1$ ισχύει $\log F(s) \geq 0$. Δηλαδή

$$\liminf_{\substack{s \to 1^+ \\ s \in \mathbb{R}}} F(s) \;\geq\; 1. \tag{1.7}$$

Το γινόμενο (1.6) περιέχει μόνο ένα **απλό πόλο** στη θέση $s = 1$ που προκύπτει από την $L(s/\chi_0)$. Αν $L(1/\chi) = 0$ για δύο ή περισσότερους χαρακτήρες $\chi \neq \chi_0$ τότε ο απλός πόλος της $L(s/\chi_0)$ στο $s = 1$ θα αναιρούνταν από την μία $L(s/\chi)$ με $L(1/\chi) = 0$ οπότε η $F(s)$ θα ήταν ολόμορφη στη θέση $s = 1$ και θα έπαιρνε για $s = 1$ την τιμή 0 λόγω του μηδενισμού της άλλης L-σειράς, άτοπο, λόγω της (1.7). Άρα το πολύ για ένα χαρακτήρα $\chi \neq \chi_0$ μπορεί να ισχύει $L(1/\chi) = 0$.
Άν τώρα $L(1/\chi) = 0$ τότε

$$L(1/\overline{\chi}) \;=\; \overline{L(1/\chi)} \;=\; 0,$$

οπότε θα έπρεπε και $\chi = \overline{\chi}$, δηλαδή ο χ θα έπρεπε να είναι **πραγματικός** χαρακτήρας.
Έστω λοιπόν χ πραγματικός χαρακτήρας με $L(1/\chi) = 0$. Ορίζουμε

$$\psi(s) := L(s/\chi)\zeta(s) = \sum_{n=1}^{\infty} \frac{\rho(n)}{n^s} \quad \text{όπου} \quad \rho(n) = \sum_{d|n} \chi(d)$$

$$\begin{aligned} \psi(s) &= \prod_{p} \frac{1}{(1-\chi(p)p^{-s})\,(1-p^{-s})} \\ &= \prod_{\chi(p)=1} \frac{1}{(1-p^{-s})^2} \prod_{\chi(p)=0} \frac{1}{1-p^{-s}} \prod_{\chi(p)=-1} \frac{1}{1-p^{-2s}} \\ &= \prod_{\chi(p)=1} \left(1+\frac{2}{p^s}+\frac{3}{p^{2s}}+\cdots\right) \prod_{\chi(p)=0} \left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots\right) \prod_{\chi(p)=-1} \left(1+\frac{1}{p^{2s}}+\frac{1}{p^{4s}}+\cdots\right). \end{aligned}$$

Επομένως

$$\rho(n) \geq 0 \;\; \forall\, n \in \mathbb{N} \quad \text{και μάλιστα} \quad \rho(n^2) \geq 1. \tag{1.8}$$

Τώρα, λόγω της υπόθεσης ότι $L(1/\chi) = 0$ (και επειδή η $\zeta(s)$ έχει πόλο πρώτης τάξης, μόνο για $s = 1$ $(\sigma > 0)$), έπεται ότι η $\psi(s)$ **δεν** έχει **ανώμαλο** σημείο για $\sigma > 0$ και η (1.5) και

το Θεώρημα Landau μας εξασφαλίζουν τη **σύγκλιση** της σειράς $\sum \rho(n)n^{-s}$ για $\sigma > 0$. Από την άλλη μεριά όμως, η σειρά

$$\sum_{n=1}^{\infty} \frac{\rho(n)}{n^{1/2}} \ \geq \ \sum_{n=1}^{\infty} \frac{\rho(n^2)}{n} \ \geq \ \sum_{n=1}^{\infty} \frac{1}{n} \ = \ \infty$$

αποκλίνει και συνεπώς, καταλήξαμε σε άτοπο. Συνεπώς

$$L(1/\chi) \neq 0 \ \text{ για κάθε χαρακτήρα } \ \chi \neq \chi_0. \quad \square$$

Πόρισμα 1.4.2 (θεώρημα του Dirichlet για αριθμητικές προόδους) *Αν N φυσικός αριθμός και a ακέραιος πρώτος προς τον N, τότε η αριθμητική πρόοδος $\{Nk+a\}_{k\in\mathbb{N}}$ περιέχει άπειρο πλήθος πρώτων και μάλιστα*

$$\sum_{\substack{p\in\mathbb{P} \\ p\equiv a \,(mod\, N)}} \frac{1}{p} \ = \ \infty$$

Απόδειξη: Για $\sigma > 1$

$$\begin{aligned}
\sum_{p^r\equiv a \,(\mathrm{mod}\, N)} \sum_{r\geq 1} \frac{1}{rp^{rs}} &= \sum_{p^r\equiv a \,(\mathrm{mod}\, N)} \sum_{r\geq 1} \frac{1}{\varphi(N)} \sum_{\chi} \overline{\chi}(a)\, \chi(p^r) \frac{1}{rp^{rs}} \\
&= \frac{1}{\varphi(N)} \sum_{\chi} \overline{\chi}(a) \sum_{p^r\equiv a \,(\mathrm{mod}\, N)} \sum_{r=1} \frac{\chi(p)^r}{rp^{rs}} \\
&= \frac{1}{\varphi(N)} \sum_{\chi} \overline{\chi}(a)\ \log\, L(s/\chi) \\
&= \frac{1}{\varphi(N)} \left[\log\, L(s/\chi_0) + \sum_{\chi\neq\chi_0} \overline{\chi}(a) \log\, L(s/\chi) \right] \qquad (1.9)
\end{aligned}$$

(Η εναλλαγή των $\sum_p$ και $\sum_\chi$ επιτρέπεται διότι οι σειρές συγκλίνουν απόλυτα. Τα αθροίσματα διατρέχουν, ως συνήθως, όλους τους πρώτους αριθμούς και όλους τους χαρακτήρες mod$N$ αντίστοιχα).

Η $\log L(s/\chi_0)$ για $s \to 1$ τείνει στο ∞ ενώ για $\chi \neq \chi_0$ η $\log L(s/\chi)$ είναι φραγμένη λόγω

του θεωρήματος 1.4.1, άρα το δεξί μέλος της (1.9) για $s = 1$ αποκλίνει. Αλλά

$$\begin{aligned}\sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{r>1} \frac{1}{rp^r} &\leq \sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{r=2}^{\infty} \frac{1}{rp^r} \\ &\leq \sum_{\substack{p \\ p^r \equiv a \pmod N}} \sum_{r=2}^{\infty} \frac{1}{2p^r} = \sum_{p} \frac{1}{2p(p-1)} \\ &\leq \sum_{n=2}^{\infty} \frac{1}{2n(n-1)} = \frac{1}{2},\end{aligned}$$

δηλαδή η σειρά συγκλίνει για $r > 1$, συνεπώς αποκλίνει για $r = 1$, οπότε

$$\sum_{\substack{p \\ p \equiv a \pmod N}} \frac{1}{p} = \infty. \quad \square$$

1.5 Μερόμορφη επέκταση και συναρτησιακή εξίσωση της $\zeta(s)$

Το πρότυπο για πολλές από τις συναρτήσεις στις οποίες θα αναφερθούμε παρακάτω αποτελεί η ζήτα συνάρτηση του Riemann. Θα μελετήσουμε λοιπόν την επέκταση της σ'ολο το μιγαδικό επίπεδο και θα αποδείξουμε τη συναρτησιακή της εξίσωση.

Κατ΄ αρχήν χρειαζόμαστε μερικές ιδιότητες της Γ-συνάρτησης.

Η Γ-συνάρτηση ορίζεται ως εξής:

$$\Gamma(s) := \int_0^{\infty} e^{-t} t^s \frac{dt}{t}, \quad \text{για} \quad \mathrm{Re}(s) > 0.$$

Ιδιότητες:

1. $\Gamma(1) = 1$
2. $\Gamma(s+1) = s\Gamma(s), \quad Re(s) > 0$

Απόδειξη:

1. Θα αποδείξουμε ότι $\Gamma(1) = 1$. Έχουμε λοιπόν ότι

$$\begin{aligned}\Gamma(1) &= \lim_{z \to +\infty} \int_0^z e^{-t} dt = \lim_{z \to +\infty} \left[-e^{-t} \Big|_0^z \right] \\ &= e^{-0} - \lim_{z \to +\infty} \frac{1}{e^z} = 1.\end{aligned}$$

2. Για τη δεύτερη ιδιότητα έχουμε

$$\begin{aligned}\Gamma(s+1) &= \int_0^\infty t^s e^{-t}dt \\ &= \lim_{z\to 0}\int_z^1 t^s e^{-t}dt + \lim_{z\to\infty}\int_1^z t^s e^{-t}dt.\end{aligned}$$

Ολοκλήρωση κατά μέρη δίνει:

$$\begin{aligned}\int_z^1 t^s e^{-t}dt &= -t^s e^{-t}\Big|_z^1 + s\int_z^1 t^{s-1}e^{-t}dt \\ &= \frac{z^s}{e^z} - \frac{1}{e} + s\int_z^1 t^{s-1}e^{-t}dt,\end{aligned}$$

οπότε

$$\lim_{z\to 0}\int_z^1 t^s e^{-t}dt = -\frac{1}{e} + s\int_0^1 t^{s-1}e^{-t}dt.$$

Επίσης

$$\begin{aligned}\int_1^z t^s e^{-t}dt &= \frac{1}{e} - \frac{z^s}{e^z} + s\int_1^z t^{s-1}e^{-t}dt \\ \Longrightarrow \quad \lim_{z\to\infty}\int_1^z t^s e^{-t}dt &= \frac{1}{e} + s\lim_{z\to\infty}\int_1^z t^{s-1}e^{-t}dt.\end{aligned}$$

Τελικά

$$\Gamma(s+1) = s\int_0^\infty t^{s-1}e^{-t}dt = s\Gamma(s). \quad \square$$

Χωρίς απόδειξη αναφέρουμε τέλος τις ιδιότητες:

3. $\Gamma(s) = \lim_{n\to\infty}\dfrac{n^s n!}{s(s+1)\cdots(s+n)}$. Εδώ για όλα τα $s\in\mathbb{C}\setminus\{-n \mid n\in\mathbb{N}_0\}$, δηλαδή η $\Gamma(s)$ επεκείνεται μερόμορφα σ΄ όλο το μιγαδικό επίπεδο με **μοναδικούς απλούς πόλους** τα σημεία $s=-n$, $n\in\mathbb{N}_0$ και υπόλοιπο ίσο με $\dfrac{(-1)^n}{n!}$.

4. $\Gamma(s)\Gamma(1-s) = \dfrac{\pi}{\sin(\pi s)} \quad \forall s\in\mathbb{C}\setminus\mathbb{Z}$

5. $\Gamma(\dfrac{s}{2})\Gamma(\dfrac{s+1}{2}) = \sqrt{\pi}2^{1-s}\Gamma(s) \quad \forall s\in\mathbb{C}\setminus\{-n \mid n\in\mathbb{N}_0\}$

Για τις αποδείξεις αυτών των ιδιοτήτων παραπέμπουμε στα βιβλία [6], [31], [41].

Γιατί τώρα η συνάρτηση $\Gamma(s)$ είναι σπουδαία για τη θεωρία των σειρών Dirichlet;

Έχουμε για $u=tn$

$$\int_0^\infty t^{s-1}e^{-nt}dt = n^{-s}\int_0^\infty u^{s-1}e^{-u}du = \Gamma(s)n^{-s},$$

δηλαδή στην περιοχή απόλυτης σύγκλισης,

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \;=\; \frac{1}{\Gamma(s)} \int_0^{\infty} \left(\sum_{n=1}^{\infty} a_n e^{-nt} \right) t^{s-1} dt$$

Αυτό σημαίνει ότι η συνηθισμένη σειρά Dirichlet

$$f(s) \;=\; \sum_{n=1}^{\infty} a_n n^{-s}$$

και η δυναμοσειρά με τους ίδιους συντελεστές

$$F(s) \;=\; \sum_{n=1}^{\infty} a_n z^n$$

σχετίζονται μεταξύ τους ως εξής:

$$f(s) \;=\; \frac{1}{\Gamma(s)} \int_0^{\infty} F(e^{-t}) t^{s-1} dt \tag{1.10}$$

δηλαδή μέσω του λεγόμενου **μετασχηματισμού Mellin**. Εδώ θα πρέπει να σημειώσουμε ότι η $\dfrac{1}{\Gamma(s)}$ είναι ολόμορφη για κάθε $s \in \mathbb{C}$ και αυτό είναι συνέπεια του τύπου του Weierstrass (δες [1], σελίδα 199).

$$\frac{1}{\Gamma(s)} \;=\; s e^{\gamma s} \prod_{n=1}^{\infty} \left[\left(1 + \frac{s}{n} \right) e^{-\frac{s}{n}} \right]$$

όπου το απειρογινόμενο συγκλίνει παντού (το γ είναι η γνωστή **σταθερά του Euler**).

Χρειαζόμαστε και κάτι από τη θεωρία των μετασχηματισμών Fourier.

Έστω $\mathfrak{F}$ ο διανυσματικός χώρος των συναρτήσεων $f : \mathbb{R} \to \mathbb{C}$ οι οποίες έχουν παράγωγο κάθε τάξης (άπειρα διαφορίσιμες) και οι οποίες φθίνουν στο άπειρο πιο γρήγορα από ότι κάθε αρνητική δύναμη, δηλαδή $|x|^N f(x) \to 0$ όταν $x \to \pm\infty$ για **όλα** τα N.

Παραδείγματα:

(i) $f(x) = e^{-\pi x^2}$

(ii) $f(x) = e^{-x^2}$

Για κάθε τέτοια συνάρτηση $f \in \mathfrak{F}$ ορίζουμε τον **μετασχηματισμό Fourier** $\hat{f}$ ως εξής:

$$\hat{f}(y) \;:=\; \int_{-\infty}^{+\infty} e^{-2\pi i x y} f(x) dx$$

Είναι εύκολο να αποδειχθεί ότι το ολοκλήρωμα συγκλίνει για όλα τα y και μάλιστα ότι $\hat{f} \in \mathfrak{F}$ (π.χ. [26], σελίδες 24-25). Επίσης ισχύουν οι ακόλουθες ιδιότητες:

(i) Αν $a \in \mathbb{R}$ και $g(x) = f(x+a)$ τότε $\hat{g}(y) = e^{2\pi i a y}\hat{f}(y)$

(ii) Αν $a \in \mathbb{R}$ και $g(x) = e^{2\pi i a x} f(x)$ τότε $\hat{g}(y) = \hat{f}(y-a)$

(iii) Αν $b > 0$ και $g(x) = f(bx)$ τότε $\hat{g}(y) = \frac{1}{b}\hat{f}(\frac{y}{b})$

Απόδειξη: Οι (i) και (ii) είναι προφανείς.

Για την ιδιότητα (iii) έχουμε

$$\hat{g}(y) \;=\; \int_{-\infty}^{+\infty} e^{-2\pi i x y} f(bx)dx \;=\; \int_{-\infty}^{+\infty} e^{-2\pi i \frac{x}{b} y} f(x)\frac{dx}{b} \;=\; \frac{1}{b}\hat{f}\left(\frac{y}{b}\right). \quad \square$$

Πρόταση 1.5.1 *Αν* $f(x) = e^{-\pi x^2}$ *τότε* $\hat{f} = f$.

Απόδειξη: $\hat{f}(y) = \displaystyle\int_{-\infty}^{+\infty} e^{-2\pi i y x} f(x)dx$. Παραγωγίζουμε ως προς y.

$$\begin{aligned}\hat{f}'(y) &= \frac{d}{dy}\left[\int_{-\infty}^{+\infty} e^{-2\pi i x y} f(x)dx\right] = \int_{-\infty}^{+\infty} (-2\pi i x) e^{-2\pi i x y} f(x)dx \\ &= -2\pi i \int_{-\infty}^{+\infty} e^{-2\pi i x y} x e^{-\pi x^2} dx\end{aligned}$$

Ολοκληρώνουμε κατά μέρη και έχουμε:

$$\begin{aligned}\hat{f}'(y) &= -2\pi i e^{-2\pi i x y}\cdot\frac{1}{-2\pi}e^{-\pi x^2}\Big|_{-\infty}^{+\infty} + 2\pi i\int_{-\infty}^{+\infty}(-2\pi i y)e^{-2\pi i y x}\frac{e^{-\pi x^2}}{-2\pi}dx \\ &= -2\pi y\int_{-\infty}^{+\infty} e^{-2\pi i y x} f(x)dx \;=\; -2\pi y\hat{f}(y)\end{aligned}$$

Επομένως η $\hat{f}$ επαληθεύει τη διαφορική εξίσωση

$$\frac{\hat{f}'(y)}{\hat{f}(y)} = -2\pi y$$

η οποία έχει λύση $\hat{f}(y) = Ce^{-\pi y^2}$. Η σταθερά C υπολογίζεται αν θέσουμε $y = 0$, δηλαδή

$$C = \hat{f}(0) = \int_{-\infty}^{+\infty} e^{-\pi x^2} dx = 1. \quad \square$$

Σημείωση: Υπολογισμός τελευταίου ολοκληρωματος.

$$C^2 \;=\; \int_{-\infty}^{+\infty} e^{-\pi x^2}dx \int_{-\infty}^{+\infty} e^{-\pi y^2}dy \;=\; \int_{\mathbb{R}} e^{-\pi(x^2+y^2)}dxdy.$$

Κάνουμε αλλαγή μεταβλητής $\left\{ \begin{array}{l} x = r\cos\theta \\ y = r\sin\theta \end{array} \right\}$, και έχουμε

$$C^2 \;=\; \int_0^{+\infty} e^{-\pi r^2} 2\pi r dr \;=\; \int_0^{+\infty} e^{-u} du = 1.$$

Πρόταση 1.5.2 (Poisson Summation Formula) *Αν* $g \in \mathfrak{F}$ *τότε:*

$$\sum_{m=-\infty}^{+\infty} g(m) \;=\; \sum_{m=-\infty}^{+\infty} \hat{g}(m)$$

Απόδειξη: Ορίζουμε

$$h(x) \;:=\; \sum_{k=-\infty}^{\infty} g(x+k)$$

Η συνάρτηση $h(x)$ είναι **περιοδική** με περίοδο 1 και έχει ανάπτυγμα Fourier

$$h(x) \;=\; \sum_{m=-\infty}^{+\infty} c_m e^{2\pi i m x}$$

όπου

$$\begin{aligned} c_m \;&=\; \int_0^1 h(x) e^{-2\pi i m x} dx \;=\; \int_0^1 \sum_{k=-\infty}^{+\infty} g(x+k) e^{-2\pi i m x} dx \\ &=\; \int_{-\infty}^{+\infty} g(x) e^{-2\pi i m x} dx \;=\; \hat{g}(m) \end{aligned}$$

όπου, για την τελευταία ισότητα, αλλάξαμε άθροιση με ολοκλήρωση καθώς και τη μεταβλητή $x+k$ με το x. Το αριστερό μέρος της προς απόδειξη σχέσης είναι $h(0)$ εξ ορισμού της $h(x)$ και το δεξιό είναι επίσης $h(0)$ το οποίο το βλέπουμε αν στην ισότητα

$$h(x) \;=\; \sum_{m=-\infty}^{\infty} c_m e^{2\pi i x}$$

θέσουμε $x = 0$ τότε θα έχουμε ότι

$$h(0) \;=\; \sum_{m=-\infty}^{+\infty} c_m \;=\; \sum_{m=-\infty}^{+\infty} \hat{g}(m). \quad \square$$

Ορίζουμε τώρα την **θήτα συνάρτηση**

$$\Theta(t) := \sum_{n=-\infty}^{+\infty} e^{-\pi t n^2} \qquad (t > 0)$$

και θα αποδείξουμε την παρακάτω πρόταση:

Πρόταση 1.5.3 *Η θήτα συνάρτηση $\Theta(t)$ επαληθεύει την παρακάτω συναρτησιακή εξίσωση*

$$\Theta(t) = \frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right)$$

Απόδειξη: Παίρνουμε $g(x) := e^{-\pi t x^2}$ για σταθερό $t > 0$ και εφαρμόζουμε τον τύπο άθροισης του Poisson (πρόταση 1.5.2)

$$\sum_{m=-\infty}^{+\infty} g(m) = \sum_{m=-\infty}^{+\infty} \hat{g}(m)$$

γράφουμε $g(x) = f(\sqrt{t}\,x)$ όπου $f(x) = e^{-\pi x^2}$. Από (1.5.1) έχουμε $\hat{f} = f$ και από ιδιότητα (iii) των σειρών Fourier παίρνουμε για $b = \sqrt{t} > 0$ ότι

$$\hat{g}(y) \;=\; t^{-\frac{1}{2}}\hat{f}\left(\frac{y}{\sqrt{t}}\right) \;=\; t^{-\frac{1}{2}}e^{-\frac{\pi y^2}{t}}.$$

Το αριστερό μέλος του τύπου άθροισης του Poisson είναι ίσο με $\Theta(t)$ και το δεξί ίσο με $t^{-\frac{1}{2}}\Theta\left(\frac{1}{t}\right)$. □

Σημείωση: Μερικές φορές θεωρούμε την $\Theta(t)$ σαν συνάρτηση μιγαδικού t όπου υποθέσαμε ότι $Re(t) > 0$. Η πρόταση 1.5.3 συνεχίζει να ισχύει για μιγαδικό t λόγω του αξιώματος της αναλυτικής συνέχισης. Έχουμε δηλαδή ότι και τα δύο μέλη της συναρτησιακής εξίσωσης της θήτα συνάρτησης (δες πρόταση 1.5.3) είναι αναλυτικές συναρτήσεις του t στο δεξιό ημιεπίπεδο. Αφού συμπίπτουν στη θετική πραγματική ημιευθεία θα συμπίπτουν παντού για $Re(t) > 0$.

Πρόταση 1.5.4 *Για $t \to 0^+$ έχουμε:*

$$\left|\Theta(t) - t^{-\frac{1}{2}}\right| \;<\; e^{-c/t}$$

όπου c θετική σταθερά.

Απόδειξη:

$$\begin{aligned}\Theta(t) - t^{-\frac{1}{2}} &= \frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right) - t^{-\frac{1}{2}} \;=\; t^{-\frac{1}{2}}\left[\Theta\left(\frac{1}{t}\right) - 1\right] \\ &= t^{-\frac{1}{2}}\left(\sum_{n=-\infty}^{+\infty} e^{\frac{-\pi n^2}{t}} - 1\right) \;=\; 2t^{-\frac{1}{2}}\sum_{n=1}^{+\infty} e^{\frac{-\pi n^2}{t}}.\end{aligned}$$

Υποθέτουμε ότι το t είναι αρκετά μικρό τέτοιο ώστε

$$\sqrt{t} \;>\; 4e^{-\frac{1}{t}} \quad \text{και} \quad e^{-\frac{3\pi}{t}} \;<\; \frac{1}{2}.$$

Τότε

$$\begin{aligned}\left|\,\Theta(t)-t^{-\frac{1}{2}}\,\right| &< \frac{1}{2}e^{\frac{1}{t}}\left(e^{-\frac{\pi}{t}}+e^{-\frac{4\pi}{t}}+\cdots\right)\\ &< \frac{1}{2}e^{-\frac{\pi-1}{t}}\left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots\right)\\ &= e^{-\frac{\pi-1}{t}} = e^{-c/t} \quad \text{για} \quad c:=\pi-1. \quad \square\end{aligned}$$

Στη συνέχεια θα συσχετίσουμε την θήτα συνάρτηση με την ζήτα συνάρτηση του Riemann. Χοντρικά θα μπορούσε να πει κάποιος ότι η $\zeta(s)$ είναι ο μετασχηματισμός Mellin της $\Theta(t)$. Θα δείξουμε το κύριο θεώρημα της παραγράφου:

Θεώρημα 1.5.5 *Η* **ζήτα συνάρτηση του Riemann** *η οποία ορίζεται, κατ' αρχήν, για* $Re(s)>1$ **επεκτείνεται αναλυτικά σ' όλο το μιγαδικό** s**-επίπεδο, εκτός από μοναδικό απλό πόλο στη θέση** $s=1$ **με υπόλοιπο ίσο πρός** 1. *Αν* $\Lambda(s):=\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ *τότε η* $\Lambda(s)$ *παραμένει αναλλοίωτη αν*

$$s\mapsto 1-s \qquad\qquad \Lambda(s)=\Lambda(1-s)$$

δηλαδή η $\zeta(s)$ *επαληθεύει τη* **συναρτησιακή εξίσωση**

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) \;=\; \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Απόδειξη: Η βασική ιδέα είναι να θεωρήσουμε τον μετασχηματισμό Mellin $\displaystyle\int_0^\infty \Theta(t)t^s\frac{dt}{t}$. Όμως χρειάζεται προσοχή. Για μεγάλο t η θήτα συνάρτηση τείνει ασυμπτωτικά στο 1 (διότι $\Theta(t)=\displaystyle\sum_{n=-\infty}^{\infty}e^{-\pi tn^2}$ όλοι οι όροι για $n\neq 0$ φθίνουν γρήγορα στο μηδέν και απομένει για $n=0$ η τιμή 1) ενώ για t μικρό, κοντά στο μηδέν, η πρόταση 1.5.3 μας λέει ότι η $\Theta(t)$ είναι ασυμπτωτικά ίση με $t^{-1/2}$. Αν λοιπόν θέλουμε σύγκλιση και στα δύο άκρα θα έπρεπε να προσθέσουμε διορθωτικούς όρους. Επιπλέον θα πρέπει το s να το αντικαταστήσουμε με το $\frac{s}{2}$, αλλιώς θα "προσγειωθούμε" στο $\zeta(2s)$. Ορίζουμε λοιπόν

$$\phi(s) \;:=\; \int_1^\infty t^{\frac{s}{2}}\big(\Theta(t)-1\big)\frac{dt}{t} \;+\; \int_0^1 t^{\frac{s}{2}}\left(\Theta(t)-\frac{1}{\sqrt{t}}\right)\frac{dt}{t}$$

Στο πρώτο ολοκλήρωμα η έκφραση

$$\Theta(t)-1 \;=\; 2\sum_{n=1}^{\infty}e^{-\pi n^2 t}$$

τείνει στο μηδέν πολύ γρήγορα για $t \to \infty$. Επομένως το ολοκλήρωμα **συγκλίνει** και μπορεί να υπολογιστεί όρο προς όρο για **κάθε** s. Η πρόταση 1.5.3 μας δίνει ότι το δεύτερο ολοκλήρωμα συγκλίνει για **κάθε** s. Αφού η $\Theta(t)$ είναι φραγμένη από μία σταθερά επί $t^{-\frac{1}{2}}$ στο διάστημα $(0,1]$, αν πάρουμε s τέτοιο ώστε $Re(s) > 1$, το δεύτερο ολοκλήρωμα είναι

$$\int_0^1 t^{\frac{s}{2}}\Theta(t)\frac{dt}{t} - \int_0^1 t^{\frac{s-1}{2}}\frac{dt}{t} \;=\; \int_0^1 t^{\frac{s}{2}}\Theta(t)\frac{dt}{t} - \frac{2}{s-1}.$$

Επομένως για $s \in \mathbb{C}$ με $Re(s) > 1$ έχουμε

$$\begin{aligned}\phi(s) &= 2\sum_{n=1}^{\infty}\int_1^{\infty} e^{-\pi n^2 t}\, t^{\frac{s}{2}}\frac{dt}{t} + \left(\int_0^1 t^{\frac{s}{2}}\frac{dt}{t} + 2\sum_{n=1}^{\infty}\int_0^1 e^{-\pi n^2 t}\, t^{\frac{s}{2}}\frac{dt}{t} \;-\; \frac{2}{s-1}\right)\\ &= 2\int_0^{\infty} e^{-\pi n^2 t}\, t^{\frac{s}{2}}\frac{dt}{t} \;+\; \frac{2}{s} \;-\; \frac{2}{s-1}.\end{aligned}$$

Τώρα κάνουμε χρήση του μετασχηματισμού Mellin (1.10)

$$\int_0^{\infty} t^{s-1}e^{-nt}dt \;=\; n^{-s}\Gamma(s)$$

καλύτερα, για κάθε σταθερά $c > 0$, ισχύει:

$$\int_0^{\infty} t^{s}e^{-ct}\frac{dt}{t} \;=\; c^{-s}\Gamma(s).$$

Ας θέσουμε $c = \pi n^2$ και το $s \mapsto \dfrac{s}{2}$

$$\begin{aligned}\frac{1}{2}\phi(s) &= \sum_{n=1}^{\infty}\left(\pi n^2\right)^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) + \frac{1}{s} + \frac{1}{1-s}\\ &= \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) + \frac{1}{s} + \frac{1}{1-s}\end{aligned}$$

όπου, πάντοτε στα παραπάνω, $Re(s) > 1$.

Τώρα η $\phi(s)$ είναι μία **ακέραια** συνάρτηση του s, αφού τα ολοκληρώματα που όρισαν την $\phi(s)$ συγκλίνουν για κάθε s, όπως είδαμε πιο μπροστά. Επομένως, υπάρχει **μερόμορφη** συνάρτηση του s σε όλο το μιγαδικό επίπεδο, η

$$\frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\left(\frac{1}{2}\phi(s) - \frac{1}{s} + \frac{1}{s-1}\right)$$

η οποία είναι η $\zeta(s)$ για $Re(s) > 1$. Επειδή $\pi^{s/2}$, $\dfrac{1}{\Gamma(s/2)}$, $\phi(s)$ είναι όλες ακέραιες, έπεται ότι οι μόνοι πιθανοί πόλοι είναι για $s = 0$ και $s = 1$. Αλλά κοντά στο $s = 0$ μπορούμε να αντικαταστήσουμε το $s\Gamma\left(\frac{s}{2}\right)$ του παρονομαστή με

$$2\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}\right) \;=\; 2\Gamma\left(\frac{s}{2}+1\right) \;\neq\; 0 \qquad \text{καθώς } s \to 0.$$

Άρα έχουμε μοναδικό πόλο για $s = 1$ του οποίου το υπόλοιπο είναι

$$\lim_{s\to 1}(s-1)\frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\left(\frac{1}{2}\phi(s)-\frac{1}{s}+\frac{1}{s-1}\right) \;=\; \frac{\pi^{\frac{1}{2}}}{\Gamma\left(\frac{1}{2}\right)} \;=\; 1.$$

Απομένει η απόδειξη της συναρτησιακής εξίσωσης. Έχουμε

$$\Lambda(s) \;=\; \frac{1}{2}\phi(s)-\frac{1}{s}-\frac{1}{s-1}.$$

Επειδή η $s \mapsto 1-s$ αφήνει αναλλοίωτο το $\frac{1}{s}+\frac{1}{s-1}$ αρκεί $\phi(s)=\phi(s-1)$.

Τώρα χρειαζόμαστε την συναρτησιακή εξίσωση της ϑήτα συνάρτησης (πρόταση 1.5.3)

$$\Theta(t) \;=\; \frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right).$$

Αν στον ορισμό της $\phi(s)$ αντικαταστήσουμε το t με $\frac{1}{t}$ παίρνουμε:

$$\phi(s) \;=\; \int_0^1 t^{-\frac{s}{2}}\left[\,\Theta\left(\frac{1}{t}\right)-1\,\right]\frac{dt}{t}+\int_1^\infty t^{-\frac{s}{2}}\left[\,\Theta\left(\frac{1}{t}\right)-\sqrt{t}\,\right]\frac{dt}{t}$$

οπότε η πρόταση 1.5.2 δίνει

$$\begin{aligned}(1.5) \quad &= \int_0^1 t^{-\frac{s}{2}}\left(\,\sqrt{t}\,\Theta(t)-1\,\right)\frac{dt}{t}+\int_1^\infty t^{-\frac{s}{2}}\left(\,\sqrt{t}\Theta(t)-\sqrt{t}\,\right)\frac{dt}{t}\\ &= \int_0^1 t^{\frac{1-s}{2}}\left(\,\Theta(t)-\frac{1}{\sqrt{t}}\,\right)\frac{dt}{t}+\int_1^\infty t^{\frac{1-s}{2}}\left(\,\Theta(t)-1\,\right)\frac{dt}{t}\\ &= \phi(1-s). \quad \square\end{aligned}$$

Κεφάλαιο 2

Η ζήτα συνάρτηση αλγεβρικών σωμάτων αριθμών

Τις ιδέες των προηγουμένων παραγράφων θα προσπαθήσουμε τώρα να γενικεύσουμε σε αλγεβρικά σώματα αριθμών. Για την κατανόηση της ύλης από εδώ και πέρα είναι απαραίτητη η γνώση του περιεχομένου ενός μαθήματος αλγεβρικής θεωρίας αριθμών, όπως αυτές περιγράφονται παραδείγματος χάριν στο [2].

2.1 Η κατανομή των ακεραίων ιδεωδών ενός αλγεβρικού σώματος αριθμών K σε κλάσεις ιδεωδών.

Υποθέτουμε ότι K είναι ένα οποιοδήποτε αλγεβρικό σώμα αριθμών. Αν n είναι ο βαθμός της επέκτασης $K/\mathbb{Q}$, s το πλήθος των πραγματικών εμφυτεύσεων και t το πλήθος των μη συζυγών μιγαδικών εμφυτεύσεων του K στο $\mathbb{C}$, τότε $n = s + 2t$.
Έστω

$$\{\sigma_1, \sigma_2, \dots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}}\}$$

το σύνολο των εμφυτεύσεων του K στο $\mathbb{C}$. Ξαναθυμόμαστε την λογαριθμική εμφύτευση του K^* στο $\mathbb{R}^{s+t}$

$$\begin{aligned} L(x) &:= L(\sigma(x)) \\ &= \left(\log|\sigma_1(x)|, \log|\sigma_2(x)|, \dots, \log|\sigma_s(x)|, 2\log|\sigma_{s+1}(x)|, \dots, 2\log|\sigma_{s+t}(x)|\right) \end{aligned}$$

Αν R είναι ο δακτύλιος των ακεραίων αλγεβρικών του K και $E(R)$ η ομάδα των μονάδων αυτού με $L(E(R))$ θα συμβολίζουμε την εικόνα της ομάδας $E(R)$ μέσω της απεικόνισης L. Ο πυρήνας $\operatorname{Ker} L(E(R)) =: W$ είναι η ομάδα των ριζών της μονάδας που ανήκουν στο K. Η W είναι πεπερασμένη ομάδα και μάλιστα κυκλική άρτιας τάξης. Ακόμη $L(E(R))$ είναι **δικτυωτό** του $\mathbb{R}^{s+t}$ και μάλιστα περιέχεται στο υπερεπίπεδο

$$H = \Big\{(y_1, y_2, \dots, y_{s+t}) \;\Big|\; \sum_{i=1}^{s+t} y_i = 0\Big\}$$

Αν ορίσουμε τώρα $e_i = \begin{cases} 1, & \text{για} \quad i = 1, 2, \dots, s \\ 2, & \text{για} \quad i = s+1, \dots, s+t \end{cases}$ και θυμηθούμε την κανονική εμφύτευση

$$\sigma \;:\; K \to \mathbb{R}^s \times \mathbb{C}^t$$

$$\sigma(x) = \big(\sigma_1(x), \sigma_2(x), \dots, \sigma_s(x), \sigma_{s+1}(x), \dots, \sigma_{s+t}(x)\big)$$

μπορούμε να γράψουμε τη λογαριθμική εμφύτευση σαν σύνθεση δύο συναρτήσεων

$$K^* \;\xrightarrow{\;\sigma\;}\; \mathbb{R}^{*s} \times \mathbb{C}^{*t} \;\xrightarrow{\;L\;}\; \mathbb{R}^{*s+t}$$

$$\alpha \;\longmapsto\; \big(\sigma_1(\alpha), \dots, \sigma_{s+t}(\alpha)\big) \;\longmapsto\; \big(\log|\sigma_1(\alpha)|^{e_1}, \dots, \log|\sigma_{s+t}(\alpha)|^{e_{s+t}}\big)$$

Αν $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{s+t-1}$ είναι ένα σύστημα θεμελιωδών μονάδων του K (Θεώρημα μονάδων του Dirichlet) τότε ορίζουμε τον **ομαλοποιητή (regulator)** αυτού του συστήματος

$$\operatorname{Reg}_K\big(\langle \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{s+t-1}\rangle\big) \;=\; \Big|\det\big(\log|\sigma_i(\varepsilon_j)|^{e_i}\big)\Big|$$

για $i = 1, 2, \dots, s+t,\ i \neq i_0,\ j = 1, 2, \dots, s+t-1$ και $i_0 \in \{1, 2, \dots, s+t\}$.
Αποδεικνύεται ότι ο ορισμός είναι ανεξάρτητος της εκλογής του συστήματος και ότι εξαρτάται μόνο από το K. Θα γράφουμε λοιπόν για τον ομαλοποιητή οποιουδήποτε συστήματος θεμελιωδών μονάδων Reg_K. Αν τέλος

$$E(R) = W \times \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \cdots \times \langle \varepsilon_r \rangle, \quad r := s + t - 1$$

τότε θα συμβολίζουμε με $E_0(R) := \langle \varepsilon_1 \rangle \times \langle \varepsilon_2 \rangle \times \cdots \times \langle \varepsilon_r \rangle$.

Πρόταση 2.1.1 (γεωμετρική σημασία του ομαλοποιητή)
Ο όγκος του δικτυωτού $L(E(R))$ είναι ίσος πρός

$$\sqrt{s+t}\, Reg_K.$$

Απόδειξη:

$$L(E(R)) \;=\; \mathbb{Z}\log(\varepsilon_1) \oplus \mathbb{Z}\log(\varepsilon_2) \oplus \cdots \oplus \mathbb{Z}\log(\varepsilon_{s+t-1}) \;\subseteq\; H$$

όπου $H = \big\{(x_1, x_2, \dots, x_{s+t}) \in \mathbb{R}^{s+t} \;\big|\; x_1 + x_2 + \cdots + x_{s+t} = 0\big\}$.
Το διάνυσμα $\overrightarrow{\mathfrak{r}} = \dfrac{1}{\sqrt{s+t}}(\underbrace{1, 1, \dots, 1}_{s}, \underbrace{1, 1, \dots, 1}_{t})$ είναι κάθετο στο υπερεπίπεδο H άρα και στο δικτυωτό $L(E(R))$ και είναι και μοναδιαίο, δηλαδή $\|\overrightarrow{\mathfrak{r}}\| = 1$. Επομένως

$$\mathrm{Vol}\big(L(E(R))\big) \;=\; \Big|\det\big(\log(\varepsilon_1), \log(\varepsilon_2), \dots, \log(\varepsilon_{s+t-1}), \overrightarrow{\mathfrak{r}}\big)\Big|$$

$$= \frac{1}{\sqrt{s+t}} \left| \det \begin{bmatrix} \log|\sigma_1(\varepsilon_1)|^{e_1} & \log|\sigma_1(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_1(\varepsilon_r)|^{e_r} & 1 \\ \log|\sigma_2(\varepsilon_1)|^{e_1} & \log|\sigma_2(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_2(\varepsilon_r)|^{e_r} & 1 \\ \dots & \dots & \dots & \dots & \dots \\ \log|\sigma_{s+t}(\varepsilon_1)|^{e_1} & \log|\sigma_{s+t}(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_{s+t}(\varepsilon_r)|^{e_r} & 1 \end{bmatrix} \right|$$

όπου $r := s + t - 1$. Προσθέτουμε όλες τις γραμμές στην i_0 γραμμή και έχουμε

$$= \frac{1}{\sqrt{s+t}} \left| \det \left[\begin{array}{cccc|c} \log|\sigma_1(\varepsilon_1)|^{e_1} & \log|\sigma_1(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_1(\varepsilon_r)|^{e_r} & 1 \\ \log|\sigma_2(\varepsilon_1)|^{e_1} & \log|\sigma_2(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_2(\varepsilon_r)|^{e_r} & 1 \\ \dots & \dots & \dots & \dots & \dots \\ \hline 0 & 0 & \dots & 0 & s+t \\ \hline \dots & \dots & \dots & \dots & \dots \\ \log|\sigma_{s+t}(\varepsilon_1)|^{e_1} & \log|\sigma_{s+t}(\varepsilon_2)|^{e_2} & \dots & \log|\sigma_{s+t}(\varepsilon_r)|^{e_r} & 1 \end{array}\right] \right|$$

Αναπτύσσουμε την ορίζουσα κατά τα στοιχεία της i_0 γραμμής και έχουμε το ζητούμενο. □

Συμβολισμός 2.1.2 *Αν $\mathfrak{K}$ η ομάδα κλάσεων ιδεωδών του σώματος K, $\mathfrak{k} \in \mathfrak{K}$ και $t \in \mathbb{R}_+$*

$$A_{\mathfrak{k}}(t) := \big\{A \in \mathfrak{k} \;\big|\; A \text{ ακέραιο ιδεώδες, } N_{K/\mathbb{Q}}(A) \le t\big\}$$

$$A(t) := \big\{A \;\big|\; A \text{ ακέραιο ιδεώδες του } K, N_{K/\mathbb{Q}}(A) \le t\big\}$$

Σκοπός αυτής της παραγράφου είναι να αποδείξουμε το ακόλουθο:

Θεμελιώδες Θεώρημα 2.1.3 *Ισχύει*

$$A_{\mathfrak{k}}(t) \;=\; \lambda \cdot t + \varepsilon_{\mathfrak{k}}(t)$$

όπου $\varepsilon_{\mathfrak{k}}(t) = O(t^{1-\frac{1}{n}})$ *και* $\lambda := \dfrac{2^{s+t}\pi^s Reg_K}{w\sqrt{|D_K|}}$

Παρατήρηση: Ο w συμβολίζει την τάξη της ομάδας των ριζών της μονάδας W του K και D_K την διακρίνουσα του σώματος K. Επειδή ο λ είναι ανεξάρτητος της κλάσης ιδεωδών $\mathfrak{k}$, προκύπτει αμέσως ότι:

$$A(t) \;=\; \lambda h t + O(t^{1-\frac{1}{n}}).$$

Η απόδειξη είναι αρκετά μακροσκελής.

Κατ' αρχήν διαλέγουμε ένα ιδεώδες B της κλάσης $\mathfrak{k}^{-1}$ το οποίο το κρατούμε σταθερό. Επομένως

$$A \in \mathfrak{K} \iff \exists\, \alpha \in K^* \text{ τ.ω. } A \cdot B = (\alpha).$$

Επίσης είναι προφανείς οι ισοδυναμίες

$$A \text{ ακέραιο ιδεώδες του } K \iff A \subseteq R \;\Leftrightarrow\; (\alpha) = AB \subseteq R \cdot B = B \;\Leftrightarrow\; \alpha \in B$$

καθώς και

$$N_{K/\mathbb{Q}}(A) \leq t \iff N_{K/\mathbb{Q}}(AB) = \big|N_{K/\mathbb{Q}}(\alpha)\big| \leq N_{K/\mathbb{Q}}(B)t.$$

Επομένως

$$\begin{aligned} & \#\big\{A \in \mathfrak{k} \;\big|\; A \text{ ακέραιο ιδεώδες του K και } N_{K/\mathbb{Q}}(A) \leq t\big\} \\ = \;& \#\big\{(\alpha) \;\big|\; \alpha \in B \smallsetminus \{0\} \text{ και } |N_{K/\mathbb{Q}}(\alpha)| \leq N_{K/\mathbb{Q}}(B)t \,\big\}\,. \end{aligned}$$

Το πρόβλημα βρίσκεται στο ότι είναι δυνατόν να ισχύει ότι $(\alpha) = (\alpha')$ για $\alpha \neq \alpha'$. Γνωρίζουμε ότι $(\alpha) = (\alpha') \;\Leftrightarrow\; \alpha' = \varepsilon\alpha$ με $\varepsilon \in E(R)$. Άρα θα πρέπει να βρούμε ένα πλήρες σύστημα αντιπροσώπων α (με τις παραπάνω ιδιότητες) modulo $E(R)$.

Λήμμα 2.1.4 *Αν D ένα πλήρες σύστημα αντιπροσώπων του K^* modulo την ομάδα $E_0(R) \cong E(R)/W$, τότε*

$$A_{\mathfrak{k}}(t) = \frac{1}{w} \cdot \#\big\{\alpha \;\big|\; (\alpha) \in B \cap D \text{ και } |N_{K/\mathbb{Q}}(\alpha)| \leq N_{K/\mathbb{Q}}(B) \cdot t\big\}$$

Απόδειξη: Η απόδειξη είναι άμεση συνέπεια των αμέσως προηγουμένων εισαγωγικών παρατηρήσεων. □

Στη συνέχεια θα αποδείξουμε ένα αποτέλεσμα της θεωρίας ομάδων.

Λήμμα 2.1.5 *Έστω $f : G \to G'$ ομομορφισμός ομάδων και $U \leq G$, $U' \leq G'$ υποομάδες των G και G' αντίστοιχα, τέτοιες ώστε η $f|_U : U \to U'$ να είναι αμφιμονοσήμαντη. Τότε, αν D' είναι πλήρες σύστημα αντιπροσώπων της U' στην G' και το $D := f^{-1}(D')$ θα είναι πλήρες σύστημα αντιπροσώπων της U στην G.*

Απόδειξη: Αρκει να αποδείξουμε ότι

(1) $G = \bigcup_{d\in D} dU$ και ότι

(2) Αν $d_1, d_2 \in D$ και $d_1U = d_2U$ τότε $d_1 = d_2$

Για την απόδειξη της (1), εξ υποθέσεως έχουμε ότι $G' = \dot{\bigcup}_{d'\in D'} d'U'$. Συνεπώς

$$\begin{aligned} G &= f^{-1}(G') = \bigcup_{d\in D} df^{-1}(U') \\ &= \bigcup_{d\in D} d\cdot \operatorname{Ker} f \cdot U = \bigcup_{d\in D} dU. \end{aligned}$$

Η τελευταία ισότητα ισχύει διότι $D = f^{-1}(D') \Rightarrow d\cdot \operatorname{Ker} f \subseteq D$.

Για την απόδειξη της (2) έχουμε

$$\begin{aligned} d_1U = d_2U &\iff d_1^{-1}d_2 \in U \implies f(d_1^{-1}d_2) \in f(U) = U' \\ &\implies f(d_1^{-1})f(d_2) \in U' \implies f(d_1)U' = f(d_2)U'. \end{aligned}$$

Αυτό σημαίνει ότι τα $f(d_1)$ και $f(d_2)$ ορίζουν την ίδια κλάση $\bmod U'$. Επειδή όμως $f(d_1) \in D'$ και $f(d_2) \in D'$ και D' είναι πλήρες σύστημα αντιπροσώπων θα έχουμε $f(d_1) = f(d_2) \Rightarrow f(d_1d_2^{-1}) = 1$ και επειδή η f είναι ένα προς ένα, έπεται ότι $d_1d_2^{-1} = 1$, δηλαδή $d_1 = d_2$. □

Γιατί αποδείχθηκε το λήμμα αυτό θα φανεί σε λίγο.

Λήμμα 2.1.6 *Έστω D ένα πλήρες σύστημα αντιπροσώπων του $\mathbb{R}^{*s} \times \mathbb{C}^{*t}$ ως πρός την $\sigma(E_0)$ (όπου σ είναι η κανονική εμφύτευση του K^* στο $\mathbb{R}^{*s} \times \mathbb{C}^{*t}$). Τότε ισχύει*

$$A_{\mathfrak{k}}(t) = \frac{1}{w}\cdot \#\Big\{ x \in \sigma(B)\cap D \;\Big|\; \big|N(x)\big| \leq N_{K/\mathbb{Q}}(B)t \Big\}$$

όπου η $N(x)$, για $x = (x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$ ορίζεται

$$N(x) := x_1x_2\cdots x_s|x_{s+1}|^2\cdots|x_{s+t}|^2.$$

Απόδειξη: Ο σ είναι μονομορφισμός δακτυλίων (δες [2]), οπότε έχουμε το σχήμα

$$K^* \overset{\sigma}{\hookrightarrow} \sigma(K^*)$$
$$E_0 \hookrightarrow \sigma(E_0)$$

Αν D πλήρες σύστημα αντιπροσώπων της ομάδας ${}^{K^*}\!/_{E_0(R)}$ τότε το $\sigma(D)$ είναι επίσης πλήρες σύστημα αντιπροσώπων της ομάδας ${}^{\sigma(K^*)}\!/_{\sigma(E_0(R))}$. Τέλος αρκεί να παρατηρήσουμε ότι

$$\big|N_{K/\mathbb{Q}}(\alpha)\big| \leq N_{K/\mathbb{Q}}(B)t \quad \Longleftrightarrow \quad \big|N(x)\big| \leq N_{K/\mathbb{Q}}(B)t,$$

το οποίο είναι προφανές. □

Λήμμα 2.1.7 *Έστω D' πλήρες σύστημα αντιπροσώπων του $\mathbb{R}^{s+t}$ ως πρός $L(\sigma(E_0(R)))$. Τότε $D := L^{-1}(D')$ είναι πλήρες σύστημα αντιπροσώπων ως προς την $\sigma(E_0(R))$.*

Απόδειξη: Σύμφωνα με το λήμμα (2.1.5), αρκεί να δείξουμε ότι η απεικόνιση

$$L\big|_{\sigma(E_0)} : \sigma(E_0) \Longrightarrow L(\sigma(E_0))$$

είναι αμφιμονοσήμαντη. Εδώ για λόγους ευκολίας συμβολίζουμε το $E_0(R)$ με E_0. Προφανώς είναι επί. Είναι και ένα προς ένα. Πράγματι έχουμε δείξει ότι

$$\mathrm{Ker}\big(L(\sigma(K^*))\big) = \sigma(W) \quad \Longrightarrow \quad \mathrm{Ker}\big(L(\sigma(E_0))\big) = \sigma(W) \cap \sigma(E_0).$$

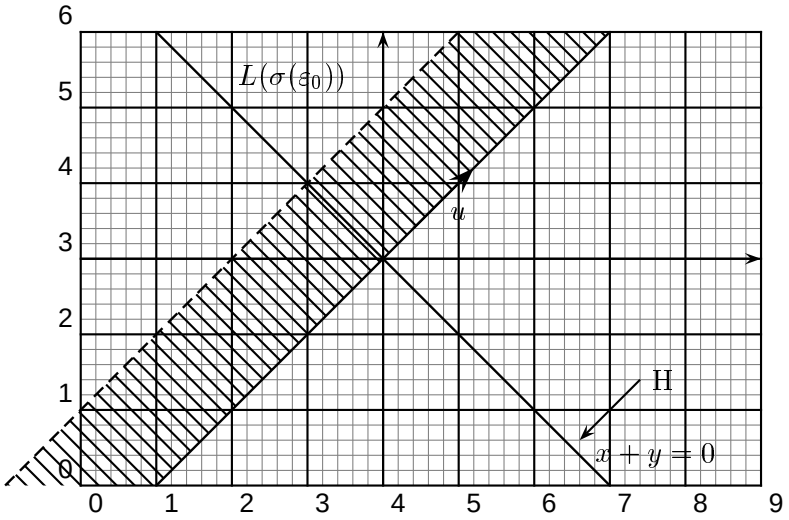
Επειδή σ μονομορφισμός, έπεται ότι

$$\sigma(W) \cap \sigma(E_0) \;=\; \sigma(W \cap E_0) \;=\; \{1\}. \quad \square$$

Σκοπός μας είναι να κατασκευάσουμε ένα πλήρες σύστημα αντιπροσώπων D' της $\mathbb{R}^{s+t}$ ως πρός την υποομάδα $L(\sigma(E_0))$. Το πλεονέκτημα είναι ότι το $L(\sigma(E_0))$ είναι δικτυωτό.

Παράδειγμα: Για $n = 2$, $s = 2$, $t = 0$, K τετραγωνικό πραγματικό σώμα αριθμών έχουμε $\mathbb{R}^{s+t} = \mathbb{R}^s = \mathbb{R}^2$

$$H = \big\{(x_1, x_2) \;\big|\; x_1 + x_2 = 0\big\} \qquad E_0 = \langle \varepsilon_0 \rangle$$



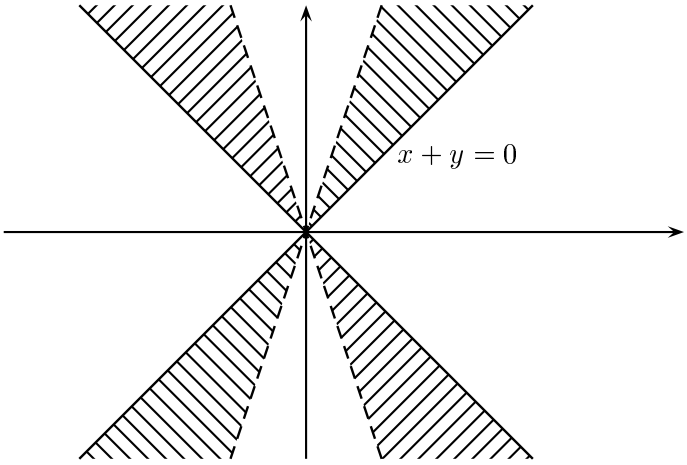
Παίρνουμε $u \perp H$. Προφανώς

$$D' = [0,1) \cdot L(\sigma(\varepsilon_0)) \oplus \mathbb{R}u$$

$$L(u_1, u_2) = (\log|u_1|, \log|u_2|)$$

και $$L^{-1}(x_1, x_2) = (\pm e^{x_1}, \pm e^{x_2})$$

οπότε $L^{-1}(D')$ είναι ο τόπος ανάμεσα στις ευθείες $(\pm e^x, \pm e^x)$ και $(\pm e^x, \pm e^x \varepsilon_0)$ (δες παρακάτω σχήμα).



Ας επιστρέψουμε στη γενική περίπτωση. Εντελώς όμοια προκύπτει ότι

Θεώρημα 2.1.8 *Αν* $u \in \mathbb{R}^{s+t} \setminus H$ *και*

$$F := [0,1) \cdot L(\sigma(\varepsilon_1)) \oplus [0,1) \cdot L(\sigma(\varepsilon_2)) \oplus \cdots \oplus [0,1) \cdot L(\sigma(\varepsilon_r))$$

Τότε $D' = F \oplus \mathbb{R}u$ *είναι ένα πλήρες σύστημα αντιπροσώπων της* $\mathbb{R}^{s+t}$ *modulo* $L(\sigma(E_0))$.

Επομένως, αν D' όπως στο θεώρημα 2.1.8 τότε

$$D \;=\; L^{-1}(D') \;=\; \left\{x \;\in\; \mathbb{R}^{*s}\times\mathbb{C}^{*t} \;\;\middle|\;\; L(x) \;\in\; F\oplus\mathbb{R}u\right\}$$

θα λέγεται μία **θεμελιώδης περιοχή** για το $\sigma(E_0)$.

Συμβολισμός 2.1.9 *Αν $D\subseteq \mathbb{R}^{*s}\times\mathbb{C}^{*t}$ και $a\in\mathbb{R}_+$ τότε συμβολίζουμε με*

$$D_a \;:=\; \left\{x\in D \;\;\middle|\;\; |N(x)|\le a\right\}$$

όπου $N(x)=x_1x_2\ldots x_s|x_{s+1}|^2\ldots|x_{s+t}|^2$.

Παρατήρηση 2.1.10 *Αν $u=(\underbrace{1,1,\ldots,1}_{s},\underbrace{2,2,\ldots,2}_{t})$ τότε η D_a είναι ομογενής και ισχύει:*

$$D_a \;=\; \sqrt[n]{a}D_1$$

Απόδειξη: Αρκεί να δείξουμε ότι η D είναι ομογενής, δηλαδή ότι $\lambda x\in D$ για κάθε $x\in D$ και κάθε $\lambda\in\mathbb{R}$. Πράγματι αν

$$x\in D \;\;\Longrightarrow\;\; L(\lambda x)=L(x)+\log|\lambda|(\underbrace{1,1,\ldots,1}_{s},\underbrace{2,2,\ldots,2}_{t})$$

το οποίο ανήκει στο D' λόγω της εκλογής του u. □

Λήμμα 2.1.11 *Αν D μία θεμελιώδης περιοχή, όπως στο Θεώρημα 2.1.8, με*

$$u \;=\; (\underbrace{1,\ldots,1}_{s},\underbrace{2,\ldots,2}_{t}),$$

τότε ισχύει:

$$A_{\mathfrak{k}}(t)=\frac{1}{w}\cdot\#\left\{\;x\in\sigma(B)\bigcap\sqrt[n]{t\cdot N_{K/\mathbb{Q}}(B)}\cdot D_1\;\right\}.$$

Απόδειξη: Έχουμε ήδη δείξει ότι

$$A_{\mathfrak{k}}(t)=\frac{1}{w}\cdot\#\Big\{x\in\sigma(B)\bigcap D \;\;\Big|\;\; |N(x)|\le t\cdot N_{K/\mathbb{Q}}(B)\Big\}$$

και αφού $D_\alpha=\left\{x\in D\;\middle|\;|N(x)|\le\alpha\right\}$, $D_\alpha=\sqrt[n]{\alpha}\,D_1$, για $\alpha:=tN_{K/\mathbb{Q}}(B)$ έχουμε

$$A_{\mathfrak{k}}(t)=\frac{1}{w}\cdot\#\left\{\;x\in\sigma(B)\bigcap D_\alpha\;\right\}=\frac{1}{w}\cdot\#\left\{\;x\in\sigma(B)\bigcap\sqrt[n]{tN_{K/\mathbb{Q}}(A)}\cdot D_1\;\right\}.\quad\square$$

Λήμμα 2.1.12 *Έστω Γ ένα n-διάστατο δικτυωτό του $\mathbb{R}^n$ και $B \subseteq \mathbb{R}^n$ το οποίο έχει αρκετά καλό σύνορο, είναι δηλαδή το σύνορό του $(n-1)$-Lipschitz παραμετρήσιμο, τότε για κάθε $a \in \mathbb{R}_+$*

$$\#\left(\Gamma \bigcap aB\right) = \frac{Vol(B)}{Vol(\Gamma)} \cdot a^n + O(a^{n-1})$$

Ορισμός 2.1.13 *Ένα $M \subseteq \mathbb{R}^n$ θα λέγεται $(n-1)$-**Lipschitz παραμετρήσιμο**, όταν υπάρχουν **πεπερασμένου** πλήθους συναρτήσεις $f_i : [0,1]^{n-1} \longrightarrow \mathbb{R}^n \quad (i = 1, 2, \ldots, m)$ τ.ω.*

$$M \subseteq \bigcup_i f_i\left([0,1]^{n-1}\right) \quad \text{και} \tag{2.1}$$

$$\sup_{\substack{x,y \in [0,1]^{n-1} \\ x \neq y}} \frac{|f_i(x) - f_i(y)|}{|x-y|} < \infty \quad \text{για κάθε } i = 1, 2, \ldots, m. \tag{2.2}$$

Απόδειξη του Λήμματος 2.1.12: Θα αποδείξουμε ότι μπορούμε να ανάγουμε το πρόβλημα στην ειδική περίπτωση που $\Gamma = \mathbb{Z}^n$. Υπάρχει κάποιος γραμμικός μετασχηματισμός ℓ του $\mathbb{R}^n$ που στέλνει το δικτυωτό Γ στο $\mathbb{Z}^n$. Η συνθήκη του Lipschitz διατηρείται μέσω γραμμικών μετασχηματισμών, δηλαδή το $B' = \ell(B)$ έχει αρκετά καλό σύνορο. Επομένως

$$\#\left(\Gamma \bigcap aB\right) = \#\left(\ell^{-1}(\mathbb{Z}^n) \bigcap aB\right) = \#\left(\mathbb{Z}^n \bigcap a\,\ell(B)\right).$$

Οπότε, αν δεχτούμε προς στιγμήν ότι το λήμμα ισχύει για το $\mathbb{Z}^n$, έχουμε ότι η παραπάνω σχέση είναι ίση με

$$\mathrm{Vol}(\ell(B)) \cdot a^n + O(a^{n-1}).$$

Γνωστό ότι, αν ο ℓ είναι γραμμικός μετασχηματισμός, τότε

$$\mathrm{Vol}(\ell(B)) \;=\; \left|\det(\ell)\right| \cdot \mathrm{Vol}(B).$$

Κάθε γραμμικός μετασχηματισμός διατηρεί την αναλογία όγκων

$$\mathrm{Vol}(\mathbb{Z}^n) = \mathrm{Vol}(\ell(\Gamma)) = \left|det(\ell)\right| \cdot \mathrm{Vol}(\Gamma) \;\Rightarrow\; \mathrm{Vol}(\ell(B)) = \frac{\mathrm{Vol}(B)}{\mathrm{Vol}(\Gamma)},$$

δηλαδή

$$\#\left(\Gamma \bigcap aB\right) \;=\; \frac{\mathrm{Vol}(B)}{\mathrm{Vol}(\Gamma)} \cdot a^n + O(a^{n-1}).$$

Απομένει να δείξουμε τον τύπο για $\Gamma = \mathbb{Z}^n$. Ας πάρουμε το μοναδιαίο $n-$κύβο $[0,1]^n$ και ας τον τοποθετήσουμε έτσι ώστε το κέντρο του να είναι ένα σημείο του δικτυωτού. Ας

θεωρήσουμε μεταφορές αυτού του κύβου. Θα τις ονομάζουμε απλώς n-κύβους. Αφού κάθε κύβος έχει όγκο 1 τότε το πλήθος των κύβων μέσα στο aB είναι περίπου $\#(\mathbb{Z}^n \cap aB)$ και επίσης περίπου όσο ο όγκος $\mathrm{Vol}(aB)$. Έχουμε δηλαδή ότι

$$\#\big(\mathbb{Z}^n \cap aB\big) \;=\; \mathrm{Vol}(aB) + \gamma(a)$$

όπου $\gamma(a) \leq \#\Big\{ n\text{-κύβων } Q \text{ με } Q \cap \partial(aB) \neq \emptyset \Big\}$. Αρκεί επομένως να να δείξουμε ότι $\gamma(a) = O(a^{n-1})$. Το ότι το σύνορο του B είναι Lipschitz-παραμετρήσιμο συνεπάγεται ότι

$$\partial B \subseteq \bigcup_f f\left([0,1]^{n-1}\right)$$

και οι συναρτήσεις f είναι πεπερασμένου πλήθους. Παίρνουμε τον $(n-1)$-κύβο $[0,1]^{n-1}$ και τον διαιρούμε σε ίσους υποκύβους, ακμής $\dfrac{1}{[a]}$. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $a \geq 1$. Έχουμε λοιπόν $[0,1]^{n-1} = \bigcup_{\nu=1}^{[a]} S_\nu$. Αμέσως φαίνεται ότι η διάμετρος κάθε κύβου S_ν είναι $\delta(S_\nu) = \dfrac{\sqrt{n-1}}{[a]}$. Επομένως $\delta\left(f(S_\nu)\right) \leq \lambda\dfrac{\sqrt{n-1}}{[a]}$ και λ μία σταθερά του Lipschitz για όλες τις συναρτήσεις f. Συνεπώς

$$\delta\left(af(S_\nu)\right) \;\leq\; \lambda\frac{a}{[a]}\sqrt{n-1} \;=\; \lambda\alpha\sqrt{n-1} \;<\; 2\lambda\sqrt{n-1}.$$

Τώρα, ας σταθεροποιήσουμε προς το παρόν την f και το ν και ας υπολογίσουμε το

$$\#\Big\{ Q \;\Big|\; Q \bigcap af(S_\nu) \neq \emptyset,\; Q \;=\; n\text{-κύβος} \Big\}.$$

Ας πάρουμε ένα σταθερό σημείο του $af(S_\nu)$ και ας θεωρήσουμε την $n-$διάστατη σφαίρα που έχει κέντρο αυτό το σημείο και ακτίνα $2\lambda\sqrt{n-1}$. Προφανώς η σφαίρα αυτή περιέχει το $af(S_\nu)$ και τέμνει **το πολύ**

$$\mu \;=\; \Big(4\lambda\sqrt{(n-1)}+2\Big)^n$$

από τους n-κύβους. (μ ανεξάρτητο του a). Επομένως

$$\begin{aligned} & \#\Big\{ Q \;\Big|\; n-\text{κύβος},\; Q\bigcap af(S_\nu) \neq \emptyset \text{ για κάποια } f \text{ και } \nu \Big\} \\ \leq\; & \Big(4\lambda\sqrt{(n-1)}+2\Big)^n \cdot \#f \cdot \#\{S_\nu\} \\ \leq\; & (\text{σταθερά}) \cdot a^{n-1}. \end{aligned}$$

Τελικά δηλαδή θα έχουμε

$$\partial(aB) = a\partial B \subseteq a\bigcup_f f\left([0,1]^{n-1}\right) = \bigcup_{f,S_\nu} af\left(S_\nu\right)$$
$$\Longrightarrow \quad \#\Big\{Q \;\Big|\; Q\bigcap \partial(aB) \neq \emptyset\Big\} \;\leq\; (\text{σταθερά})\cdot a^{n-1}$$

Στη συνέχεια αποδεικνύουμε το ακόλουθο

Λήμμα 2.1.14 *Για μία θεμελιώδη περιοχή D του $\sigma(E_0)$ το σύνορό της, έστω D_1 (δές συμβολισμό 2.1.9), είναι $(n-1)$-Lipschitz παραμετρήσιμο.*

Απόδειξη:

$$D_1 = \left\{x \in \mathbb{R}^{*\,s}\times\mathbb{C}^{*\,t} \;\middle|\; L(x)\in F\oplus\mathbb{R}\upsilon \;\text{ και }\; N(x)\leq 1\right\}$$

Σκοπός μας είναι, κατ' αρχήν, να βρούμε μία κατάλληλη παραμετρικοποίηση της D_1. Παίρνουμε πάλι σαν υ το διάνυσμα

$$\upsilon = (\underbrace{1,1,\ldots,1}_{s},\underbrace{2,2,\ldots,2}_{t})$$

$F = [0,1)\upsilon_1\oplus\cdots\oplus[0,1)\upsilon_{s+t-1} = L(\sigma(E_0(R)))$ όπου $\upsilon_i := L(\sigma(\varepsilon_i))$. Υπενθυμίζουμε ότι για $x = (x_1, x_2, \ldots, x_s, x_{s+1}, \ldots, x_{s+t})$

$$N(x) := x_1x_2\cdots x_s|x_{s+1}|^2\cdot|x_{s+2}|^2\cdots|x_{s+t}|^2$$

και

$$L(x) = \left(\log|x_1|,\ldots,\log|x_s|,2\log|x_{s+1}|,\ldots,2\log|x_{s+t}|\right).$$

Ορίζουμε $D_1^+ := \left\{x\in D_1 \;\middle|\; x_1,x_2,\ldots,x_s\geq 0\right\}$. Προφανώς ισχύουν:

1. $\mathrm{Vol}(D_1) = 2^s\cdot\mathrm{Vol}(D_1^+)$,
2. Αν ∂D_1^+ είναι $(n-1)$-Lipschitz παραμετρήσιμο τότε και το ∂D είναι $(n-1)$-Lipschitz παραμετρήσιμο.

Στη συνέχεια θα παραμετρήσουμε το D_1. Το $x\in D_1^+$ ακριβώς τότε όταν $x\in D_1$ και $x_1,x_2,\ldots,x_s\geq 0$. Τώρα, $x\in D_1$ συνεπάγεται ότι

$$L(x)\in F\oplus\mathbb{R}\upsilon, \quad \text{όπου} \quad \upsilon = (\underbrace{1,1,\ldots,1}_{s},\underbrace{2,2,\ldots,2}_{t}),$$

δηλαδή

$$L(x) = (\log|x_1|, \log|x_2|, \dots, \log|x_s|, 2\log|x_{s+1}|, \dots, 2\log|x_{s+t}|) \in \mathbb{F} \oplus \mathbb{R}\upsilon$$

Λόγω του ότι $x_1, x_2, \dots, x_s \geq 0$, έπεται ότι $|x_i| = x_i$ για $i = 1, 2, \dots, s$. Επομένως, υπάρχει $u \in \mathbb{R}$ τέτοιο ώστε $\log x_1 \in F + u$, $\log x_2 \in F + u$, $\dots$, $\log x_s \in F + u$, $2\log|x_{s+1}| \in F + 2u$, $2\log|x_{s+2}| \in F + 2u$, $\dots$, $2\log|x_{s+t}| \in F + 2u$. Συνεπώς,

$$\log x_i = \sum_{k=1}^{r} \lambda_k \upsilon_k^{(i)} + u$$

για $i = 1, 2, \dots, s$, και

$$2\log|x_j| = \sum_{k=1}^{r} \lambda_k \upsilon_k^{(j)} + 2u$$

για $j = s+1, s+2, \dots, s+t$, όπου $r := s + t - 1$.

Παρατηρούμε ότι $N(x) \leq 1 \iff u \leq 0$. Πράγματι,

$$\big|N(x)\big| \leq 1 \quad \Longleftrightarrow \quad \log\big|N(x)\big| \leq 0 \quad \Longleftrightarrow \quad \sum_{k=1}^{r} \lambda_k \sum_{i=1}^{s+t} \upsilon_k^{(i)} + nu \leq 0.$$

Επειδή $\upsilon_k = L(\sigma(\varepsilon_k)) \in L(\sigma(E_0(R))) \subseteq H$, έπεται ότι

$$\sum_{i=1}^{s+t} \upsilon_k^{(i)} = 0.$$

Επομένως $N(x) \leq 1 \iff nu \leq 0 \iff u \leq 0$.

Από τα παραπάνω συμπεραίνουμε ότι

$$x \in D_1^+ \quad \Longleftrightarrow \quad L(x) \in F \oplus (-\infty, 0] \cdot (\underbrace{1, 1, \dots, 1}_{s}, \underbrace{2, 2, \dots, 2}_{t}).$$

Στη συνέχεια θα προσπαθήσουμε να απαλλαγούμε του u. Προς τούτο εισάγουμε μία καινούργια μεταβλητή $\lambda_{s+t} := e^u$. Προφανώς ισχύει:

$$u \in (-\infty, 0] \quad \Longleftrightarrow \quad \lambda_{s+t} \in (0, 1].$$

Άρα, έχουμε ότι $x \in D_1^+$ τότε και μόνο τότε όταν

$$x_i = \lambda_{s+t} \cdot e^{\sum_{k=1}^{r} \lambda_k \upsilon_k^{(i)}}, \qquad \text{για} \quad i = 1, 2, \dots, s$$

και

$$|x_j| = \lambda_{s+t} \cdot e^{\frac{1}{2}\sum_{k=1}^{r} \lambda_k v_k^{(j)}} \qquad \text{για} \quad j = s+1, s+2, \ldots, s+t$$

όπου $0 \leq \lambda_k < 1$ για $1 \leq k \leq s+t-1$ και $0 < \lambda_{s+t} \leq 1$.

Καλύτερα, λόγω του ότι $x_1, x_2, \ldots, x_s \geq 0$, έχουμε ότι $x \in D_1^+$ ακριβώς τότε όταν

$$\left.\begin{array}{ll} & x_i = \lambda_{s+t} \cdot e^{\sum_{k=1}^{r} \lambda_k v_k^{(i)}} \qquad \text{για } i = 1, 2, \ldots, s \\ \text{και} & \\ & x_j = \lambda_{s+t} \cdot e^{\frac{1}{2}\sum_{k=1}^{r} \lambda_k v_k^{(j)}} \qquad \text{για } j = s+1, s+2, \ldots, s+t \end{array}\right\} \tag{2.3}$$

όπου $0 \leq \lambda_k < 1$ για $k = 1, 2, \ldots, r := s+t-1$, και $0 < \lambda_{s+t} \leq 1$.

Η ισοδυναμία αυτή μάς δίνει μία παραμετρικοποίηση του D_1^+ μέσω ενός ημιανοιχτού n-κύβου. Αν επιτρέψουμε στα λ_k να πάρουν και τις συνοριακές τους τιμές (ίσον με μηδέν ή ένα) τότε έχουμε μία παραμετρικοποίηση της θήκης $\overline{D_1^+}$.

Ας ορίσουμε μία συνάρτηση

$$f : \mathbb{R}^n \longrightarrow \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^n,$$

μέσω της ισοδυναμίας (2.3), ως εξής:

$$(\lambda_1, \lambda_2, \ldots, \lambda_n) \longmapsto (x_1, x_2, \ldots, x_{s+t}).$$

Θα δείξουμε ότι $\partial D_1^+ \subseteq F(\partial([0,1]^n))$, δηλαδή θα εφαρμόσουμε τον ορισμό της Lipschitz παραμετρησιμότητας για μία μόνο συνάρτηση, την f. Αρκεί να δείξουμε ότι:

1. $f([0,1]^n) \supseteq \overline{D_1^+}$, και

2. το $(0,1)^n$ απεικονίζεται στο εσωτερικό του D_1^+, δηλαδή $f((0,1)^n) \subseteq \overset{o}{D_1^+}$.

Απόδειξη της 1: Προφανώς, η f είναι συνεχής και $[0,1]^n$ συμπαγές. Συνεπώς το $f([0,1]^n)$ είναι επίσης συμπαγές. Ιδιαίτερα το $f([0,1]^n)$ είναι κλειστό και περιέχει, εξ ορισμού της f, το D_1^+. Επομένως $\overline{D_1^+} \subseteq f([0,1]^n)$.

Απόδειξη της 2: Αρκεί να αποδείξουμε ότι η f είναι **ανοιχτή** απεικόνιση. Για να το

επιτύχουμε αυτό, αναλύουμε την f σε γινόμενο καταλλήλων συναρτήσεων.

$$\begin{pmatrix} \lambda_1 \\ \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \overset{f_1}{\longmapsto} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_{s+t-1} \\ \log \lambda_{s+t} \\ \log \lambda_{s+t+1} \\ \vdots \\ \log \lambda_n \end{pmatrix}$$

$$\overset{f_2}{\longmapsto} \begin{pmatrix} \log \lambda_{s+t} + \sum \lambda_k v_k^{(i)} \\ \vdots \\ 2\log \lambda_{s+t} + \sum \lambda_k v_k^{(j)} \\ \vdots \\ \lambda_{s+t+1} \\ \vdots \\ \lambda_n \end{pmatrix} \begin{matrix} \} \, i = 1, 2, \dots, s \\ \} \, j = s+1, s+2, \dots, s+t \end{matrix}$$

$$\overset{f_3}{\longmapsto} \begin{pmatrix} e^{\sum_{k=1}^r \lambda_k v_k^{(i)}} \\ \vdots \\ e^{\frac{1}{2}\sum_{k=1}^r \lambda_k v_k^{(j)}} \\ \vdots \\ 2\pi\lambda_{s+t+1} \\ \vdots \\ 2\pi\lambda_n \end{pmatrix} \begin{matrix} \} \, i = 1, 2, \dots, s \\ \} \, j = s+1, s+2, \dots, s+t \end{matrix}$$

$$\overset{f_4}{\longmapsto} \begin{pmatrix} e^{\sum_{k=1}^r \lambda_k v_k^{(i)}} \\ \vdots \\ e^{\frac{1}{2}\sum_{k=1}^r \lambda_k v_k^{(j)}} \cos 2\pi\lambda_{s+t+1} \\ e^{\frac{1}{2}\sum_{k=1}^r \lambda_k v_k^{(j)}} \sin 2\pi\lambda_{s+t+1} \\ e^{\frac{1}{2}\sum_{k=1}^r \lambda_k v_k^{(j)}} \cos 2\pi\lambda_n \\ e^{\frac{1}{2}\sum_{k=1}^r \lambda_k v_k^{(j)}} \sin 2\pi\lambda_n \end{pmatrix} \begin{matrix} \} \, i = 1, 2, \dots, s \\ \} \, j = s+1, s+2, \dots, s+t \end{matrix}$$

Τα πεδία ορισμού και τα πεδία τιμών των συναρτήσεων:

$$(0,1)^n \xrightarrow{f_1} \mathbb{R}^n \xrightarrow{f_2} \mathbb{R}^n \xrightarrow{f_3} \mathbb{R}^s \times (0,\infty)^t \times \mathbb{R}^t \xrightarrow{f_4} \mathbb{R}^s \times \mathbb{C}^t$$

Αρκεί να αποδείξουμε ότι οι f_1, f_2, f_3, f_4 είναι **ανοιχτές**. Η f_1 είναι ανοιχτή, είναι ένα πρός ένα και επί, η f_3 είναι ανοιχτή, αφού είναι η εκθετική συνάρτηση, η f_4 είναι επίσης ανοιχτή. Η f_2 είναι γραμμική, αρκεί λοιπόν να δείξουμε ότι έχει rank n. Αυτό όμως είναι προφανές διότι τα υ_k και το $(\underbrace{1,1,\ldots,1}_{s},\underbrace{2,2,\ldots,2}_{t})$ είναι γραμμικά ανεξάρτητα διανύσματα του $\mathbb{R}^{r+s}$, δηλαδή και η f_2 είναι ανοιχτή.

Επομένως και η f είναι ανοιχτή. Απομένει να αποδείξουμε ότι η f είναι Lipschitz ορισμένη στο $[0,1]^n$. Αρκεί να παρατηρήσουμε ότι υπάρχουν όλες οι μερικές παράγωγοι και είναι συνεχείς. Συνεπώς όλες οι μερικές παράγωγοι είναι φραγμένες στον κύβο $[0,1]^n$. Ο κύβος $[0,1]^n$ είναι συμπαγές σύνολο και η f συνεχής σε συμπαγές, άρα είναι φραγμένη και, συνεπώς, Lipschitz, δηλαδη το λήμμα. □

Η απόδειξη του θεωρήματος θα έχει τελειώσει εάν τέλος αποδείξουμε το παρακάτω λήμμα.

Λήμμα 2.1.15 *Αν D θεμελιώδης περιοχή του $\sigma(E_0)$ τότε*

$$Vol(D_1) \;=\; 2^s \pi^t Reg_K.$$

Απόδειξη: Για την ιακωβιανή της f, ισχύει:

$$\big|J(f)\big| \;=\; \prod_{i=1}^{4} \big|J(f_i)\big|$$

και έχουμε

$$\begin{aligned}
|J(f_1)| &= \frac{1}{\lambda_{s+t}},\\
|J(f_3)| &= (2\pi)^t x_1 x_2 \cdots x_s \cdot \frac{1}{2}|x_{s+1}| \cdots |x_{s+t}|,\\
|J(f_4)| &= |x_{s+1}| \cdots |x_{s+t}|, \quad \text{και}\\
|J(f_2)| &= \det \left(\begin{array}{c|c} \begin{array}{c} \upsilon_1 \\ \vdots \\ \hline \upsilon_{s+t+1} \\ \hline 1,1,\ldots,1,2,2,\ldots,2 \end{array} & \begin{array}{c} 0 \\ \\ \\ \end{array} \\ \hline \begin{array}{c} \\ 0 \\ \\ \end{array} & \begin{array}{ccc} 1 & & \\ & \ddots & \\ & & 1 \end{array} \end{array}\right)\\
&= \det \left(\begin{array}{c} \upsilon_1 \\ \hline \vdots \\ \hline \upsilon_{s+t+1} \\ \hline 1,1,\ldots,1,2,2,\ldots,2 \end{array}\right).
\end{aligned}$$

Προσθέτουμε όλες τις στήλες στην τελευταία στήλη και λαμβάνουμε υπ' όψιν ότι

$$\upsilon_k^{(1)} + \cdots + \upsilon_k^{(s+1)} = \log\left|N_{K/\mathbb{Q}}(\varepsilon_k)\right| = \log 1 = 0$$

$|J(f_2)| = n \cdot \det(\upsilon_i) = n \cdot \mathrm{Reg}_K$. Συνεπώς

$$\begin{aligned}
|J(f)| &= \frac{1}{\lambda_{s+k}} \cdot n \cdot \mathrm{Reg}_K \cdot \pi^t |N(x)|\\
&= n\pi^t \mathrm{Reg}_K \cdot \frac{1}{\lambda_{s+t}} \cdot \lambda_{s+t}^n \cdot e^{\left(\sum_{k=1}^{s+t-1} \sum_{i=1}^{s+t-1} \lambda_k \upsilon_k^{(i)}\right)}\\
&= n\pi^t \mathrm{Reg}_K \frac{1}{\lambda_{s+t}} \lambda_{s+t}^n\\
&= n \cdot \pi^t \cdot \mathrm{Reg}_K \cdot \lambda_{s+t}^{n-1}
\end{aligned}$$

Επομένως,

$$\begin{aligned}
\mathrm{Vol}(D_1^+) &= \int_0^1 \int_0^1 \cdots \int_0^1 n\pi^t \mathrm{Reg}_K \cdot \lambda_{s+t}^{n-1} d\lambda_1 d\lambda_2 \cdots d\lambda_n\\
&= \int_0^1 n\pi^t \mathrm{Reg}_K \lambda_{s+t}^n d\lambda_{s+t}\\
&= \pi^t \mathrm{Reg}_K. \quad \square
\end{aligned}$$

Αν τώρα πάρουμε σαν $B = D_1$ στο (2.1.12) και το συνδυάσουμε με το (2.1.11) έχουμε

$$\begin{aligned} A_{\mathfrak{k}}(t) &= \frac{1}{w} \cdot \# \left\{ x \in \sigma(B) \bigcap \sqrt[n]{tN_{K/\mathbb{Q}}(B)} \cdot D_1 \right\} \\ &= \frac{1}{w} \frac{\mathrm{Vol}(D_1)}{\mathrm{Vol}(\sigma(B))} \cdot t \cdot N_{K/\mathbb{Q}}(B) + O(t^{1-\frac{1}{n}}) \\ &\overset{(*)}{=} \frac{1}{w} \frac{2^s \pi^t \mathrm{Reg}_K}{2^{-t}|D_K|^{1/2} N_{K/\mathbb{Q}}(B)} \cdot t \cdot N_{K/\mathbb{Q}}(B) + O(t^{1-\frac{1}{n}}) \\ &= \frac{2^s (2\pi)^t \mathrm{Reg}_K}{w\sqrt{|D_K|}} \cdot t + O(t^{1-\frac{1}{n}}) \end{aligned}$$

Η ισότητα $(*)$ είναι άμεσο αποτέλεσμα γνωστής πρότασης της Αλγεβρικής Θεωρίας Αριθμών.

Στη συνέχεια θα γενικεύσουμε το θεμελιώδες θεώρημα αυτής της παραγράφου γενικεύοντας την έννοια της ομάδας κλάσεων ιδεωδών. I_K ήταν η ομάδα όλων των ιδεωδών του K, H_K η ομάδα των κυρίων ιδεωδών αυτού και $\mathfrak{K} = {}^{I_K}\!/_{H_K}$ η ομάδα κλάσεων ιδεωδών του σώματος K. Τώρα θα δημιουργήσουμε κλάσεις ισοδυναμίας μέσω μιάς μικρότερης ομάδας.

Ορισμός 2.1.16 *1. Το $\alpha \in K$ θα λέγεται* **πλήρως θετικό** *(total positive) $\alpha \gg 0$ όταν και μόνον όταν* **όλοι** *οι πραγματικοί συζυγείς του α είναι θετικοί, δηλαδή*

$$\sigma_1(\alpha), \ldots, \sigma_s(\alpha) > 0.$$

2. Σαν **κύρια κλάση** *με την* **στενή έννοια** *θα ορίσουμε την ομάδα*

$$H_K^+ = \{(\alpha) \mid \alpha \in K^*, \alpha \gg 0\}.$$

3. Η ομάδα $\mathfrak{K}^+ = {}^{I_K}\!/_{H_K^+}$ λέγεται **ομάδα κλάσεων με την στενή έννοια**.

Ορισμός 2.1.17 *Έστω $\mathfrak{m}$ ένα ακέραιο ιδεώδες του K.*

1. Η υποομάδα

$$H_{\mathfrak{m}}^+ := \left\{ (\alpha) \;\middle|\; \alpha \in K^*, \alpha \gg 0, \alpha = \frac{\alpha_1}{\alpha_2}, \alpha_i \in R_K, a_i \equiv 1 \,(mod\, \mathfrak{m}) \right\}$$

θα λέγεται n **ακτίνα** *modulo $\mathfrak{m}$ του K. (Εδώ ακτίνα μεταφράζουμε τη λέξη Strahl από τα γερμανικά ή τη λέξη ray από τα αγγλικά.)*

2. *Έστω* $A_{\mathfrak{m}}$ *η ομάδα ιδεωδών του* K *τα οποία είναι πρώτα προς τον* $\mathfrak{m}$ *(δηλαδή κανένα πρώτο ιδεώδες* P, $P|\mathfrak{m}$, *δεν εμφανίζεται στην ανάλυση των* $A \in A_{\mathfrak{m}}$*). Η ομάδα* $\mathfrak{K}_{\mathfrak{m}}^{+} = {}^{A_{\mathfrak{m}}}/_{H^{+}_{\mathfrak{m}}}$ *θα λέγεται ομάδα κλάσεων modulo* $\mathfrak{m}$ *στο* K *(Strahlklassengruppe modulo* $\mathfrak{m}$ *ή ray class group του* K*).*

Χωρίς απόδειξη αναφέρουμε το

Θεώρημα 2.1.18 *Η ομάδα κλάσεων modulo* $\mathfrak{m}$ *του* K, $\mathfrak{K}_{\mathfrak{m}}^{+}$ *είναι* **πεπερασμένης τάξης**.

Θεώρημα 2.1.19 *Για κάθε κλάση* $\mathfrak{k}_m^{+} \in \mathfrak{K}_{\mathfrak{m}}^{+}$ *ισχύει*

$$\begin{aligned} A_{\mathfrak{K}_{\mathfrak{m}}^{+}}(t) &= \#\left\{A \in \mathfrak{K}_{\mathfrak{m}}^{+} \;\middle|\; A \text{ ακέραιο}, N_{K/\mathbb{Q}}(A) \leq t\right\} \\ &= \left(\lambda \frac{h}{|\mathfrak{K}_{\mathfrak{m}}^{+}|} t\right) + O(t^{1-\frac{1}{n}}) \end{aligned}$$

όπου λ *όπως στο Θεμελιώδες Θεώρημα 2.1.3.*

Απόδειξη: Ανάλογη του Θεμελιώδους Θεωρήματος 2.1.3. □

2.2 Η ζήτα συνάρτηση του Dedekind αλγεβρικού σώματος αριθμών

2.2.1 Ορισμός και ιδιότητες

Ανάλογα προς τη ζήτα συνάρτηση του Riemann θα ορίσουμε τώρα τη **ζήτα συνάρτηση του Dedekind** ενός αλγεβρικού σώματος αριθμών K. Για λόγους ευκολίας θα συμβολίζουμε την norm ενός ιδεώδους A του K με $N(A)$ αντί $N_{K/\mathbb{Q}}(A)$. Ορίζουμε

$$\zeta_K(s) := \sum_{\substack{A \in I_K \\ A \text{ ακέραιο}}} \frac{1}{(N(A))^s}, \quad s \in \mathbb{C}, \quad Re(s) > 1.$$

Η ζήτα συνάρτηση του Riemann είναι η ζήτα συνάρτηση του Dedekind για το σώμα $\mathbb{Q}$.

Λήμμα 2.2.1 *Η ζήτα συνάρτηση του Dedekind* $\zeta_K(s)$ **συγκλίνει απόλυτα** *για* $Re(s) > 1$ *και παριστά, σ΄ αυτό το ημιεπίπεδο μία* **ολόμορφη συνάρτηση**.

Απόδειξη: $\zeta_K(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$ όπου $a_m = \#\{A \in I_K \;|\; A \text{ ακέραιο}, \; N(A) = m\}$. Επομένως

$$A(t) = \sum_{m \leq t} a_m$$

(η σειρά αποκλίνει), άρα μπορούμε να εφαρμόσουμε το θεώρημα (1.2.5). Επειδή

$$A(t) \;=\; \lambda \cdot h \cdot t + O(t^{1-\frac{1}{n}}) \;=\; O(t).$$

θα έχουμε ότι η $\zeta_K(s)$ συγκλίνει για $Re(s) > 1$ και επειδή $a_m \in \mathbb{N}$ για κάθε φυσικό m, θα συγκλίνει και απολύτως για $Re(s) > 1$ και σύμφωνα με το θεώρημα 1.2.4 παριστά μία ολόμορφη συνάρτηση στο εν λόγω ημιεπίπεδο. □

Το κύριο θεώρημα της παρούσης παραγράφου είναι το:

Θεμελιώδες Θεώρημα 2.2.2 (αναλυτικός τύπος του αριθμού κλάσεων)
Έστω K αλγεβρικό σώμα αριθμών, $n = (K : \mathbb{Q})$. Η $\zeta_K(s)$ επεκτείνεται σε μία **μερόμορφη συνάρτηση** *στο ημιεπίπεδο $Re(s) > 1-\frac{1}{n}$ με μοναδικό* **απλό πόλο** *για $s = 1$ και*

$$Res_{s=1}(\zeta_K(s)) \;=\; \lim_{s\to 1^+}(s-1)\zeta_K(s) \;=\; \lambda \cdot h \;=\; \frac{2^s(2\pi)^t\, Reg_K}{w\sqrt{|D_K|}} \cdot h.$$

Σημείωση: Στην οριακή περίπτωση που $r = s + t - 1 = 0$, θέτουμε $\mathrm{Reg}_K = 1$.

Απόδειξη: Θα κάνουμε χρήση του θεωρήματος 1.5.5 της σελίδας 31, ότι η $\zeta(s)$ είναι μερόμορφη στο $\mathbb{C}$ (εδώ φτάνει το $Re(s) > 0$) με μοναδικό απλό πόλο για $s = 1$ και υπόλοιπο ίσο με 1.

$$\zeta_K(s) \;=\; \sum_{m=1}^{\infty}\frac{a_m}{m^s} \;=\; \sum_{m=1}^{\infty}\frac{a_m - \lambda\cdot h}{m^s} + \lambda\cdot h\cdot\zeta(s)$$

Προφανώς

$$\begin{aligned}\sum_{m\le t}(a_m - \lambda h) \quad &= \quad A(t) - [t]\lambda\, h \;=\; A(t) - \lambda\, t\, h + O(1)\\ &\overset{\vartheta.\ 2.1.3}{=} \quad O(t^{1-\frac{1}{n}}) + O(1) \;=\; O(t^{1-\frac{1}{n}})\end{aligned}$$

Επομένως

1. Η $\displaystyle\sum_{m=1}^{\infty}\frac{a_m - \lambda\, h}{m^s}$ είναι ολόμορφη για $Re(s) > 1 - \frac{1}{n}$ (δες Θεωρήματα 1.2.5 και 1.2.6).

2. Η $\zeta_K(s)$ επεκτείνεται στο ημιεπίπεδο $Re(s) > 1 - \frac{1}{n}$ και έχει μοναδικό απλό πόλο στη θέση $s = 1$.

3. $Res\,\zeta_K(s)_{s=1} = \lambda \cdot h \cdot Res\,\zeta(s)_{s=1} = \lambda \cdot h$

Εύκολα μπορεί να δείξει κανείς ότι $a_m\, a_n = a_{mn}$ για $(m,n)=1$ (δες π.χ. [19], σελίδα 144). Τώρα εφαρμόζουμε το θεώρημα 1.3.2.

$$\begin{aligned}\zeta_K(s) &= \sum_{\substack{A\in I_K\\ A\ \text{ακέραιο}}} \frac{1}{N(A)^s} = \prod_{P\in\mathbb{P}(K)} \left\{1+\frac{1}{N(P)^s}+\frac{1}{N(P)^{2s}}+\cdots\right\}\\ &= \prod_{P\in\mathbb{P}(K)} \frac{1}{1-N(P)^{-s}} \qquad \text{(Γινόμενο Euler)}\end{aligned}$$

Το $\mathbb{P}(K)$ συμβολίζει το σύνολο όλων των πρώτων ιδεωδών του αλγεβρικού σώματος αριθμών K. □

2.2.2 Υπολογισμός του αριθμού κλάσεων μέσω του Θεωρήματος (2.2.2)

Έστω $K=\mathbb{Q}(\sqrt{d})$ τετραγωνικό σώμα αριθμών διακρίνουσας d. Ο νόμος ανάλυσης στο K είναι:

$$pR_K = \begin{cases} PP', & N(P)=N(P')=p, & \text{αν } \left(\frac{d}{p}\right)=1\\ P, & N(P)=p^2, & \text{αν } \left(\frac{d}{p}\right)=-1\\ P^2, & N(P)=p, & \text{αν } \left(\frac{d}{p}\right)=0\end{cases}$$

οπότε η ζήτα συνάρτηση του K γράφεται:

$$\begin{aligned}\zeta_K(s) &= \prod_{P\in\mathbb{P}(K)} \frac{1}{1-N(P)^{-s}}\\ &= \prod_{\left(\frac{d}{p}\right)=1} \frac{1}{(1-p^{-s})^2} \prod_{\left(\frac{d}{p}\right)=-1} \frac{1}{1-p^{-2s}} \prod_{\left(\frac{d}{p}\right)=0} \frac{1}{1-p^{-s}}\\ &= \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}} \prod_{\left(\frac{d}{p}\right)=1} \frac{1}{1-p^{-s}} \prod_{\left(\frac{d}{p}\right)=-1} \frac{1}{1+p^{-s}} \prod_{\left(\frac{d}{p}\right)=0} \frac{1}{1-0\cdot p^{-s}}\\ &= \zeta_{\mathbb{Q}}(s) \prod_{p\in\mathbb{P}} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \zeta_{\mathbb{Q}}(s) L(s/\chi)\end{aligned}$$

όπου $\chi(p)=\left(\frac{d}{p}\right)$ και $\zeta_{\mathbb{Q}}(s)$ είναι η ζήτα συνάρτηση του Riemann, $\zeta(s)$.

Αυτό το αποτέλεσμα είναι ειδική περίπτωση ενός γενικότερου θεωρήματος. Προέκυψε σαν συνδυασμός του γινομένου Euler για τη ζήτα συνάρτηση του Dedekind και του νόμου ανάλυσης ενός τετραγωνικού αλγεβρικού σώματος αριθμών.

Αν τώρα περάσουμε στα υπόλοιπα της $\zeta_K(s)=\zeta_{\mathbb{Q}}(s)L(s/\chi)$ στη θέση $s=1$ για $K=\mathbb{Q}(\sqrt{d})$

με $d = D_K$, δηλαδή $n = 2$, $t = 1$, $s = 0$, $\mathrm{Reg}_K = 1$, τότε βρίσκουμε:

$$\frac{2\pi}{w\sqrt{|d|}}\, h_K \;=\; 1 \cdot L(1/\chi) \;=\; L(1/\chi).$$

Σαν ειδική περίπτωση ενός θεωρήματος που θα αποδείξουμε παρακάτω προκύπτει ότι για $d < 0$

$$\big|L(1/\chi)\big| \;=\; \frac{\pi}{|d|\sqrt{|d|}} \left| \sum_{\substack{(\nu,d)=1 \\ 0<\nu<|d|}} \chi(\nu)\nu \right|.$$

Επομένως: **Τύπος αριθμού κλάσεων για μιγαδικά τετραγωνικά σώματα**

$$h_K \;=\; \frac{w}{2|d|} \left| \sum_{\substack{(\nu,d)=1 \\ 0<\nu<|d|}} \chi(\nu)\nu \right|$$

Παραδείγματα:

1. Για $d = -4$, $p \in \mathbb{P}$, $p \neq 2$, $\chi(p) = \left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right)$ άρα $h = \frac{4}{2 \cdot 4}\big|\chi(1) \cdot 1 + \chi(3) \cdot 3\big| = \frac{1}{2}|1 - 3| = 1$

2. Για $d = -20$, $\chi(p) = \left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right)_{p\neq 2} = (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) =$

$$= \begin{cases} 1, & \text{όταν } p \equiv \pm 1 \pmod 5 \\ -1, & \text{όταν } p \equiv \pm 2 \pmod 5 \end{cases}$$

$$h_{\mathbb{Q}(\sqrt{-20})} = \frac{1}{20}\,\big(\,\chi(1)\cdot 1 + \chi(3)\cdot 3 + \chi(7)\cdot 7 + \chi(9)\cdot 9 + \chi(11)\cdot 11 + \\ + \chi(13)\cdot 13 + \chi(17)\cdot 17 + \chi(19)\cdot 19\,\big)$$

Για $\nu = 1, 3, 7, 9, 11, 13, 17, 19$ έχουμε $\chi(\nu) = 1, 1, 1, 1, -1, -1, -1, -1$ αντίστοιχα. Επομένως

$$h_{\mathbb{Q}(\sqrt{-20})} \;=\; \frac{1}{20}|1+3+7+9-11-13-17-19| \;=\; \frac{1}{20}|20-60| \;=\; 2.$$

Ορισμός 2.2.3 *Ένας χαρακτήρας Dirichlet mod N θα λέγεται* **άρτιος** *αν $\chi(-1) = 1$ και* **περιττός** *αν $\chi(-1) = -1$. Ξαναθυμόμαστε τον ορισμό των* **αθροισμάτων Gauss**. *Αν ζ είναι μία* **πρωταρχική** *N-ρίζα της μονάδας, χ χαρακτήρας Dirichlet modulo N και $a \in \mathbb{Z}$*

$$\tau_a(\chi) := \sum_{x \bmod N} \chi(x)\zeta^{ax}$$

$$\tau_1(\chi) := \tau(\chi)$$

Θεώρημα 2.2.4 *Έστω* χ **πρωταρχικός** *χαρακτήρας modulo* N, $N>1$. *Αν* χ **άρτιος** *τότε*

$$L(1/\chi) \;=\; -\frac{\tau(\chi)}{N}\sum_{\substack{0<\nu<N\\(\nu,N)=1}}\overline{\chi}(\nu)\log|1-\zeta^{-\nu}|$$

όπου $\zeta = e^{\frac{2\pi i}{N}}$. *Αν* χ **περιττός** *τότε*

$$L(1/\chi) = \frac{\pi i\tau(\chi)}{N^2}\sum_{\substack{0<\nu<N\\(\nu,N)=1}}\overline{\chi}(\nu)\nu$$

όπου $\overline{\chi}$ *ο συζυγής του* χ.

Υπενθυμίζουμε μερικές ιδιότητες των αθροισμάτων Gauss, για πρωταρχικό χαρακτήρα mod N, $N>1$, χρήσιμες για τα παρακάτω.

(1) $\big|\tau_a(\chi)\big| = \begin{cases}\sqrt{N}, & \text{αν } (a,N)=1\\ 0, & \text{αν } (a,N)\neq 1\end{cases}$

(2) $\tau_a(\chi) = \overline{\chi}(a)\tau(\chi)$

(3) $\displaystyle\sum_{\nu \bmod N}\zeta^{\nu r} = \begin{cases}N, & \text{όταν } r\equiv 0(N)\\ 0, & \text{όταν } r\not\equiv 0(N)\end{cases}$

Η ιδιότητα (3) είναι προφανής. Αποδείξεις των (1) και (2) μπορεί να βρεί ο ενδιαφερόμενος αναγνώστης στο [20], σελίδα 91. Το ότι για $(a,N)>1$ ισχύει $\tau_\alpha(\chi)=0$ προκύπτει ήδη από την (1).

Προχωρούμε τώρα στην απόδειξη του θεωρήματος 2.2.4.

Απόδειξη:

$$L(s/\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} \;=\; \sum_{\substack{x \bmod N\\(x,N)=1}}\chi(x)\Bigg(\underbrace{\sum_{n\equiv x \bmod N}\frac{1}{n^s}}_{(*)}\Bigg)$$

όπου η $(*) \;=\; \displaystyle\sum_{n=1}^{\infty}\frac{c_n}{n^s}$ με $c_n = \begin{cases}1, & \text{αν } n\equiv x\,(\mathrm{mod}\,N)\\ 0, & \text{αν } n\not\equiv x\,(\mathrm{mod}\,N).\end{cases}$

Η ιδιότητα (3) των αθροισμάτων Gauss μας δίνει

$$\begin{aligned} L(s/\chi) &= \sum_{\substack{x \bmod N \\ (x,N)=1}} \chi(x) \sum_{n=1}^{\infty} \frac{1}{N} \sum_{\nu \bmod N} \zeta^{(x-n)\nu} \cdot \frac{1}{n^s} \\ &= \frac{1}{N} \sum_{\nu \bmod N} \left(\sum_{\substack{x \bmod N \\ (x,N)=1}} \chi(x) \zeta^{x\nu} \right) \sum_{n=1}^{\infty} \frac{\zeta^{-n\nu}}{n^s} \\ &= \frac{1}{N} \sum_{\nu \bmod N} \tau_\nu(x) \sum_{n=1}^{\infty} \frac{\zeta^{-n\nu}}{n^s} \end{aligned}$$

Αν $(\nu, N) \neq 1$, τότε $\tau_\nu(x) = 0$. Επομένως

$$L(s/\chi) = \frac{1}{N} \sum_{\substack{\nu \bmod N \\ (\nu,N)=1}} \tau_\nu(x) \sum_{n=1}^{\infty} \frac{\zeta^{-n\nu}}{n^s}$$

Ισχυρίζομαι ότι:

(4) Αν $\nu \not\equiv 0 \,(\mathrm{mod}\, N)$ τότε η $\displaystyle\sum_{n=1}^{\infty} \frac{\zeta^{-n\nu}}{n^s}$ συγκλίνει για $Re(s) > 0$ και είναι συνεχής στο δεξιό ημιεπίπεδο $Re(s) > 0$.

Πράγματι:

για $\nu \not\equiv 0 \,(\mathrm{mod}\, N)$ έχουμε ότι $A(t) = \displaystyle\sum_{n \leq t} \zeta^{-\nu n} = O(1)$ και επομένως το θεώρημα 1.2.4 δίνει ότι η σειρά συγκλίνει για $Re(s) > 0$ και είναι ολόμορφη σ΄ αυτό το ημιεπίπεδο. Έχουμε λοιπόν:

$$L(1/\chi) = \frac{1}{N} \sum_{\substack{\nu \bmod N \\ (\nu,N)=1}} \tau_\nu(\chi) \sum_{n=1}^{\infty} \frac{(\zeta^{-\nu})^n}{n}$$

Για $\zeta^{-\nu} \neq 1$ (δηλαδή για $|\zeta^{-\nu}| < 1$) η τελευταία σειρά γράφεται

$$\sum_{n=1}^{\infty} \frac{\zeta^{-n\nu}}{n} = -\log(1 - \zeta^{-\nu})$$

(Ο πρωτεύων κλάδος του λογαρίθμου). Αυτό και η ιδιότητα 2 των αθροισμάτων Gauss $\tau_a(\chi) = \overline{\chi(a)}\tau(\chi)$ μας δίνουν:

Λήμμα 2.2.5 *Αν χ και N όπως στο θεώρημα (2.2.4) τότε*

$$L(1/\chi) = -\frac{\tau(\chi)}{N} \sum_{\substack{\nu \bmod N \\ (\nu,N)=1}} \overline{\chi}(\nu) \log(1 - \zeta^{-\nu})$$

Ας συμβολίσουμε

$$S_\chi := \sum_{\nu \bmod N} \overline{\chi}(\nu) \log(1-\zeta^{-\nu})$$

Λήμμα 2.2.6 *Αν* $\zeta = e^{2\pi i/N}$ *τότε*

$$S_\chi := \sum_{\substack{\nu \bmod N \\ (\nu,N)=1}} \overline{\chi}(\nu) \log|1-\zeta^{-\nu}| \qquad \textit{για } \chi(-1)=1$$

και

$$S_\chi = \frac{\pi\, i}{N} \sum_{\substack{0<\nu<N \\ (\nu,N)=1}} \overline{\chi}(\nu)\, \nu \qquad \textit{για } \chi(-1)=-1$$

Παρατήρηση: Άμεση συνέπεια των λημμάτων (2.2.5) και (2.2.6) είναι η αλήθεια του θεωρήματος 2.2.4. □

Για την απόδειξη του λήμματος (2.2.6) χρειαζόμαστε πρώτα το

Λήμμα 2.2.7 *Αν* $0<\nu<N$ *και* $(\nu,N)=1$ *για τον πρωτεύοντα κλάδο του λογαρίθμου έχουμε:*

$$\begin{aligned} \log(1-\zeta^{-\nu}) &= \log\left|1-\zeta^{-\nu}\right| + i\pi\left(\frac{1}{2}-\frac{\nu}{N}\right) \\ \log(1-\zeta^{\nu}) &= \log\left|1-\zeta^{\nu}\right| - i\pi\left(\frac{1}{2}-\frac{\nu}{N}\right) \end{aligned}$$

όπου $\zeta := e^{2\pi i/N}$.

Απόδειξη: Έστω $\Theta := e^{-2\pi i\nu/2N}$, δηλαδή $\Theta^2 = \zeta^{-\nu}$ οπότε θα έχουμε

$$\begin{aligned} 1-\zeta^{-\nu} &= 1-\Theta^2 = \left(\overline{\Theta}-\Theta\right)\Theta \\ &= \left(2\sin\frac{\pi\nu}{N}\right) i\,\Theta \\ &= \left(2\sin\frac{\pi\nu}{N}\right) e^{\pi i\left(\frac{1}{2}-\frac{\nu}{N}\right)} \\ \Longrightarrow \qquad \log(1-\zeta^{-\nu}) &= \log\left|1-\zeta^{-\nu}\right| + i\pi\left(\frac{1}{2}-\frac{\nu}{N}\right). \end{aligned}$$

Όμοια αποδεικνύεται και η δεύτερη σχέση. □

Για την απόδειξη του λήμματος (2.2.6) έχουμε:

Απόδειξη: Αν χ άρτιος τότε συνεπάγεται ότι $\chi(\nu) = \chi(-\nu)$ οπότε:

$$\begin{aligned} S_\chi &= \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \log(1-\zeta^{-\nu}) \\ &= \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(-\nu) \log(1-\zeta^{-\nu}). \end{aligned}$$

Αν αντικαταστήσουμε το $-\nu$ με ν έχουμε

$$S_\chi = \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \log(1-\zeta^{\nu}).$$

Προσθέτουμε κατά μέλη τις δύο εκφράσεις του S_χ και έχουμε

$$\begin{aligned} S_\chi &= \frac{1}{2} \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \left\{ \log(1-\zeta^{-\nu}) + \log(1-\zeta^{\nu}) \right\} \\ &= \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \log|1-\zeta^{-\nu}| \end{aligned}$$

Έστω τώρα ότι χ περιττός, τότε $\chi(-1) = -1$ συνεπώς $\chi(-\nu) = -\chi(\nu)$ άρα θα έχουμε ότι

$$\begin{aligned} S_\chi &= \frac{1}{2} \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \left\{ \log(1-\zeta^{-\nu}) - \log(1-\zeta^{\nu}) \right\} \\ &= \pi i \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \left(\frac{1}{2} - \frac{\nu}{N} \right) \\ &= -\frac{\pi i}{N} \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu)\nu + \frac{\pi i}{2} \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu) \\ &= -\frac{\pi i}{N} \sum_{\substack{\nu=1 \\ (\nu,N)=1}}^{N-1} \overline{\chi}(\nu)\nu \end{aligned}$$

Η τελευταία ισότητα προκύπτει, επειδή $\chi \neq \chi_0$. □

2.3 Ο τύπος του αριθμού κλάσεων για τετραγωνικά σώματα αριθμών

2.3.1 Τετραγωνικά μιγαδικά σώματα αριθμών.

Έστω $K = \mathbb{Q}(\sqrt{d})$ τετραγωνικό μιγαδικό σώμα αριθμών δικρίνουσας d . Έχουμε ήδη αποδείξει ότι $\zeta_K(s) = \zeta_{\mathbb{Q}}(s)L(s/\chi)$ όπου χ ο χαρακτήρας χ_d που αντιστοιχεί στην θεμελιώδη διακρίνουσα d.

Το θεώρημα (1.1.9) μας εξασφαλίζει ότι ο χ_d είναι πρωταρχικός χαρακτήρας $\bmod|d|$ και ότι

$$\chi_d(-1) = \begin{cases} 1, & \text{αν } d > 0 \\ -1, & \text{αν } d < 0 \end{cases}$$

Έστω τώρα $d < 0$, συνεπώς ο χ_d είναι περιττός. Ο τύπος για τον αριθμό κλάσεων είναι:

$$h_K \frac{2\pi}{w\sqrt{d}} = L(1/\chi).$$

Το κύριο θεώρημα της προηγούμενης παραγράφου δίνει

$$\frac{2\pi}{w\sqrt{|d|}} h_K = \frac{\pi \cdot i \cdot \tau(\chi)}{d^2} \sum_{\substack{0<\nu<|d| \\ (\nu,|d|)=1}} \overline{\chi}(\nu)\nu.$$

Ισχύει ακόμη το

Θεώρημα 2.3.1 *Αν χ πρωταρχικός τετραγωνικός χαρακτήρας modulo N τότε*

$$\tau(\chi) = \begin{cases} \sqrt{N}, & \text{όταν } \chi \text{ άρτιος} \\ i\sqrt{N}, & \text{όταν } \chi \text{ περιττός} \end{cases}$$

Απόδειξη του θεωρήματος αυτού μπορεί να βρεί ο ενδιαφερόμενος στο [8], κεφάλαιο 5, θεώρημα 7.

Επομένως

Θεώρημα 2.3.2 (τύπος του αριθμού κλάσεων)

$$h_K = -\frac{w}{2\,|d|} \sum_{\substack{0<x<|d| \\ (x,d)=1}} \chi(x)\, x$$

Θεώρημα 2.3.3 *Για $d < -4$, d θεμελιώδης διακρίνουσα, ισχύει:*

$$h_K = \frac{w}{2} \cdot \frac{1}{2 - \chi(2)} \cdot \sum_{\substack{0<\nu<\frac{|d|}{2} \\ (\nu,|d|)=1}} \chi(\nu)$$

Απόδειξη: Υποθέτουμε ότι ο d είναι περιττός. Έστω

$$U := \sum_{\nu=1}^{|d|-1} \overline{\chi}(\nu)\,\nu$$

Αν ο ν είναι άρτιος, γράφουμε $\nu = 2k$ με $0 < k < \frac{|d|}{2}$ και αν ο ν είναι περιττός τότε γράφουμε $\nu = 2k - |d|$ όπου $\frac{|d|}{2} < k < |d|$. Επομένως

$$\begin{aligned} U &= \sum_{0<k<\frac{|d|}{2}} \chi(2k)\,2k + \sum_{\frac{|d|}{2}<k<|d|} \chi(2k-|d|)\,(2k-|d|) \\ &= \sum_{0<k<\frac{|d|}{2}} \chi(2k)\,2k + \sum_{\frac{|d|}{2}<k<|d|} \chi(2k)\,(2k-|d|) \\ &= 2\sum_{0<k<|d|} \chi(2k)\,k \;-\; |d| \sum_{\frac{|d|}{2}<k<|d|} \chi(2k) \\ &= 2\chi(2)U - |d|\chi(2) \sum_{\frac{|d|}{2}<x<|d|} \chi(k) \end{aligned}$$

Συνεπώς

$$U = \frac{|d|\chi(2)}{2\chi(2)-1} \cdot \sum_{\frac{|d|}{2}<k<|d|} \chi(k)$$

Επειδή $\chi(2) = \pm 1$ η σταθερά γράφεται $\frac{|d|}{2 - \chi(2)}$ και επειδή $\sum_{0<k<|d|} \chi(k) = 0$ έχουμε

$$U = \frac{-|d|}{2 - \chi(2)} \cdot \sum_{0<k<\frac{|d|}{2}} \chi(k),$$

δηλαδή έχουμε αποδείξει το θεώρημα για d περιττό.

Η περίπτωση κατά την οποία d άρτιος αφήνεται σαν **άσκηση** στον αναγνώστη. □

Αν τώρα $d = -p$, $p \equiv 3 \pmod 4$ τότε $\chi(x) = \left(\frac{-p}{x}\right) = \left(\frac{x}{p}\right)$ και

$$\chi(2) \;=\; \left(\frac{2}{p}\right) \;=\; \begin{cases} -1, & p \equiv 3 \pmod 8 \\ 1, & p \equiv 7 \pmod 8 \end{cases}$$

Επομένως

Θεώρημα 2.3.4 *Έστω p πρώτος, $p \neq 3$, $p \equiv 3 \,(mod\, 4)$, $h := h_{\mathbb{Q}(\sqrt{-p})}$. Τότε*

$$h \;=\; \begin{cases} \dfrac{1}{3}(R-N), & \text{όταν } p \equiv 3 \,(mod\, 8) \\ R-N, & \text{όταν } p \equiv 7 \,(mod\, 8) \end{cases}$$

Όπου R, N το πλήθος των τετραγωνικών υπολοίπων (όχι υπολοίπων) $mod\, p$ στο διάστημα $(0, p/2)$.

Παράδειγμα: Για $d = -19$ στο $[0, 9]$ έχουμε 6 τετραγωνικά υπόλοιπα 1,4,5,6,7,9 και 3 *όχι* τετραγωνικά υπόλοιπα 2,3,8. Επομένως

$$h(-19) \;=\; \frac{1}{3}(6-3) \;=\; 1.$$

Ο Gauss υπολόγισε το $h(d)$ για $0 > d > -10.000$ και δεν βρήκε άλλη θεμελιώδη διακρίνουσα με $h(d) = 1$ εκτός των $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Διατύπωσε την εικασία ότι δεν υπάρχουν άλλα μιγαδικά τετραγωνικά σώματα αριθμών με $h(d) = 1$ και ότι

$$h(d) \longrightarrow \infty \quad \text{για} \quad d \to -\infty. \tag{2.4}$$

Η (2.4) αποδείχτηκε το 1934 απο τον Heilbronn. Το 1935 ο Siegel απέδειξε κάτι πολύ πιο ισχυρό:

$$\textit{για κάθε } \varepsilon > 0 \quad \textit{ισχύει} \quad h(d) > C\,|d|^{\frac{1}{2}-\varepsilon}$$

όπου C κατάλληλη, αλλά μη εξαρτώμενη από το ε, σταθερά.

Είναι εύκολο να δειχτεί ότι

$$h(d) \;<\; c'\,|d|^{\frac{1}{2}+\varepsilon},$$

δηλαδή έχομε το θεώρημα του **Siegel**:

$$\lim_{d\to-\infty} \frac{\log h(d)}{\log |d|} \;=\; \frac{1}{2}.$$

Το ότι δεν υπάρχει άλλο τετραγωνικό μιγαδικό σώμα αριθμών με $h(d) = 1$, είναι αποτέλεσμα του Heegner (1952), η απόδειξη του οποίου όμως είχε ένα "κενό" το οποίο έκλεισε στα τέλη της δεκαετίας του 1960, αρχές της δεκαετίας του 1970. Στο θέμα αυτό ίσως επανέλθουμε, σε προσεχή μας έκδοση.

2.3.2 Τετραγωνικά πραγματικά σώματα αριθμών.

Ο αριθμός κλάσεων για πραγματικό τετραγωνικό σώμα αριθμών

$$K = \mathbb{Q}(\sqrt{d}), \quad \text{διακρίνουσας } d > 0.$$

Η γνωστή ήδη σχέση $\operatorname{Res}\zeta_K(s)_{s=1} = L(1/\chi)$ δίνει

$$\frac{2^{s+t}\pi^t \mathrm{Reg}_K \cdot h_K}{w\sqrt{|d|}} = -\frac{\tau(\chi)}{|d|} \cdot \sum_{\substack{0<x<|d| \\ (x,d)=1}} \chi(x) \log|1-\zeta^x|$$

όπου $\zeta = e^{\frac{2\pi i}{|d|}}$, $s=2$, $t=0$, $w=2$, $\mathrm{Reg}_K = \log\varepsilon_0$ με ε_0 την κανονικοποιημένη ($\varepsilon_0 > 1$) θεμελιώδη μονάδα του K.

Λόγω των γνωστών ιδιοτήτων,

$$\tau(\chi) = \sqrt{d}, \qquad \left|1-\zeta^x\right| = \left|1-\zeta^{-x}\right|$$

και $\chi(-x) = \chi(x)$ (διότι $d>0$ συνεπώς ο χ είναι άρτιος) θα έχουμε

$$\text{δεξιό μέλος} = -\frac{2}{\sqrt{d}} \sum_{\substack{0<x<\frac{|d|}{2} \\ (x,d)=1}} \chi(x) \log\left|1-\zeta^x\right|.$$

Επειδή, για x, $\quad 0 < x < \frac{|d|}{2}$

$$\left|1-\zeta^x\right| = \left|\zeta^{-\frac{x}{2}} - \zeta^{\frac{x}{2}}\right| = \left|e^{-\frac{2\pi i x}{2d}} - e^{+\frac{2\pi i x}{2d}}\right| = 2\sin\frac{\pi x}{d}$$

έχουμε

$$\begin{aligned} \text{δεξιό μέλος} &= -\frac{2}{\sqrt{d}} \sum_{\substack{0<x<\frac{d}{2} \\ (x,d)=1}} \chi(x) \left(\log 2 + \log\sin\frac{\pi x}{d}\right) \\ &= -\frac{2}{\sqrt{d}} \sum_{\substack{0<x<\frac{d}{2} \\ (x,d)=1}} \chi(x) \log\left(\sin\frac{\pi x}{d}\right). \end{aligned}$$

Επομένως έχουμε

Θεώρημα 2.3.5 *Έστω $K = \mathbb{Q}(\sqrt{d})$ τετραγωνικό πραγματικό σώμα αριθμών διακρίνουσας $d>0$, χ ο πρωταρχικός χαρακτήρας που αντιστοιχεί στην d και $\varepsilon_0 > 1$ θεμελιώδης μονάδα*

του. Τότε

$$h_K \cdot \log \varepsilon_0 = \log \left[\frac{\displaystyle\prod_{\substack{0<x<\frac{d}{2} \\ \chi(x)=-1}} \sin \frac{\pi x}{d}}{\displaystyle\prod_{\substack{0<x<\frac{d}{2} \\ \chi(x)=1}} \sin \frac{\pi x}{d}} \right]$$

Παράδειγμα:

$K = \mathbb{Q}(\sqrt{5})$, $d = 5$. Γράφουμε τον τύπο σαν

$$\varepsilon_0^{h_K} = \frac{\displaystyle\prod_{\substack{0<x<\frac{d}{2} \\ \chi(x)=-1}} \sin \frac{\pi x}{d}}{\displaystyle\prod_{\substack{0<x<\frac{d}{2} \\ \chi(x)=1}} \sin \frac{\pi x}{d}}$$

όπου $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$. Θα έχουμε λοιπόν ότι

$$\text{δεξιό μέλος} = \frac{\sin \frac{2\pi}{5}}{\sin \frac{\pi}{5}} = 2 \cos \frac{\pi}{5} = \frac{1+\sqrt{5}}{2} \quad \Longrightarrow \quad h_K = 1.$$

Θα προσπαθήσουμε τώρα να δώσουμε **αριθμητικό** περιεχόμενο στον τύπο του αριθμού κλάσεων. Έχουμε το ακόλουθο διάγραμμα:

$$\begin{array}{ccc}
\mathbb{Q}(\zeta_d) & \longleftrightarrow & \{1\} \\
\Big| & & \Big| \\
\Big| \ \tau(\chi) = \pm\sqrt{d} & & \Big| \\
\mathbb{Q}(\sqrt{d}) & \longleftrightarrow & H \\
\Big| & & \Big| \\
\Big| & & \Big| \\
\mathbb{Q} & \longleftrightarrow & G = \mathrm{Gal}\left(\mathbb{Q}(\zeta_d)/\mathbb{Q}\right) \cong \mathbb{Z}_d^*
\end{array}$$

Λήμμα 2.3.6 *Έστω*

$$H_d^* \ = \ \left\{ \overline{a} \in \mathbb{Z}_d^* \ \middle| \ \chi(a) = 1 \right\}$$

και σ *ο ισομορφισμός* $\mathbb{Z}_d^* \cong G$ $\sigma(\overline{a}) \longmapsto \sigma_a$ *όπου* $\sigma_a : \zeta_d \longrightarrow \zeta_d^a$ $(\zeta_d = e^{\frac{2\pi i}{d}})$. *Τότε*

$$H \;=\; \sigma(H_d^*).$$

Απόδειξη: Επειδή $\tau(\chi) = \pm\sqrt{d}$, θα ισχύει $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\tau(\chi))$. Το $\sigma_a \in H$ ακριβώς τότε όταν $\sigma_a(\tau(\chi)) \in \mathbb{Q}(\tau(x))$ αλλά

$$\begin{aligned}\sigma_a(\tau(\chi)) &= \sigma_a\left(\sum_{z \bmod d}^{*} \chi(z)\zeta_d^z\right) = \sum_{z \bmod d}^{*} \chi(z)\zeta_d^{az} \\ &= \overline{\chi}(a) \sum_{z \bmod d}^{*} \chi(az)\zeta_d^{az} = \chi(a)\cdot\tau(\chi)\end{aligned}$$

οπότε $\sigma_a(\tau(\chi)) = \tau(\chi) \iff \chi(a) = 1$. Το $*$ στην άθροιση σημαίνει, άθροιση ως προς όλα τα $z \bmod d$ για τα οποία $(z,d) = 1$. □

Λήμμα 2.3.7 *Έστω* $N \in \mathbb{N} \setminus \{1\}$ *και* $(a,N) = (a',N) = 1$. *Ο αριθμός*

$$\frac{1-\zeta_N^a}{1-\zeta_N^{a'}}$$

είναι **μονάδα** *του κυκλοτομικού σώματος αριθμών* $\mathbb{Q}(\zeta_N)$. *Οι μονάδες αυτές λέγονται* **κυκλοτομικές**.

Απόδειξη: Επειδή $(a',N) = 1$ θα έχουμε ότι υπάρχει $x \bmod N$ τέτοιο ώστε $a'x \equiv a \pmod N$ οπότε

$$\frac{1-\zeta_N^a}{1-\zeta_N^{a'}} \;=\; \frac{1-\zeta_N^{a'x}}{1-\zeta_N^{a'}} \;=\; 1+\zeta_N^{a'}+\cdots+\zeta_N^{a'(x-1)} \;\in\; \mathbb{Z}[\zeta_N].$$

Ομοίως αποδεικνύεται ότι $\dfrac{1-\zeta_N^{a'}}{1-\zeta_N^{a}} \;\in\; \mathbb{Z}[\zeta_N]$. □

Ο τύπος για τον αριθμό κλάσεων τροποποιείται ως εξής:

$$2h_K \cdot \log\varepsilon_0 \;=\; \log\left|\frac{\displaystyle\prod_{\substack{x \bmod d \\ \chi(x)=-1}} (1-\zeta^x)}{\displaystyle\prod_{\substack{x \bmod d \\ \chi(x)=1}} (1-\zeta^x)}\right|$$

Τώρα παίρνουμε ένα x_0 τέτοιο ώστε $\chi(x_0) = -1$ και γράφουμε:

$$\begin{aligned}2h_K \cdot \log\varepsilon_0 &= \log\left|\prod_{\substack{x \bmod d \\ \chi(x)=1}} \frac{(1-\zeta^{xx_0})}{(1-\zeta^x)}\right| \;=\; \log\left|\prod_{\overline{x}\in H_d^*} \sigma_x\left(\frac{1-\zeta^{x_0}}{1-\zeta}\right)\right| \\ &= \log\left|N_{\frac{\mathbb{Q}(\zeta_d)}{\mathbb{Q}(\sqrt{d})}}\left(\frac{1-\zeta^{x_0}}{1-\zeta}\right)\right|\end{aligned}$$

Επομένως $2h_K = \dfrac{\log|E_0|}{\log(\varepsilon_0)}$ όπου $E_0 := N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}(\sqrt{d})}\left(\dfrac{1-\zeta^{x_0}}{1-\zeta}\right)$, δηλαδή αποδείξαμε το θεώρημα

Θεώρημα 2.3.8 *Αν $K = \mathbb{Q}(\sqrt{d})$ ένα πραγματικό τετραγωνικό σώμα αριθμών διακρίνουσας $d > 0$, τότε ισχύει:*

$$2h_K \ = \left[\ \langle \varepsilon_0 \rangle : \langle |E_0| \rangle\ \right] = \left[\ \langle E(K) \rangle : \langle \pm E_0 \rangle\ \right]$$

όπου E_0 όπως παραπάνω και x_0 τέτοιο ώστε $\chi(x_0) = -1$. □

Στο επόμενο κεφάλαιο θα μελετήσουμε αναλυτικά τον αριθμό κλάσεων ιδεωδών αβελιανών επεκτάσεων του $\mathbb{Q}$. Θα αποδείξουμε ότι ο h_K γράφεται σαν γινόμενο δύο φυσικών αριθμών, ο ένας από τους οποίους είναι δείκτης υποομάδας της ομάδας των μονάδων του K και ο άλλος ρητή έκφραση που μοιάζει με την περίπτωση των μιγαδικών τετραγωνικών σωμάτων αριθμών.

Κεφάλαιο 3

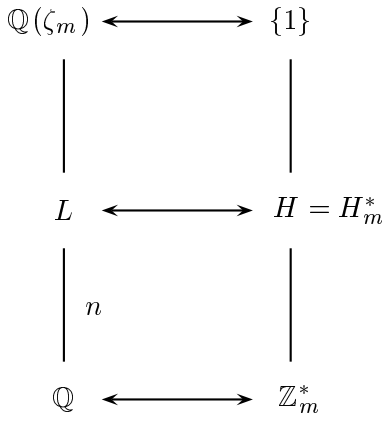
Αριθμός κλάσεων ιδεωδών αβελιανών επεκτάσεων του $\mathbb{Q}$

3.1 Η ανάλυση της ζήτα συνάρτησης αβελιανών επεκτάσεων του $\mathbb{Q}$.

Στο τρίτο κεφάλαιο θα μελετήσουμε τη ζήτα συνάρτηση αλγεβρικών σωμάτων αριθμών τα οποία είναι αβελιανές επεκτάσεις του $\mathbb{Q}$. Αν L ένα τέτοιο σώμα τότε, σύμφωνα με το γνωστό θεώρημα των Kronecker - Weber (δες [2], σελίδα 14), περιέχεται σε κάποιο κυκλοτομικό σώμα $\mathbb{Q}(\zeta_N)$ όπου ζ_N μία πρωταρχική N-ρίζα της μονάδας.

Ο ελάχιστος φυσικός αριθμός m τέτοιος ώστε $L \subseteq \mathbb{Q}(\zeta_m)$ λέγεται **οδηγός** (conductor, Führer) του σώματος L.

Ο νόμος ανάλυσης στο L (δες [2], σελίδα 184)



μας δίνει ότι για κάθε πρώτο $p \in \mathbb{P}$ τέτοιο ώστε $p \nmid m$, ο δείκτης διακλάδωσης $e := e_L(p) = e_L\left({}^{P}\!/_{p\mathbb{Z}}\right) = 1$ και ο βαθμός αδρανείας $f = f_L(p) = f_L\left({}^{P}\!/_{p\mathbb{Z}}\right) = \mathrm{ord}(\overline{p} \bmod H_m^*)$.
Ας θεωρήσουμε τώρα τη ζήτα συνάρτηση του L.

$$\zeta_L(s) \;=\; \prod_{P \in \mathbb{P}(L)} \frac{1}{1 - N(P)^{-s}}.$$

Η $N(P) = p^f$ όπου p πρώτος που ορίζεται από τη σχέση $p\mathbb{Z} = P \cap \mathbb{Z}$ και f ο βαθμός αδρανείας του p στο L, $f = f_L(p) = f_L\left(\frac{P}{p\mathbb{Z}}\right)$. Επειδή για σταθερό $p \in \mathbb{P}$, όλα τα $P \in \mathbb{P}(L)$ τέτοια ώστε $P \mid p$ έχουν τον ίδιο βαθμό αδρανείας, μπορούμε να γράψουμε

$$\begin{aligned}
\zeta_L(s) &= \prod_{p \in \mathbb{P}} \prod_{\substack{P \in \mathbb{P}(L) \\ P \mid p}} \left(1 - p^{-s f_L(p)}\right)^{-1} \\
&= \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} \prod_{\substack{P \in \mathbb{P}(L) \\ P \mid p}} \left(1 - p^{-s f_L(p)}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \nmid m}} \prod_{P \mid p} \left(1 - p^{-s f_L(p)}\right)^{-1} \\
&= \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} \prod_{P \mid p} \left(1 - p^{-s f_L(p)}\right)^{-1} \cdot \prod_{\substack{p \in \mathbb{P} \\ p \nmid m}} \left(1 - p^{-s f_L(p)}\right)^{-\frac{n}{f_L(p)}}
\end{aligned}$$

διότι $\dfrac{n}{f_L(p)}$ είναι το πλήθος των πρώτων ιδεωδών P του L τέτοιων ώστε $P \big| p$.
Τώρα παίρνουμε τον τελευταίο παράγοντα

$$\left(1 - \frac{1}{p^{s f_L(p)}}\right)^{\frac{n}{f_L(p)}} = \prod_{k=1}^{f_L(p)} \left(1 - \frac{\zeta^k}{p^s}\right)^{\frac{n}{f_L(p)}}$$

όπου $\zeta := e^{\frac{2\pi i}{f_L(p)}}$.

Η κυκλική ομάδα που παράγεται από το στοιχείο $\overline{p}\, mod\, H_m^*$ της ομάδας πηλίκων ${}^{\mathbb{Z}_m^*}\!/_{H_m^*}$ έχει τάξη $f_L(p)$ και η αντίστοιχη ομάδα χαρακτήρων είναι ισόμορφη προς αυτήν και παράγεται από τον χαρακτήρα χ για τον οποίο ισχύει $\chi\left((\overline{p}\, mod\, H_m^*)^\nu\right) = \zeta^\nu$.
Επομένως

$$\left(1 - p^{-s f_L(p)}\right)^{\frac{n}{f_L(p)}} \;=\; \prod_{\chi \in (\widehat{\langle \overline{p}\, H_m^* \rangle})} \left(1 - \frac{\chi(\overline{p} H_m^*)}{p^s}\right)^{\frac{n}{f_L(p)}}$$

Κάθε τέτοιος χαρακτήρας επεκτείνεται σε χαρακτήρες όλης της ομάδας ${}^{\mathbb{Z}_m^*}\!/_{H_m^*}$ σε πλήθος ακριβώς όσο ο δείκτης

$$\left[{}^{\mathbb{Z}_m^*}\!/_{H_m^*} \;:\; \overline{p} H_m^*\right] \;=\; \frac{\mathrm{ord}\left({}^{\mathbb{Z}_m^*}\!/_{H_m^*}\right)}{\mathrm{ord}\left(\overline{p} H_m^*\right)} \;=\; \frac{[\mathbb{Z}_m^* \;:\; H_m^*]}{f_L(p)} \;=\; \frac{n}{f_L(p)}.$$

Όλοι αυτοί οι χαρακτήρες δίνουν την ίδια τιμή στην $\overline{p}H_m^*$ δηλαδή

$$\left(1-p^{-sf_L(p)}\right)^{-\frac{n}{f_L(p)}} = \prod_{\chi\in\left(\widehat{\mathbb{Z}_m^*/H_m^*}\right)}\left(1-\chi(\overline{p}H_m^*)p^{-s}\right)$$

Έχουμε λοιπόν το

Θεώρημα 3.1.1 *Αν L αβελιανή επέκταση του $\mathbb{Q}$ με οδηγό m και H_m^* η υποομάδα της $\mathbb{Z}_m^*$ που αντιστοιχεί στο L, τότε η ζήτα συνάρτηση του σώματος L παραγοντοποιείται*

$$\zeta_L(s)=\prod_{\substack{p\in\mathbb{P}\\ p|m}}\prod_{\substack{P\in\mathbb{P}(L)\\ P|p}}\left(1-p^{-sf_L(p)}\right)^{-1}\cdot\prod_{\chi\in\left(\widehat{\mathbb{Z}_m^*/H_m^*}\right)}\left(\prod_{\substack{p\in\mathbb{P}\\ p\nmid m}}\left(1-\chi(\overline{p})p^{-s}\right)^{-1}\right)$$

όπου $\chi(\overline{p}) := \chi(\overline{p}H_m^*)$.

Το γεγονός ότι κάθε χαρακτήρας $\chi\in\widehat{\mathbb{Z}_m^*}$ επάγεται από κάποιον πρωταρχικό χαρακτήρα $\chi' \bmod \lambda$ όπου $\lambda|\varphi(m)$ και ότι αν G πεπερασμένη αβελιανή ομάδα και H υποομάδα της G, $H\leq G$, οι ακόλουθες ομάδες

$$\left\{\chi\in\widehat{G}\;\middle|\;\chi|_H=1\right\}\;\cong\;\left(\widehat{G/H}\right)$$
$$\chi\longmapsto\hat{\chi},\ \text{όπου}\ \hat{\chi}(gH)\;:=\;\chi(g)$$

είναι μεταξύ τους ισόμορφες, μας δίνει

Θεώρημα 3.1.2 *Αν L αβελιανή επέκταση του $\mathbb{Q}$ με οδηγό m και H_m^* η υποομάδα της $\mathbb{Z}_m^*$ που αντιστοιχεί στο L, τότε*

$$\zeta_L(s)\;=\;G(s)\cdot\prod_{\substack{\chi\in\widehat{\mathbb{Z}_m^*}\\ \chi|_{H_m^*}=1}}L(s/\chi')$$

όπου

$$G(s)\;:=\;\prod_{p|m}\frac{\displaystyle\prod_{\chi\in\widehat{\mathbb{Z}_m^*/H_m^*}}\left(1-\frac{\chi'(p)}{p^s}\right)}{\displaystyle\prod_{P|p}\left(1-p^{-sf_L(p)}\right)}.$$

Τώρα, όπως και στην ζήτα συνάρτηση του Riemann $\zeta(s)=\zeta_{\mathbb{Q}}(s)$ της παραγράφου 1.5 του κεφαλαίου 1, μπορούμε να αποδείξουμε τη **συναρτησιακή εξίσωση** της $\zeta_L(s)$ (δες [19], [23], [43]) και, κάνοντας χρήση αυτής, μπορούμε να δούμε ότι

Θεώρημα 3.1.3 $G(s) = 1$

Χωρίς απόδειξη. (Δες [42], σελίδα 371 ή [43], σελίδα 427.)

Ας δούμε δύο ειδικές περιπτώσεις του θεωρήματος 3.1.3

1. Αν $m = p$ ο μόνος διακλαδιζόμενος πρώτος στο $\mathbb{Q}(\zeta_p)$ είναι ο p, $pR = P^{p-1}$ όπου $P = \langle 1-\zeta_p \rangle$. Κάθε χαρακτήρας $\chi \neq \chi_0$ είναι πρωταρχικός, δηλαδή $\chi = \chi'$ και $\chi'(p) = 0$, άρα

$$G(s) \;=\; \frac{1-\dfrac{1}{p^s}}{1-\dfrac{1}{p^s}} \;=\; 1.$$

2. Αν L τετραγωνικό σώμα αριθμών τότε έχουμε ήδη δείξει ότι

$$\zeta_L(s) \;=\; \zeta_{\mathbb{Q}}(s) \cdot L(s/\chi).$$

Επομένως έχουμε το παρακάτω θεώρημα:

Θεώρημα 3.1.4 (κύριο θεώρημα της παραγράφου)
Έστω L μία αβελιανή επέκταση του $\mathbb{Q}$ με οδηγό m, $L \subseteq \mathbb{Q}(\zeta_m)$ και H_m^* η υποομάδα της $\mathbb{Z}_m^*$ που αντιστοιχεί στο L. Τότε έχουμε

$$\zeta_L(s) \;=\; \prod_{\substack{\chi \in \widehat{\mathbb{Z}_m^*} \\ \chi|_{H_m^*}=1}} L(s/\chi') \;=\; \zeta_{\mathbb{Q}}(s) \cdot \prod_{\substack{\chi \in \widehat{\mathbb{Z}_m^*} \\ \chi|_{H_m^*}=1,\, \chi \neq \chi_0}} L(s/\chi')$$

όπου ο χ επάγεται από τον πρωταρχικό χαρακτήρα χ'.

Θεώρημα 3.1.5 (τύπος αριθμού κλάσεων)
Αν το σώμα L είναι όπως στο Θεώρημα 3.1.4, ο αριθμός κλάσεων αυτού $h_{_L}$ δίνεται από τη σχέση:

$$h_L \;=\; \frac{w\sqrt{|D_K|}}{2^{s+t}\pi^t Reg_L} \cdot \prod_{\substack{\chi \neq \chi_0 \\ \chi|_{H_m^*}=1}} L(1/\chi')$$

Απόδειξη: Από το Θεώρημα 3.1.4 έπεται ότι το υπόλοιπο

$$Res\zeta_L(s)_{s=1} \;=\; \prod_{\substack{\chi \neq \chi_0 \\ \chi|_{H_m^*}=1}} L(1/\chi')$$

Στη συνέχεια εφαρμόζουμε το Θεμελιώδες Θεώρημα 2.2.2. □

3.2 Ο αριθμός κλάσεων του $L = \mathbb{Q}(\zeta_p)$, $p \in \mathbb{P}$, $p \neq 2$

Υπενθυμίζουμε ότι ο δακτύλιος των ακεραίων αλγεβρικών του L είναι $R = \mathbb{Z}[\zeta_p]$, μία βάση ακεραιότητας είναι το σύνολο $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ και η διακρίνουσα του L είναι $(-1)^{\frac{p-1}{2}} p^{p-2}$, $w = 2p$ και $pR = P^{p-1}$, όπου $P = \langle 1 - \zeta_p \rangle$, οπότε το θεώρημα 3.1.5 δίνει

$$h_L = \frac{2p \cdot p^{\frac{p-2}{2}}}{2^{\frac{p-1}{2}} \pi^{\frac{p-1}{2}} \mathrm{Reg}_L} \prod_{\substack{\chi \in \widehat{\mathbb{Z}_p^*} \\ \chi \neq \chi_0}} L(1/\chi').$$

Τώρα γνωρίζουμε ότι

$$\tau(\chi) = \begin{cases} \sqrt{p}, & \text{αν } \chi(-1) = 1 \\ i\sqrt{p}, & \text{αν } \chi(-1) = -1, \end{cases}$$

το οποίο, σε συνδυασμό με το θεώρημα (2.2.4), μας δίνει τη σχέση

$$\prod_{\substack{\chi \in \widehat{\mathbb{Z}_m^*} \\ \chi \neq \chi_0}} L(1/\chi') \;=\; \pm \frac{\pi^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}}} \prod_{\chi \neq \chi_0} S(\chi)$$

όπου

$$S(\chi) \;=\; \begin{cases} \displaystyle\sum_{0<x<p} \overline{\chi}(x) \log|1 - \zeta^x|, & \text{αν } \chi \text{ άρτιος} \\ \frac{1}{p} \sum_{0<x<p} \overline{\chi}(x)\, x, & \text{αν } \chi \text{ περιττός} \end{cases}$$

Εδώ χρησιμοποιήσαμε και το γεγονός ότι:

Πρόταση 3.2.1 *Υπάρχουν ακριβώς* $\dfrac{p-1}{2}$ *άρτιοι χαρακτήρες και* $\dfrac{p-1}{2}$ *περιττοί.*

Απόδειξη: Έστω

$$\widehat{\mathbb{Z}_p^*}^+ \;:=\; \{\chi \in \widehat{\mathbb{Z}_p^*} \;\mid\; \chi \text{ άρτιος}\}.$$

Αν χ^* οποιοσδήποτε περιττός χαρακτήρας της $\mathbb{Z}_p^*$, τότε προφανώς

$$\widehat{\mathbb{Z}_p^*} \;=\; \widehat{\mathbb{Z}_p^*}^+ \;\dot{\bigcup}\; \chi^* \widehat{\mathbb{Z}_p^*}^+$$

οπότε κάθε πλευρική κλάση θα έχει το ίδιο πλήθος χαρακτήρων $\dfrac{p-1}{2}$. Αρκεί λοιπόν να αποδείξουμε ότι υπάρχει πάντοτε τουλάχιστο ένας περιττός χαρακτήρας χ^* της $\mathbb{Z}_p^+$.
Αν δεν υπήρχε, τότε για κάθε χαρακτήρα χ της $\mathbb{Z}_p^*$ θα είχαμε

$$\chi(-1) \;=\; 1,$$

δηλαδή όλοι οι χαρακτήρες θα ήταν άρτιοι, άρα

$$\#\widehat{\mathbb{Z}_p^*} = \#\left(\widehat{\frac{\mathbb{Z}_p^*}{\{\pm 1\}}}\right) \Rightarrow p-1 = \frac{p-1}{2}$$

Συνεπώς καταλήξαμε σε άτοπο. □

Ας παρατηρήσουμε ακόμα ότι

1. Το γινόμενο $\prod L(1/\chi')$ είναι **πραγματικό** (από τον τύπο του αριθμού κλάσεων) και
2. $S(\overline{\chi}) = \overline{S(\chi)}$

Τελικά έχουμε

Πρόταση 3.2.2

$$2^{\frac{p-3}{2}} \cdot Reg_L \cdot h_L \;=\; \pm p \cdot \prod_{\substack{\chi \in \widehat{\mathbb{Z}_p^*} \\ \chi \neq \chi_0}} S(\chi)$$

όπου

$$S(\chi) \;=\; \begin{cases} \displaystyle\sum_{0<x<p} \overline{\chi}(x) \log\left|1-\zeta^x\right|, & \text{αν } \chi \text{ άρτιος} \\ \displaystyle\frac{1}{p} \sum_{0<x<p} \overline{\chi}(x)\, x, & \text{αν } \chi \text{ περιττός} \end{cases}$$

Στη συνέχεια θα γράψουμε τον h_L σαν γινόμενο

$$h_L \;=\; h_0 h^*$$

όπου

$$h_0 \;:=\; \frac{1}{\mathrm{Reg}_L} \left| \prod_{\substack{\chi \neq \chi_0 \\ \chi \text{ άρτιος}}} S(\chi) \right|$$

και

$$h^* \;:=\; \frac{p}{2^{\frac{p-3}{2}}} \left| \prod_{\chi \text{ περιττός}} S(\chi) \right|.$$

(Εννοείται ότι πάντοτε τα χ είναι χαρακτήρες της $\mathbb{Z}_p^*$. Σύντομα θα αλλάξουμε το συμβολισμό μας σε $h^* = h_1$ και $h_0 = h_2$ και θα τους ονομάζουμε **ο πρώτος** και **ο δεύτερος παράγοντας του αριθμού κλάσεων** αντιστοίχως.)

Θεώρημα 3.2.3 *Ο h_0 είναι ίσος προς τον δείκτη $(E : E_0)$ όπου E η υποομάδα όλων των* **πραγματικών θετικών μονάδων** *του L και E_0 η ομάδα που παράγεται από τις* **κυκλοτομικές μονάδες**

$$\Theta_k = \frac{\zeta^k - \zeta^{-k}}{\zeta - \zeta^{-1}}, \quad \gamma\iota\alpha\, k = 2, \dots, \frac{p-1}{2}$$

$$h_0 \;=\; (\,E \,:\, E_0\,).$$

Θεώρημα 3.2.4 *Ο h^* είναι φυσικός αριθμός.*

Παρατήρηση 3.2.5 *Ο h_0 είναι ο αριθμός κλάσεων του μεγίστου πραγματικού υποσώματος $L_0 = \mathbb{Q}(\zeta_p) \cap \mathbb{R}$ του L, $h_0 = h_{L_0}$.*

Απόδειξη: (Του θεωρήματος 3.2.3)
Κατ' αρχήν αποδεικνύουμε το λήμμα.

Λήμμα 3.2.6 *Αν $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ είναι ανεξάρτητες μονάδες του αλγεβρικού σώματος αριθμών L οι οποίες παράγουν μία υποομάδα A της $E(R)$ modulo ρίζες της μονάδας και $\xi_1, \xi_2, \dots, \xi_r$ είναι επίσης ανεξάρτητες μονάδες του L οι οποίες παράγουν μία υποομάδα B, τότε αν $A \subseteq B$ και ο δείκτης της υποομάδας A στην ομάδα B είναι πεπερασμένος, θα έχουμε*

$$[\,B \,:\, A\,] \;=\; \frac{R_L\,(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r)}{R_L\,(\xi_1, \xi_2, \dots, \xi_r)}.$$

Απόδειξη: Γράφουμε

$$\varepsilon_i = \prod_{\ell} n_{i\ell}^{a_{i\ell}} \cdot (\text{ρίζες της μονάδος}) \quad \mu\varepsilon \quad a_{i\ell} \in \mathbb{Z}.$$

Συνεπώς

$$e_j \log\bigl|\sigma_j(\varepsilon_i)\bigr| \;=\; \sum_{\ell} a_{i\ell} e_j \log\bigl|\sigma_j(\xi_\ell)\bigr|$$

(όπου $e_j = 1$ ή 2 ανάλογα με την εμφύτευση). Άρα

$$R_L(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r) \;=\; \bigl|\det(a_{i\ell})\bigr| \cdot \bigl|R_L(\xi_1, \xi_2, \dots, \xi_r)\bigr|.$$

Είναι γνωστό όμως ότι (δες [2], σελίδα 85)

$$[\,B \,:\, A\,] \;=\; \bigl|\det(a_{i\ell})\bigr|$$

και συνεπώς έχουμε το ζητούμενο. □

Λήμμα 3.2.7 *Για* $L = \mathbb{Q}(\zeta_p)$, $p \in \mathbb{P}\,(p \neq 2)$ *κάθε σύστημα θεμελιωδών μονάδων του* $L^+ = L \cap \mathbb{R}$ *είναι σύστημα θεμελιωδών μονάδων και του* L, *και μάλιστα*

$$E(R_L) \;=\; W \cdot E(R_{L^+})$$

Απόδειξη: Αρκεί να αποδείξουμε ότι κάθε μονάδα ε του L γράφεται

$$\varepsilon = \mu\varepsilon' \qquad \text{όπου} \quad \left| \begin{array}{l} \mu \text{ είναι ρίζα της μονάδας} \\ \varepsilon' \text{ είναι μονάδα του } L^+ \end{array} \right.$$

Αν το αποδείξουμε τότε θα έχουμε τελειώσει διότι κάθε θεμελιώδης μονάδα παραμένει θεμελιώδης αν πολλαπλασιαστεί με ρίζα της μονάδας. Έστω

$$\mu := \frac{\varepsilon}{\overline{\varepsilon}} \;=\; \frac{\varepsilon}{\sigma_{-1}(\varepsilon)}$$

Το μ είναι ρίζα της μονάδας. Αρκεί να δείξουμε ότι όλοι οι συζυγείς του έχουν μέτρο 1.

$$\sigma_\chi(\mu) \;=\; \sigma_\chi(\varepsilon)\frac{1}{\sigma_\chi\sigma_{-1}(\varepsilon)} \;=\; \frac{\sigma_\chi(\varepsilon)}{\sigma_{-1}(\sigma_\chi(\varepsilon))} \;=\; \frac{\sigma_\chi(\varepsilon)}{\overline{\sigma_\chi(\varepsilon)}}.$$

Συνεπώς

$$\big|\sigma_\chi(\mu)\big| = 1 \quad \forall \chi \in \mathbb{Z}_p^*.$$

Επομένως

$$\frac{\varepsilon^2}{\varepsilon\overline{\varepsilon}} = \mu = \pm\zeta_p^\nu,\ \nu \in \mathbb{Z} \quad \Longrightarrow \quad \varepsilon^2 = \pm\zeta_p^\nu|\varepsilon|^2.$$

Ισχυρίζομαι ότι το σωστό πρόσημο είναι το θετικό. Αν το δεχθούμε αυτό τότε έχουμε τελειώσει, διότι

$$\begin{aligned} \varepsilon^2 \;&=\; \zeta_p^{2\nu'} \cdot |\varepsilon|^2, \quad \text{διότι } 2 \nmid p \\ \Longrightarrow \quad \varepsilon \;&=\; \pm\zeta_p^{\nu'} \cdot |\varepsilon|, \quad \text{και } \varepsilon \text{ μονάδα του } L^+. \end{aligned}$$

Έστω ότι το πρόσημο είναι αρνητικό, δηλαδή

$$\varepsilon^2 = -\zeta_p^\nu|\varepsilon|^2 \quad \Longrightarrow \quad \varepsilon = -\zeta_p^\nu \cdot \overline{\varepsilon}.$$

Τώρα

$$\varepsilon \;=\; a_0 + a_1(1-\zeta_p) + \ldots + a_{p-2}(1-\zeta_p)^{p-2}$$

$$p \simeq P^{p-1}, \quad P = \langle 1 - \zeta_p^{\nu} \rangle, \quad p \nmid \nu$$

$$\overline{\varepsilon} \;=\; a_0 + a_1(1-\zeta_p^{-1}) + \ldots + a_{p-2}(1-\zeta_p^{-1})^{p-2}$$

$$\Longrightarrow \quad \varepsilon \equiv \overline{\varepsilon_0} \equiv a_0 \bmod P.$$

Επομένως

$$\varepsilon(1+\zeta_p^{\nu}) \equiv 0 \bmod P \quad \text{και} \quad \varepsilon \text{ μονάδα},$$

δηλαδή

$$1 + \zeta_p^{\nu} \equiv 0 \bmod P.$$

Αλλά και

$$1 - \zeta_p^{\nu} \equiv 0 \bmod P$$

Συνεπώς

$$2 \equiv 0 \bmod P \quad \Longrightarrow \quad 2 \in P \quad \Longrightarrow \quad p = 2,$$

άρα φτάσαμε σε άτοπο διότι $p \neq 2$. □

Με τ θα συμβολίζουμε τον $\mathbb{Q}$-αυτομορφισμό του L ο οποίος στέλνει κάθε στοιχείο του L στο συζυγές του. Η ομάδα του Galois

$$\mathrm{Gal}\left(L\diagup\mathbb{Q}\right) = \{\mathrm{Id}, \tau\} \dot{\bigcup} \left(\bigcup_{x=2}^{\frac{p-1}{2}} \{\sigma_x, \sigma_{-x}\} \right).$$

Ο $\mathrm{rank}\, E(R_L) = \dfrac{p-1}{2}$.

Για να σχηματίσουμε τον Reg_L διαλέγουμε τους $\{\sigma_x\}_{x=2,3,\ldots,\frac{p-1}{2}}$

Επομένως

$$\mathrm{Reg}_L\left(\Theta_2, \Theta_3, \ldots, \Theta_{\frac{p-1}{2}}\right) \;=\; \left|\det\left(\log|\sigma_x(\Theta_k)|^2\right)\right|_{x,k=2,\ldots,\frac{p-1}{2}}$$

$$\log|\sigma_x(\Theta_k)|^2 = \xi_{kx} - \xi_x$$

όπου

$$\xi_y := \log|\zeta^y - \zeta^{-y}|^2.$$

Τώρα θα χρησιμοποιήσουμε το ακόλουθο

Λήμμα 3.2.8 *Έστω G πεπερασμένη αβελιανή ομάδα, $U \leq G$ και έστω $\xi : G \to \mathbb{R}$ μία συνάρτηση με τις παρακάτω ιδιότητες:*

1. *$\xi_g := \xi(g)$ εξαρτάται μόνο από την πλευρική κλάση gU.*

2. *$\forall g \in G : \sum_{h \bmod U} (\xi_{gh} - \xi_h) = 0.$*

Τότε ισχύει

$$\left|\det(\xi_{gh} - \xi_h)_{\substack{g,h \bmod U \\ g,h \notin U}}\right| = \left|\prod_{\substack{\chi \in \left(\widehat{G/U}\right) \\ \chi \neq \chi_0}} \left(\sum_{g \bmod U} \overline{\chi}(g)\xi_g\right)\right|.$$

Προτού αποδείξουμε το λήμμα, ας το εφαρμόσουμε τώρα για $G = \mathbb{Z}_p^*$ και $U = \{\pm 1\}$, οπότε έχουμε

$$\left(\widehat{G/U}\right) = \left\{\chi \in \widehat{\mathbb{Z}_p^*} \;\middle|\; \chi \text{ άρτιος}\right\}$$

και

$$\xi_x := \log\left|\zeta^x - \zeta^{-x}\right|^2.$$

Οι απαιτήσεις (1) και (2) του λήμματος 3.2.8 ισχύουν στην περίπτωση μας. Πράγματι η (1) ισχύει λόγω της απόλυτης τιμής στον ορισμό ξ_x. Για την (2) έχουμε

$$\begin{aligned}
\sum_{x \bmod \{\pm\overline{1}\}} (\xi_{yx} - \xi_x) &= \sum_{x \bmod \{\pm\overline{1}\}} \left(\log\left|(\zeta^{yx} - \zeta^{-yx}\right|^2 - \log\left|(\zeta^x - \zeta^{-x}\right|^2\right) \\
&= \sum_{x \bmod \{\pm\overline{1}\}} 2\log\left(\left|(\zeta^{yx} - \zeta^{-yx}\right| \frac{1}{\left|(\zeta^x - \zeta^{-x}\right|}\right) \\
&= 2\log\left|\prod_{x \bmod \{\pm\overline{1}\}} \frac{\zeta^{yx} - \zeta^{-yx}}{\zeta^x - \zeta^{-x}}\right| = 2\log\left|\prod_{x \bmod \{\pm\overline{1}\}} \sigma_x \frac{\zeta^y - \zeta^{-y}}{\zeta - \zeta^{-1}}\right| \\
&= 2\log\left|N_{L^+/\mathbb{Q}}(\theta_y)\right| = 2\log 1 = 0.
\end{aligned}$$

Επομένως το λήμμα 3.2.8 δίνει:

$$\begin{aligned}
\mathrm{Reg}_L(\Theta_2,\Theta_3,\ldots,\Theta_{\frac{p-1}{2}}) &= \left|\det\left(\xi_{xy}-\xi_x\right)_{\substack{x,y\in\mathbb{Z}_p^*\\ \bmod\{\pm\overline{1}\}\\ x,y\notin\{\pm\overline{1}\}}}\right| \\
&= \left|\prod_{\substack{\chi\in\widehat{\mathbb{Z}_p^*}\\ \chi(-1)=\overline{1}\\ \chi\neq\chi_0}}\left(\sum_{x\bmod\{\pm\overline{1}\}}\overline{\chi}(x)\log|\zeta^x-\zeta^{-x}|^2\right)\right| \\
&= \left|\prod_{\substack{\chi\ \text{άρτιος}\\ \chi\neq\chi_0}} S(\chi)\right|
\end{aligned}$$

διότι

$$\begin{aligned}
\sum_{\substack{x\in\mathbb{Z}_p^*\\ x\bmod\{\pm\overline{1}\}}}\overline{\chi}(x)\log|\zeta^x-\zeta^{-x}|^2 &= \sum_{x\in\mathbb{Z}_p^*}\overline{\chi}(x)\log|\zeta^x(1-\zeta^{-2x})| \\
&= \chi(2)\sum_{y\in\mathbb{Z}_p^*}\overline{\chi}(y)\log\left|1-\zeta^{-y}\right)|
\end{aligned}$$

Επομένως, λόγω του ορισμού του h_0 στη σελίδα 72, έχουμε

$$\begin{aligned}
h_0 &= \frac{\mathrm{Reg}_L(\Theta_2,\Theta_3,\ldots,\Theta_{\frac{p-1}{2}})}{\mathrm{Reg}_L} \\
&\overset{(\lambda.\ 3.2.6)}{=} \left[L(E(R_L))\ :\ L(\Theta_2,\Theta_3,\ldots,\Theta_{\frac{p-1}{2}})\right] \\
&= \left[E(R_L)\ :\ \langle\Theta_2,\Theta_3,\ldots,\Theta_{\frac{p-1}{2}}\rangle\cdot W\right].
\end{aligned}$$

Απο το λήμμα 3.2.7 έχουμε ότι $E(R_L)=E\cdot W$ οπότε

$$h_0=\left[E\ :\ \langle\Theta_2,\Theta_3,\ldots,\Theta_{\frac{p-1}{2}}\rangle\right].$$

Απόδειξη: (Του λήμματος 3.2.8).

Έστω

$$\begin{aligned}
A &= \left(\xi_{gh}-\xi_h\right)_{\substack{g,h\bmod U\\ g,h\notin U}} \\
B &= \left(\chi(g)\right)_{\substack{\chi\in(\widehat{G/U})-\{\chi_0\}\\ g\bmod U\ g\notin U}}
\end{aligned}$$

$BA = \big(\gamma_{\chi,h}\big)_{\chi,h}$ με $\gamma_{\chi,h} = \displaystyle\sum_{\substack{g \bmod U \\ g \notin U}} \chi(g)(\xi_{gh} - \xi_h)$

$$\begin{aligned}\gamma_{\chi,h} &= \sum_{g \bmod U} \chi(g)(\xi_{gh} - \xi_h) \\ &= \sum_{g \bmod U} \chi(g)\xi_{gh} - \xi_h \sum_{g \bmod U} \chi(g) \\ &= \sum_{g \bmod U} \chi(g)\xi_{gh} = \overline{\chi}(h) \sum_{g' \bmod U} \chi(g')\xi_{g'}\end{aligned}$$

Επομένως

$$\begin{aligned}\det(B \cdot A) &= \pm \Big(\prod_{\chi \neq \chi_0} \Big(\sum_{g \bmod U} \chi(g)\xi_g \Big) \Big) \det\left(\overline{\chi}(h)\right) \\ \Longrightarrow \big|\det B\big| \cdot \big|\det A\big| &= \left| \prod_{\chi = \chi_0} \Big(\sum_{g \bmod U} \chi(g)\xi_g \Big) \right| \cdot \big|\det\left(\overline{B}\right)\big|.\end{aligned}$$

Επειδή $\big|\det B\big| = \big|\det \overline{B}\big|$, αν δείξουμε ότι $\det B \neq 0$, θα έχουμε τελειώσει. Προς τούτο παίρνουμε

$$\det(B\,\overline{B}^{\top}) = \det(\delta_{\chi\psi})$$

όπου

$$\begin{aligned}\delta_{\chi\psi} &= \sum_{\substack{g \bmod U \\ g \notin U}} \chi(g)\overline{\psi}(g) = \left(\sum_{g \bmod U} \left(\chi\psi^{-1}\right)(g) \right) - 1 \\ &= \begin{cases} [\,G : U\,] - 1, & \text{αν } \chi = \psi \\ -1, & \text{αν } \chi \neq \psi. \end{cases}\end{aligned}$$

Επομένως για $u = [\,G : U\,]$ έχουμε

$$\det(B\overline{B}^{\top}) = \begin{bmatrix} u-1 & -1 & \dots & \dots & -1 \\ -1 & u-1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ -1 & -1 & \dots & -1 & u-1 \end{bmatrix} = u^{u-2} \neq 0.$$

□

Απόδειξη του θεωρήματος 3.2.4:

$$h^* = \frac{p}{2^{\frac{p-3}{2}}} \left| \prod_{\chi \text{ περιττός}} S(\chi) \right| \quad \text{όπου} \quad S(\chi) = \frac{1}{p} \sum_{0<x<p} \chi(x)x.$$

$\mathbb{Z}_p^*$ είναι κυκλική τάξης $p-1 = \langle \overline{g} \rangle$ με $\text{ord}(\overline{g}) = p-1$. Ομοίως $\widehat{\mathbb{Z}_p^*} = \langle \psi_0 \rangle$ με $\text{ord}(\psi_0) = p-1$ όπου $\xi := \psi_0(\overline{g})$ είναι πρωταρχική $(p-1)$-ρίζα της μονάδας. Προφανώς

1. ψ_0 είναι περιττός.
2. Ο χ είναι περιττός ακριβώς τότε όταν $\chi = \psi_0^k$ και $2 \nmid k$.

Ορισμός 3.2.9

1. $g_s := \min(\overline{g}^s \cap \mathbb{N})$
2. $F(x) := \sum_{s=0}^{p-2} g_s x^s$

Παρατήρηση:

$$h^* = \frac{1}{(2p)^{\frac{p-3}{2}}} \prod_{\substack{k=1 \\ 2 \nmid k}}^{p-2} F(\xi^k)$$

Απόδειξη: Κατ' αρχήν ο χ είναι περιττός αν και μόνο αν

$$\chi = \psi_0^k \quad \text{για} \quad 1 \leq k \leq p-2, \;\; 2 \nmid k,$$

οπότε

$$\begin{aligned} S(\chi) &= \frac{1}{p} \sum_{0<x<p} \chi(x)x = \frac{1}{p} \sum_{s=0}^{p-2} \chi(g^s) g_s \\ &= \frac{1}{p} \sum_{s=0}^{p-2} g_s \xi^{ks} = \frac{1}{p} F(\xi^k). \end{aligned}$$

Τελειώνοντας έχουμε ότι το πλήθος των παραγόντων είναι $\frac{p-1}{2}$. □

Λήμμα 3.2.10

$$2^{\frac{p-3}{2}} \;\Big|\; \prod_{\substack{k=1 \\ 2 \nmid k}}^{p-2} F(\xi^k).$$

Απόδειξη: $m = \frac{p-1}{2}$. Άρα $g^m \equiv -1 \,(\mathrm{mod}\, p)$ και $\xi^m = -1$. Ισχυρίζομαι ότι

$$g_{m+s} \not\equiv g_s \,(\mathrm{mod}\, 2), \quad \text{για } s = 0, \ldots, m-1. \tag{3.1}$$

Πράγματι

$$\begin{aligned} g_{m+s} + g_s \equiv g^{m+s} + g^s \equiv g^s(g^m+1) \equiv 0 (\mathrm{mod}\, p) \\ \Longrightarrow\ g_{m+s} + g_s = \nu p \implies g_{m+s} + g_s = p \\ \Rightarrow\ g_{m+s} + g_s \not\equiv 0 (\mathrm{mod}\, 2) \end{aligned}$$

δηλαδή η (3.1) ισχύει. Έστω τώρα $k \not\equiv 0 \,(\mathrm{mod}\, 2)$.

$$\begin{aligned} F(\xi^k) &= \sum_{s=0}^{p-2} g_s \xi^{ks} = \sum_{s=0}^{m-1} \left(g_s \xi^{ks} + g_{m+s} \xi^{k(m+s)} \right) \\ &= \sum_{s=0}^{m-1} (g_s - g_{m+s})\, \xi^{ks} \end{aligned} \tag{3.2}$$

και επειδή $g_{m+s} - g_s \equiv 1 \,(\mathrm{mod}\, 2)$, το δεξί μέλος της (3.2) είναι ισοδύναμο με

$$\sum_{s=0}^{m-1} \xi^{ks} \,(\mathrm{mod}\, 2)$$

όπου η ισοδυναμία εννοείται στον $\mathbb{Z}[\zeta_p]$. Από την άλλη μεριά

$$\sum_{s=0}^{m-1} \xi^{ks} = \frac{1-\xi^{mk}}{1-\xi^k} = \frac{2}{1-\xi^k}.$$

Επομένως

$$\begin{aligned} & F(\xi^k)(1-\xi^k) \equiv 0 \,(\mathrm{mod}\, 2) \\ \Longrightarrow\ & \prod_{\substack{k=1 \\ 2 \nmid k}}^{p-2} F(\xi^k)(1-\xi^k) \equiv 0 \,(\mathrm{mod}\, 2^{\frac{p-1}{2}}). \end{aligned}$$

Τώρα $\prod\limits_{\substack{k=1 \\ 2 \nmid k}}^{p-2} (1-\xi^k) = 2$. Πράγματι

$$\begin{aligned} \prod_{k=1}^{p-2} (1-\xi^k) &= \left. \frac{x^{p-1}-1}{x-1} \right|_{x=1} = p-1 \quad \text{και} \\ \prod_{\substack{k=1 \\ 2|k}}^{p-2} (1-\xi^k) &= \left. \prod_{\nu=1}^{\frac{p-3}{2}} (1-\xi^{2\nu}) \right|_{x=1} = \frac{p-1}{2}. \end{aligned}$$

Συνεπώς αποδείξαμε τον ισχυρισμό του λήμματος 3.2.10. □

Λήμμα 3.2.11

$$p^{\frac{p-3}{2}} \;\Big|\; \prod_{\substack{k=1\\ 2\nmid k}}^{p-2} F(\xi)$$

Απόδειξη:

$$F(x) \;\equiv\; \sum_{s=0}^{p-2}(gx)^s \;(\mathrm{mod}\, p),$$

όπου $\displaystyle\sum_{s=0}^{p-2}(gx)^s = \frac{1-(gx)^{p-1}}{1-gx}$. Άρα

$$F(x)(1-gx) \;\equiv\; 1-(gx)^{p-1} \;\equiv\; 1-x^{p-1}\,(\mathrm{mod}\, p)$$

και επομένως

(1) $F(\xi)(1-g\xi^k) \equiv 0 \bmod p\,\mathbb{Z}[\zeta_p]$.

Τώρα θα μελετήσουμε τους παράγοντες του $1-g\xi^k$. Υπενθυμίζουμε την

(2) ανάλυση του p στο $\mathbb{Q}(\xi) = \mathbb{Q}(e^{\frac{2\pi i}{p-1}})$. Αφού $p \equiv 1\,(\mathrm{mod}\,(p-1))$ συνεπάγεται ότι ο p αναλύεται πλήρως στο $\mathbb{Q}(\xi)$, άρα

$$pR = \prod_{\substack{k \bmod (p-1)\\ (k,p-1)=1}} \sigma_k(P), \quad \sigma_k \,:\, \xi \longrightarrow \xi^k$$

όπου P κάποιο πρώτο ιδεώδες του $\mathbb{Q}(\zeta)$, $P\big|p$ και $\sigma_k(P)$ όλα μεταξύ τους ανα δύο διαφορετικά. Ας συμβολίσουμε $P_k := \sigma_k(P)$ για $(k, p-1) = 1$.

(3) Ισχυρίζομαι τώρα ότι:

(α'). $P\big|\langle 1-g\xi\rangle = (1-g\xi)R$ με κάποιο κατάλληλα εκλεγμένο P, $P\big|p$.

(β'). $P_k\big|\langle 1-g\xi^k\rangle$ για $(k, p-1) = 1$.

(γ'). Αν $(k, p-1) \neq 1$ τότε για κάθε k' με $(k', p-1) = 1$ έχουμε $P_{k'} \nmid \langle 1-g\xi^k\rangle$.

(δ'). Τα $\langle 1-g\xi^k\rangle$, $k\,(\mathrm{mod}\,(p-1))$ είναι ανά δύο *όχι* ισοδύναμα $\bmod P'$ για όλα τα ιδεώδη $P'\big|p$.

Απόδειξη: Για το (γ') έχουμε: $(k, p-1) = d > 1$, συνεπώς $\xi^{k\frac{p-1}{d}} = 1$. Έστω ότι

$$\begin{aligned} P'\big|1-g\xi^k \;&\Longrightarrow\; g\xi^k \equiv 1\,(\mathrm{mod}\, P')\\ &\Longrightarrow\; g^{\frac{p-1}{d}}\xi^{k\frac{p-1}{d}} \equiv 1\,(\mathrm{mod}\, P')\\ &\Longrightarrow\; g^{\frac{p-1}{d}} \equiv 1\,(\mathrm{mod}\, P'). \end{aligned}$$

Επειδή $g \in \mathbb{Z}$ και $d \big| p-1$, έπεται ότι $g^{\frac{p-1}{d}} \in \mathbb{Z}$. Επομένως $g^{\frac{p-1}{d}} \in P' \cap \mathbb{Z} = p\mathbb{Z}$, άρα

$$g^{\frac{p-1}{d}} \equiv 1 \,(\mathrm{mod}\, p) \implies p-1 \Big| \frac{p-1}{d} \implies d = 1.$$

Συνεπώς καταλήξαμε σε άτοπο.

Για την απόδειξη του (α′) έχουμε:

$$\prod_{k \bmod (p-1)} (1 - g\xi^k) \;=\; (1 - g^{p-1}) \;\in\; p\,\mathbb{Z}[\xi]$$
$$\implies \prod_{k \bmod (p-1)} (1 - g\xi^k) \;\in\; p\,\mathbb{Z}[\xi] \;\subseteq\; P.$$

Υπάρχει λοιπόν k με $\langle 1 - g\xi^k \rangle \subseteq P$, $(k, p-1) = 1$, άρα υπάρχει k, $(k, p-1) = 1$, τέτοιο ώστε $P \big| 1 - g\xi^k$.

Για την απόδειξη του (δ′) έχουμε:

Έστω $1 - g\xi^k \equiv 1 - g\xi^{k'} \,(\mathrm{mod}\, P')$ για κάποιο $P' \big| p$. Άρα $g\xi^k \equiv g\xi^{k'} \,(\mathrm{mod}\, P')$ και αφού $g \notin P'$, $\xi^k \equiv \xi^{k'} \,(\mathrm{mod}\, P')$. Αν $k \not\equiv k' \,(\mathrm{mod}\, p-1)$ τότε

$$P' \big| 1 - \xi^{k-k'} \Big| \prod_{\nu=1}^{p-2} (1 - \xi^\nu) \;=\; \frac{x^{p-1} - 1}{x - 1}\Big|_{x=1} \;=\; p - 1$$

το οποίο όμως είναι άτοπο. □

Από τα παραπάνω συνάγουμε ότι $\xi^k = \xi^{k'}$ οπότε υπάρχει ακριβώς ένα P, $P \big| p$, τέτοιο ώστε $P \big| \langle 1 - g\xi \rangle$ και επομένως

$$P_k = \sigma_k(P) \;\big|\; \sigma_k(1 - g\xi) \;=\; (1 - g\xi^k),$$

δηλαδή το (β′).

Από (1) και (3) έχουμε:

$$(4) \begin{cases} F(\xi^k) \equiv 0 \,(\mathrm{mod}\, p), & \text{για } (k, p-1) \neq 1 \\ F(\xi^k) \equiv 0 \,(\mathrm{mod}\, p/P_k), & \text{για } (k, p-1) = 1 \end{cases}$$

Από (2) έχουμε ότι $p\mathbb{Z}[\zeta] = \prod_{\substack{k \bmod (p-1) \\ (k,p-1)=1}} P_k$. Επομένως

$$\prod_{\substack{k=1 \\ 2 \nmid k}}^{p-2} F(\xi^k) \equiv 0 \bmod \frac{p^{\frac{p-1}{2}}}{\prod_{\substack{k \bmod (p-1) \\ (k,p-1)=1}} P_k} \;=\; p^{\frac{p-3}{2}}.$$

Αποδείξαμε και το λήμμα 3.2.11. □

Από τα λήμματα 3.2.10 και 3.2.11 έπεται η αλήθεια του θεωρήματος 3.2.4. □

Τώρα θα εξετάσουμε συνθήκες κάτω από τις οποίες $p \mid h^*$.

Θεωρούμε το κύριο ιδεώδες που παράγεται από τον αριθμό h^* στο $\mathbb{Q}(\xi)$.

$$\left(2^{\frac{p-3}{2}}h^*\right)=\prod_{\substack{k=1\\ 2\nmid k}}^{p-2}\frac{F(\xi^k)P_k}{p} \tag{3.3}$$

όπου

$$P_k \;=\; \begin{cases}\sigma_k(P), & \text{αν}\;\; (k,p-1)=1\\ (1), & \text{αν}\;\; (k,p-1)\neq 1\end{cases}$$

Προφανώς αν $p|h^*$ τότε $h^*\in P_k\;\;\forall k,\;1\leq k\leq p-2,\;(k,p-2)=1$ διότι $p\mathbb{Z}=P_k\cap\mathbb{Z}\;\;\forall\, k$. Αν πάλι $h^*\in P_k$ για κάποιο k τότε $h^*\in P_k\cap\mathbb{Z}=p\,\mathbb{Z}\;\Rightarrow\;p|h^*$. Άρα

$$p|h^*\;\;\Longleftrightarrow\;\;h^*\in P_k\quad\text{για κάποιο}\;\;k$$

Χωρίς περιορισμό της γενικότητας παίρνουμε το P_{-1} και έχουμε

$$p|h^*\;\;\Longleftrightarrow\;\;P_{-1}\big|h^*$$

Λόγω της (4) το δεξί μέλος της (3.3) είναι γινόμενο **ακεραίων** ιδεωδών. Επομένως

$$\begin{aligned}P_{-1}\big|h^*\;\;&\Longleftrightarrow\;\;\exists\,k=1,2,\ldots,p-2,\;2\nmid k,\quad\text{τέτοιο ώστε}\;\;P_{-1}\Big|\frac{F(\xi^k)P_k}{p}\\ &\Longleftrightarrow\;\;\exists\,k=1,2,\ldots,p-2,\;2\nmid k,\quad\text{τέτοιο ώστε}\;\;P_{-1}^2\Big|F(\xi^k)P_k\\ &\Longleftrightarrow\;\;\exists\,k=1,2,\ldots,p-2,\;2\nmid k,\quad\text{τέτοιο ώστε}\\ &\qquad\qquad\begin{cases}P_{-1}^2\big|F(\xi^k), & \text{όταν}\;\;k\not\equiv -1\,(\mathrm{mod}\,p-1)\\ P_{-1}\big|F(\xi^k), & \text{όταν}\;\;k\equiv -1\,(\mathrm{mod}\,p-1).\end{cases}\end{aligned}$$

Ισχυρίζομαι ότι

(**i**). $P_{-1}\nmid F(\xi^{-1})$

$$F(\xi)\;=\;\sum_{s=0}^{p-2}(g\xi)^s\;\equiv\;\sum_{s=0}^{p-2}1\;\equiv\;p-1\;\equiv\;-1\,(\mathrm{mod}\,p)$$

διότι $P\big|1-g\xi\;\;\Longrightarrow\;\;g\xi\equiv 1\,(\mathrm{mod}\,P)$. Επομένως

$$F(\xi^{-1})\;\equiv\;p-1\;\equiv\;-1\;\not\equiv\;0\,(\mathrm{mod}\,P_{-1}).$$

Από τα παραπάνω συμπεραίνουμε ότι:

(**ii**). $p \big| h^* \;\Rightarrow\; \exists\, k = 1, 2, \ldots, p-3,\ 2 \nmid k, \quad \tau.\omega \quad P_{-1}^2 \Big/ F(\xi^k)$

Διαλέγουμε τώρα την πρωταρχική ρίζα έτσι ώστε

(**iii**). $g^{p-1} \equiv 1 \,(\mathrm{mod}\, p^2)$.

(Γιατί είναι αυτό δυνατό;) Συνεπώς

$$\prod_{k=0}^{p-2}(1 - g\xi^k) \;=\; 1 - g^{p-1} \;\equiv\; 0 \,(\mathrm{mod}\, p^2),$$

οπότε

$$P_k^2 \big| (1 - g\xi^k), \quad k \bmod (p-1) \;\; (k, p-1) = 1.$$

Για $k \equiv -1 \,(\mathrm{mod}\, p-1)$ έχουμε λοιπόν

(**iv**). $P_{-1}^2 \big| 1 - g\xi^{-1} \;\Longrightarrow\; g \equiv \xi \bmod P_{-1}^2$.

Από την (**iv**) έπεται ότι:

$$F(\xi^k) \;=\; \sum_{s=0}^{p-2} g_s g^{sk} \bmod P_{-1}^2.$$

Δηλαδή

$$\begin{aligned} p \,\big|\, h^* \;&\Longleftrightarrow\; \exists\, k = 1, 2, \ldots, p-4,\ 2 \nmid k, \quad \tau.\omega \;\; \sum_{s=0}^{p-2} g_s g^{ks} \equiv 0 \,(\mathrm{mod}\, P_{-1}^2) \\ &\Longleftrightarrow\; \exists\, k = 1, 2, \ldots, p-4,\ 2 \nmid k, \quad \tau.\omega \;\; \sum_{s=0}^{p-2} g_s g^{ks} \equiv 0 \,(\mathrm{mod}\, p^2). \end{aligned}$$

Αν τώρα συμβολίσουμε

$$S_k(p) \;:=\; \sum_{n=1}^{p-1} n^k$$

τότε έχουμε το:

Θεώρημα 3.2.12 *Ισχύει η ισοδυναμία:*

$$p \,\big|\, h^* \;\Longleftrightarrow\; \exists\, k = 2, 4, \ldots, p-3, \quad \tau.\omega \;\; p^2 \big| S_{k+1}(p).$$

Απόδειξη:

$$g_s \equiv g^s + a_s p \,(\mathrm{mod}\, p^2)$$

όπου $a_s = \frac{1}{p}(g_s - g^s)$. Άρα

$$\begin{aligned}
g_s^{k+1} &\equiv (g^s + a_s p)^{k+1} \pmod{p^2} \\
\Longrightarrow\ g_s^{k+1} &\equiv g^{s(k+1)} + (k+1)a_s g^{sk} p \pmod{p^2} \\
&\equiv g^{s(k+1)} + (k+1)g^{sk} g_s - (k+1)g^{s(k+1)} \pmod{p^2} \\
\Longrightarrow\ (k+1)g^{sk} g_s &\equiv g_s^{k+1} + k g^{s(k+1)} \pmod{p^2} \\
\Longrightarrow\ (k+1)\sum_{s=0}^{p-2} g^{sk} g_s &\equiv \sum_{s=0}^{p-2} g_s^{k+1} + k\sum_{s=0}^{p-2} g^{s(k+1)} \pmod{p^2} \\
\Longrightarrow\ (k+1)\sum_{s=0}^{p-2} g^{sk} g_s &\equiv S_{k+1}(p) \pmod{p^2}. \quad \square
\end{aligned}$$

Επομένως το πρόβλημά μας είναι να βρούμε πότε

$$p^2 \big| S_{k+1} \pmod{p}.$$

Εδώ θα ορίσουμε τους **αριθμούς Bernoulli**.

Ορισμός 3.2.13

$$\frac{z}{e^z - 1} \;=\; \sum_{k=0}^{\infty} \frac{B_k}{k!}\, z^k, \quad \text{όπου } |z| < 1.$$

Συχνά παίρνουμε $f(x) = \sum_{\mu=0}^{m} a_\mu x^\mu$ και στη συνέχεια

$$f(x,z) \;=\; \sum_{n=0}^{\infty} f(x) z^n \;\in \mathbb{C}[x]\big[[z]\big],$$

οπότε αν θέσουμε $f_m(B) := \sum_{\mu=0}^{m} a_\mu B_\mu$ τότε μπορούμε να γράψουμε

$$f(B,z) \;=\; \sum_{n=0}^{\infty} f_n(B) z^n,$$

δηλαδή $\dfrac{z}{e^z - 1} = e^{Bz}$, $(f(x,z) = e^{xz})$. Ισχύουν

1. $e^{az} e^{Bz} = e^{(a+B)z}$ για $a \in \mathbb{C}$
2. $(1+B)^m - B^m = 0$ για $m \geq 2$, δηλαδή
$$m B_{m-1} + \sum_{k=0}^{m-2} \binom{m}{k} B_k \;=\; 0$$
3. $B_k = 0$ για $2 \nmid k$, $k \geq 3$

Σύνδεση αριθμών Bernoulli με $S_k(p)$

.

Θεώρημα 3.2.14

$$(k+1)S_k(n) \;=\; (n+B)^{k+1} - B^{k+1}$$

Απόδειξη:

$$\begin{aligned}
\sum_{k=0}^{\infty}\Big((n+B)^{k+1}-B^k\Big)\,\frac{z^k}{k!} &= e^{(n+B)z}-e^{Bz} \;=\; e^{Bz}\left(e^{nz}-1\right)\\
&= z\,\frac{e^{nz}-1}{e^z-1} \;=\; z\sum_{x=0}^{n-1}e^{xz} \;=\; z\sum_{x=0}^{n-1}\sum_{k=0}^{\infty}\frac{x^k z^k}{k!}\\
&= \sum_{k=0}^{\infty}\left(\sum_{x=0}^{n-1}x^k\right)\frac{z^{k+1}}{k!} \;=\; \sum_{k=0}^{\infty}\big((k+1)S_k(n)\big)\frac{z^{k+1}}{(k+1)!}\\
&= \sum_{k=0}^{\infty}\big(\,kS_{k-1}(n)\,\big)\,\frac{z^n}{n!} \quad \square
\end{aligned}$$

Θεώρημα 3.2.15 (Θεώρημα του von Staudt) *Έστω $p\in\mathbb{P}$, $p\neq 2$ και $k\in\mathbb{N}$, $2\big|k$. Τότε*

1. *Αν $(p-1)\nmid k$ τότε ο B_k είναι p-ακέραιος.*
2. *Αν $(p-1)\,\big|\,k$ τότε*

$$\begin{cases} pB_k \quad \text{είναι } p\text{-ακέραιος} \\ pB_k \equiv -1\,(mod\,p) \end{cases}$$

Παρατήρηση: Το θεώρημα ισχύει και για $p=2$.

Ορισμός 3.2.16 *Ένας ρητός αριθμός $\frac{a}{b}$, $(a,b)=1$, θα λέγεται* **p-ακέραιος** *όταν και μόνο όταν $p\nmid b$. Ο*

$$R_p=\left\{\frac{a}{b}\;\middle|\;a,b\in\mathbb{Z},\;p\nmid b\right\}$$

λέγεται **δακτύλιος των p-ακεραίων αριθμών**.

Έστω A, B p-ακέραιοι. Ορίζουμε

$$A \equiv B \pmod{p} \quad \text{τότε και μόνο τότε όταν} \quad p \big| (A-B) \text{ στο } R_p,$$
$$\text{δηλαδή όταν} \quad A - B \in pR_p \iff A \equiv B \pmod{pR_p}.$$

Απόδειξη του θεωρήματος 3.2.15:

(1) Ισχυρίζομαι ότι:

$$\begin{cases} pB_k \text{ είναι } p\text{-ακέραιος } \forall\, k \in \mathbb{N} \\ pB_k \equiv S_k(p) \pmod{p} \end{cases}$$

Απόδειξη: (του (1)). Το p είναι σταθερό. Θα εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής ως προς k. Από το θεώρημα 3.2.14 έπεται ότι

$$(k+1)S_k(p) \;=\; (k+1)pB_k + \sum_{m=0}^{k-1} \binom{k+1}{m} p^{k-m} pB_m.$$

Λήμμα 3.2.17 $\dfrac{1}{k+1}\binom{k+1}{m} p^{k-m}$ *είναι* p*-ακέραιος και μάλιστα* $\equiv 0\ (mod\, p)$.

Το λήμμα θα αποδειχτεί λίγο αργότερα.

Από το λήμμα 3.2.17 συνεπάγεται ότι

$$pB_k \;=\; S_k(p) - \sum_{m=0}^{k-1} \left(\binom{k+1}{m} \frac{p^{k-m}}{k+1} \right) pB_m \tag{3.4}$$

είναι p-ακέραιος. Ακόμη $pB_k \equiv S_k(p) \pmod{p}$.

(2) Ισχυρίζομαι ότι

$$S_k(p) \equiv 0 \pmod{p}, \qquad \text{όταν } p-1 \nmid k$$
$$S_k(p) \equiv -1 \pmod{p}, \quad \text{όταν } p-1 \big| k.$$

Παρατήρηση: Από (1) και (2) έπεται το θεώρημα 3.2.15.

Απόδειξη: (του (2))

$$S_k(p) \;=\; \sum_{x=1}^{p-1} x^k \;=\; \sum_{s=0}^{p-2} g^{ks}$$

όπου g είναι πρωταρχική ρίζα $\bmod p$.

Αν $p-1 \nmid k$ τότε

$$(1-g^k)S_k(p) \;=\; 1-g^{k(p-1)} \;\equiv\; 0 \,(\mathrm{mod}\, p)$$

ενώ $1-g^k \not\equiv 0 \,(\mathrm{mod}\, p)$. Άρα $S_k(p) \equiv 0 \,(\mathrm{mod}\, p)$.

Αν $p-1 \mid k$ τότε

$$S_k(p) \;=\; \sum_{x=1}^{p-1} x^k \;\equiv\; \sum_{x=1}^{p-1} 1 \,(\mathrm{mod}\, p) \;\equiv\; p-1 \;\equiv\; -1 \,(\mathrm{mod}\, p). \quad \square$$

Θεώρημα 3.2.18 *Για $p \neq 2$ και $k = 2, \ldots, p-1$, $2 \nmid k$, έχουμε*

$$pB_k \equiv S_k(p) \,(mod\, p^2).$$

Απόδειξη: Λογω της σχέσης (3.4) και για $m \leq k-1 < p-1$, $p-1 \nmid m$, έχουμε ότι ο B_m είναι p-ακέραιος, δηλαδή

$$\sum_{m=0}^{k-1} \left(\binom{k+1}{m} \frac{p^{k-m}}{k+1} \right) pB_m \;\equiv\; 0 \,(\mathrm{mod}\, p^2))$$
$$\Longrightarrow \quad pB_k \;\equiv\; S_k(p) \,(\mathrm{mod}\, p^2). \quad \square$$

Απόδειξη: (Του λήμματος 3.2.17)

Κατ' αρχήν ισχυρίζομαι ότι για $r \in \mathbb{N}$ και $p \in \mathbb{P}$ αν $e(r)$ είναι ο μέγιστος p-εκθέτης του r, τότε

$$e(r!) \;=\; \sum_{n=1}^{\infty} \left[\frac{r}{p^n} \right].$$

Η απόδειξη αφήνεται σαν άσκηση στον αναγνώστη. Αν λοιπόν $p \neq 2$ τότε έχουμε

$$e(r!) \;\leq\; \sum_{n=1}^{\infty} \frac{r}{p^n} \;=\; r\,\frac{\frac{1}{p}}{1-\frac{1}{p}} \;=\; \frac{r}{p-1} \;<\; \frac{r}{2} \;<\; r-1$$
$$\Longrightarrow \quad \frac{\binom{k+1}{m}}{k+1} \;=\; \frac{(k+1)\cdots(m+1)}{(m+1-k)!}$$

και

$$e\,\big(\,(m+1-k)!\,\big) < \; m-k,$$

οπότε

$$e\left(\frac{\binom{k+1}{m}}{k+1} p^{m-k} \right) \;>\; m-k-(m-k) \;\geq\; 0. \quad \square$$

Θεώρημα 3.2.19 *Έστω $p \in \mathbb{P}$, $p \neq 2$. Τότε ισχύει*

$$p \big| h^* \iff \exists\, k = 2, 3, \ldots, p-3,\ 2 \big| k \ \text{και}\ p \big| B_k.$$

Αν $p = 2$ τότε $h^* = 1$.

Απόδειξη: Συνάγεται εύκολα με χρήση των θεωρημάτων 3.2.12 και 3.2.18. □

Παρατηρήσεις:

1. Έστω $k \leq p-3$ τότε $(p-1) \nmid B_k$ συνεπώς ο B_k είναι p-ακέραιος.

2. Αρκεί να υπολογίσουμε το $B_k \bmod p$ διότι αν R_p ο δάκτυλιος των p-ακεραίων τότε

$$\begin{aligned} & R_p \big/ pR_p \cong \mathbb{Z} \big/ p\mathbb{Z} \\ \Longrightarrow\ & \forall\, k \leq p-3 \quad \exists\, \beta_k \in \mathbb{Z},\ B_k = \beta_k \pmod p. \end{aligned}$$

Το β_k μπορούμε να το υπολογίσουμε από τους αναδρομικούς τύπους $\bmod p$

$$\begin{aligned} (\beta+1)^m \equiv \beta^m \pmod p \ &\Longrightarrow\ \sum_{n=0}^{m} \binom{m}{n} \beta_n \equiv \beta_m \pmod p \\ &\Longrightarrow\ m\beta_{m-1} + \sum_{n=0}^{m-2} \binom{m}{n} \beta_n \equiv 0 \pmod p. \end{aligned}$$

3. Αν $p \big| h^*$ τότε $p \big| h_{\mathbb{Q}(\zeta_p)} = h_0 h^*$.

Χωρίς αποδείξεις αναφέρουμε τα παρακάτω.

Θεώρημα 3.2.20

$$p \nmid h^* \implies p \nmid h_0.$$

Για την απόδειξη χρειαζόμαστε p-αδικές μεθόδους.

Εικασία 3.2.21 *Πάντοτε ισχύει $p \nmid h_0$.*

Η εικασία είναι ανοιχτή μέχρι σήμερα.

Από το θεώρημα 3.2.19 και αν δεχτούμε την εικασία 3.2.21 προκύπτει το

Θεώρημα 3.2.22 *Έστω $p \in \mathbb{P}$, $p \neq 2$ και $h := h_{\mathbb{Q}(\zeta_p)}$. Τότε*

$$p \,|\, h \iff \exists\, k \in \{2, 3, \ldots, p-3\},\ 2 \,|\, k \ \text{και}\ p \,|\, B_k.$$

Ορισμός 3.2.23 *Ο πρώτος p, $p \neq 2$, θα λέγεται*

$$\begin{aligned} \textbf{ομαλός } \textit{(regular)} &\iff p \nmid h_{\mathbb{Q}(\zeta_p)}, \\ \textbf{ανώμαλος } \textit{(irregular)} &\iff p \,|\, h_{\mathbb{Q}(\zeta_p)}. \end{aligned}$$

"Πειραματικά" βλέπουμε ότι υπάρχουν πιο πολλοί ομαλοί απ' ότι ανώμαλοι πρώτοι.

Εικασία 3.2.24 *Υπάρχουν άπειροι ομαλοί πρώτοι.*

Θεώρημα 3.2.25 *Υπάρχουν άπειροι ανώμαλοι πρώτοι.*

37, 59 και 67 είναι οι μοναδικοί ανώμαλοι πρώτοι που είναι μικρότεροι από το 100.

Κεφάλαιο 4

Αβελιανές L-σειρές

4.1 Θεωρήματα πυκνότητας πρώτων ιδεωδών

Στην παράγραφο αυτή θα μελετήσουμε την κατανομή των πρώτων ιδεωδών αλγεβρικού σώματος αριθμών K. Το θεμελιώδες θεώρημα 2.2.2 μάς δίνει ότι

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) \gneqq 0. \tag{4.1}$$

Από εδώ και κάτω το $s \in \mathbb{R}$, $s > 1$. Από τη σχέση (4.1) έχουμε ότι:

$$\log\zeta_K(s) \;=\; -\log(s-1)+O(1) \quad \text{για } s\to 1^+$$

Λήμμα 4.1.1 *Ισχύει ότι*

$$\log\zeta_K(s) \;=\; \sum_{P\in\mathbb{P}(K)}\frac{1}{N(P)^s}+O(1) \quad \text{για } s\to 1^+.$$

Απόδειξη:

$$\begin{aligned}\log\zeta_K(s) &= \log\left(\prod_{P\in\mathbb{P}(K)}\frac{1}{1-\frac{1}{N(P)^s}}\right) = \sum_{P\in\mathbb{P}(K)}\sum_{m=1}^{\infty}\frac{1}{mN(P)^{sm}}\\ &= \sum_{P\in\mathbb{P}(K)}\frac{1}{N(P)^s}+\sum_{P\in\mathbb{P}(K)}\sum_{m\geq 2}\frac{1}{mN(P)^{sm}}\end{aligned}$$

Τώρα

$$\sum_{P\in\mathbb{P}(K)}\sum_{m\geq 2}\frac{1}{mN(P)^{sm}} \;\leq\; (K:\mathbb{Q})\sum_{p\in\mathbb{P}}\sum_{m\geq 2}\frac{1}{p^{sm}}$$

$$= \;(K:\mathbb{Q})\sum_{p\in\mathbb{P}}\frac{\frac{1}{p^{2s}}}{1-\frac{1}{p^s}} \;\leq\; (K:\mathbb{Q})\sum_{p\in\mathbb{P}}2\,\frac{1}{p^{2s}} \;\leq\; (K:\mathbb{Q})\cdot 2\zeta_{\mathbb{Q}}(2) \;<\; \infty. \quad \square$$

Επομένως

Θεώρημα 4.1.2

$$\sum_{P\in\mathbb{P}(K)} \frac{1}{N(P)^s} \;=\; -\log(s-1)+O(1)$$

καθώς $s\to 1^+$.

Παρατηρήσεις: Άμεση συνέπεια του θεωρήματος είναι

1. Το σύνολο $\#\,\mathbb{P}(K)$ είναι άπειρο, και ιδιαίτερα,
2. αν $K=\mathbb{Q}$ τότε το σύνολο $\#\,\mathbb{P}(\mathbb{Q})=\mathbb{P}$ είναι άπειρο.

Λήμμα 4.1.3 *Έστω* $A\subseteq\mathbb{P}(K)$ *με* $\#\{P\in A \mid f_P=f\left(P/p\right)=1\}<\infty$. *Τότε*

$$\sum_{P\in A}\frac{1}{N(P)^s}=O(1)$$

Απόδειξη: Αν $f_P=f\left(P/p\right)\neq 1$ τότε $N(P)\geq p^2$, συνεπώς

$$\sum_{P\in A}\frac{1}{N(P)^s} \;=\; \sum_{\substack{P\in A\\ f_P\neq 1}}\frac{1}{N(P)^s}+O(1)$$

όπου

$$\sum_{\substack{P\in A\\ f_P\neq 1}}\frac{1}{N(P)^s} \;\leq\; (K:\mathbb{Q})\sum_{p\in\mathbb{P}}\frac{1}{p^{2s}} \;\leq\; (K:\mathbb{Q})\zeta(2) \;<\; \infty. \quad \square$$

Επομένως

Θεώρημα 4.1.4

$$\sum_{\substack{P\in\mathbb{P}(K)\\ f_P=1}}\frac{1}{N(P)^s} \;=\; -\log(s-1)+O(1).$$

Συνεπώς υπάρχουν **άπειρα πρώτα ιδεώδη πρώτου βαθμού** στο K.

Ορισμός 4.1.5 *Έστω* $A\subseteq\mathbb{P}(K)$ *τέτοιο ώστε να υπάρχει* $\delta=\delta(A)>0$ *με*

$$\sum_{P\in A}\frac{1}{N(P)^s} \;=\; -\delta\log(s-1)+O(1)$$

καθώς $s\to 1^+$. *Τότε ο* δ *θα λέγεται* **πυκνότητα του Dirichlet του** A.

Έχουμε λοιπόν το ακόλουθο

Θεώρημα 4.1.6 *Η πυκνότητα του Dirichlet όλων των πρώτων ιδεωδών του K βαθμού ένα, υπάρχει και είναι ίση με ένα.*

Παρατήρηση 4.1.6′: Έστω $A \subseteq B \subseteq \mathbb{P}(K)$ και $\#\{P \in B \setminus A \mid f_P = 1\} < \infty$. Τότε αν υπάρχει η πυκνότητα του Dirichletγια ένα τουλάχιστο από τα σύνολα A, B θα υπάρχει και για το άλλο και μάλιστα $\delta(A) = \delta(B)$.

Το πρόβλημα που θα μας απασχολήσει παρακάτω είναι το εξής:

Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών. Μπορούμε να χαρακτηρίσουμε το L μέσω της ανάλυσης όλων των $P \in \mathbb{P}(K)$ στο L;

Η απάντηση είναι ΝΑΙ αν L/K επέκταση του Galois. Υπενθυμίζουμε ότι για κάθε επέκταση αλγεβρικών σωμάτων αριθμών L/K, όπου $(L : K) = n$, ισχύουν:

$$\begin{aligned} P \in \mathbb{P}(K) \implies & PR_L = Q_1^{e_1} \cdots Q_r^{e_r} \\ f_i = f\left(\frac{Q_i}{P}\right) = & \left(\frac{R_L}{Q_i} : \frac{R_K}{P}\right) \\ N_{L/K}(Q_i) = & N_{K/Q}(P)^{f_i} \\ e_1 f_1 + e_2 f_2 + \cdots + e_r f_r = & n \end{aligned}$$

Αν $r = n$ τότε λέμε ότι ο P **αναλύεται πλήρως στο** L. Αν P δεν διακλαδίζεται στο L και $r = 1$ (οπότε $f = n$) τότε λέμε ότι P **αδρανεί στο** L. Η πλήρης ανάλυση και η αδράνεια είναι δύο ακραίες καταστάσεις στην ανάλυση των πρώτων ιδεωδών του K.

Έστω τώρα L/K επέκταση του Galois. Υπάρχουν άπειρα πρώτα ιδεώδη και των δύο τύπων ή όχι;

Εν γένει αυτό **δεν** είναι σωστό. Πράγματι αν P αδρανεί στο L τότε $PR_L = Q$ και το σύμβολο του Frobenious $\left(\frac{L/K}{Q}\right)$ έχει τάξη $f = n$, δηλαδή παράγει όλη την ομάδα του Galois $G = G\left(L/K\right)$. Επομένως τέτοιο P μπορεί να υπάρχει μόνο αν η G είναι κυκλική. Και το αντίστροφο είναι αληθές, θα ξαναγυρίσουμε σ′ αυτό όταν αναφερθούμε στο **θεώρημα πυκνότητας του Tchebotarev (Čebotarev)**.

Έστω τώρα

$$\mathcal{A}_{L/K} := \{P \in \mathbb{P}(K) \mid P \text{ αναλύεται πλήρως στο } L\}.$$

Θεώρημα 4.1.7 *Έστω L/K επέκταση του Galois. Τότε ισχύει*

$$\delta\left(\mathcal{A}_{L/K}\right) = \frac{1}{(L : K)}$$

Απόδειξη: Αν $P \in \mathcal{A}_{L/K}$ τότε $PR_L = Q_1 Q_2 \dots Q_n$ όπου n είναι ο βαθμός της επέκτασης ${}^{L}\!/_{K}$ και $N(Q_1) = \dots = N(Q_n) = N(P)$. Συνεπώς

$$\sum_{P \in \mathcal{A}_{L/K}} \frac{1}{N(P)^s} \;=\; \frac{1}{n} \sum_{Q/P \in \mathcal{A}_{L/K}} \frac{1}{N(Q)^s} \tag{4.2}$$

Ισχυρίζομαι ότι

$$\begin{aligned} A \;&:=\; \left\{ Q \in \mathbb{P}(L) \;\middle|\; f\left(\frac{Q}{p\mathbb{Z}}\right) = 1,\; e\left(\frac{Q}{Q \cap R_K}\right) = 1 \right\} \\ &\subseteq\; \left\{ Q \in \mathbb{P}(L) \;\middle|\; \exists\, P \in \mathcal{A}_{L/K} \;\; Q \big| P \right\} =: B. \end{aligned} \tag{4.3}$$

Από τη σχέση (4.3), το θεώρημα 4.1.6 και την παρατήρηση 4.1.6′ έπεται ότι

$$\sum_{Q/P \in \mathcal{A}_{L/K}} \frac{1}{N(Q)^s} \;=\; -\log(s-1) + O(1) \quad \text{για} \;\; s \to 1^+,$$

οπότε η (4.2) δίνει ότι

$$\delta(\mathcal{A}_{L/K}) \;=\; \frac{1}{n} \;=\; \frac{1}{(L:K)}.$$

Απόδειξη της σχέσης (4.3):

Έστω ότι $Q|P$. Αφού ${}^{L}\!/_{K}$ Galois θα έχουμε ότι

$$f_1 = f_2 = \dots = f_r = f\left(\frac{Q}{P}\right) = 1$$

και

$$e_1 = e_2 = \dots = e_r = e\left(\frac{Q}{P}\right) = 1$$

οπότε

$$P \in \mathcal{A}_{L/K}. \quad \square$$

Λήμμα 4.1.8 *Έστω ${}^{L_1}\!/_{K}, {}^{L_2}\!/_{K}$ επεκτάσεις αλγεβρικών σωμάτων αριθμών και $L = L_1 \cdot L_2$. Τότε (το $P \in \mathbb{P}(K)$ αναλύεται πλήρως στο $L_1 \cdot L_2$) τότε και μόνο τότε όταν (το P αναλύεται πλήρως στα L_1 και L_2).*

Απόδειξη: Η απόδειξη είναι γνωστή όταν ${}^{L_1}\!/_{K}$ και ${}^{L_2}\!/_{K}$ είναι κανονικές επεκτάσεις ([22], σελίδα 128). Τέλος, αρκεί να παρατηρήσουμε ότι το $P \in \mathbb{P}(K)$ αναλύεται πλήρως στην ${}^{L}\!/_{K}$ τότε και μόνον τότε όταν αναλύεται πλήρως στην ${}^{E}\!/_{K}$ όπου E η κανονική θήκη του L στο K. $\square$

Λήμμα 4.1.9 *Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών και E η κανονική θήκη της L/K. Τότε το $P \in \mathbb{P}(K)$ αναλύεται πλήρως στο E τότε και μόνον τότε όταν αναλύεται πλήρως στο L.*

Απόδειξη: Κατ' αρχήν, αν ο P αναλύεται πλήρως στο E, τότε θα αναλύεται πλήρως και στο σώμα L. Αντίστροφα, έστω ότι ο P αναλύεται πλήρως στο L. Ο P θα αναλύεται πλήρως και σε κάθε συζυγές $\sigma(L)$ του L, όπου το σ διατρέχει όλους τους K-μονομορφισμούς του L.

Αν τώρα $Q \in \mathbb{P}(E)$ τέτοιο ώστε $Q \big| P$, τότε το **σώμα ανάλυσης** του Q στο E θα περιέχει όλα τα συζυγή $\sigma(L)$. Επομένως θα περιέχει και την σύνθεσή τους (γινόμενο), δηλαδή το E. Αυτό σημαίνει ότι το E ταυτίζεται με το σώμα ανάλυσης του Q, δηλαδή ότι ο P αναλύεται πλήρως στο E. □

Θεώρημα 4.1.10 *Αν L/K επέκταση αλγεβρικών σωμάτων αριθμών, τότε*

$$\delta(\mathcal{A}_{L/K}) \;=\; \frac{1}{(E:K)}$$

όπου E η κανονική θήκη της L/K.

Απόδειξη: Συνέπεια του θεωρήματος 4.1.7 και του λήμματος 4.1.9. □

Θεμελιώδες Θεώρημα 4.1.11 *Αν L/K επέκταση του Galois, αλγεβρικών σωμάτων αριθμών, τότε το L προσδιορίζεται* **μονοσήμαντα** *από το $\mathcal{A}_{L/K}$.*

Το Θεώρημα αποτελεί θετική απάντηση στο πρόγραμμα που πρότεινε ο Kronecker να χαρακτηρίσουμε τις επεκτάσεις του K μαζί με όλες τις αλγεβρικές και αριθμητικές ιδιότητές τους, αποκλειστικά μέσω συνόλων πρώτων ιδεωδών του σώματος K. Κατά τρόπο ανάλογο, που το θεώρημα του Cauchy χαρακτηρίζει τη συνάρτηση μέσω των τιμών της στο σύνορο. (In ähnlicher Weise wie nach dem Cauchysehen Satz eine Funktion durch ihre Randwerte bestimmt ist).

Το θεώρημα είναι συνέπεια του:

Λήμμα 4.1.12 *Έστω L_1/K, L_2/K επεκτάσεις του Galois αλγεβρικών σωμάτων αριθμών και έστω*

$$\delta\left(\mathcal{A}_{L_1/K} - \mathcal{A}_{L_2/K}\right) \;=\; \delta\left(\mathcal{A}_{L_2/K} - \mathcal{A}_{L_1/K}\right) \;=\; 0$$

(δηλαδή $\mathcal{A}_{L_1/K}$ και $\mathcal{A}_{L_2/K}$ διαφέρουν κατά κάποιο σύνολο με πυκνότητα Dirichlet ίση με 0). Τότε $L_1 = L_2$.

Απόδειξη: (Του λήμματος).

Έστω $L = L_1 L_2$. Η (4.1.8) δίνει

$$\mathcal{A}_{L/K} \;=\; \mathcal{A}_{L_1/K} \cap \mathcal{A}_{L_2/K}$$

$$\begin{aligned} \Longrightarrow \quad & \delta(\mathcal{A}_{L/K}) = \delta\left(\mathcal{A}_{L_1/K} \cap \mathcal{A}_{L_2/K}\right) \\ = \quad & \delta\left(\mathcal{A}_{L_1/K}\right) - \delta\left(\mathcal{A}_{L_1/K} - \mathcal{A}_{L_2/K}\right) \\ = \quad & \delta\left(\mathcal{A}_{L_1/K}\right) + 0 \;=\; \delta\left(\mathcal{A}_{L_1/K}\right) \;=\; \frac{1}{(L_1 : K)}. \end{aligned}$$

Αλλά

$$\delta\left(\mathcal{A}_{L/K}\right) = \frac{1}{(L : K)} \quad \Longrightarrow \quad (L : K) = (L_1 : K)$$

και

$$L_1 \subseteq L \quad \Longrightarrow \quad L = L_1.$$

Ομοίως

$$\begin{aligned} \delta\left(\mathcal{A}_{L/K}\right) \;&=\; \delta\left(\mathcal{A}_{L_1/K} \cap \mathcal{A}_{L_2/K}\right) \\ &= \delta\left(\mathcal{A}_{L_2/K}\right) \end{aligned}$$

$$\Longrightarrow \quad (L : K) = (L_2 : K)$$

και

$$L_2 \subseteq L \quad \Longrightarrow \quad L = L_2.$$

Επομένως

$$L_1 = L_2 \quad \square$$

Παρατηρήσεις:

1. Για $K = \mathbb{Q}$ και $L = \mathbb{Q}(\zeta_m)$ και

$$\mathcal{A}_{L/K} = \left\{(p) \;\middle|\; p \in \mathbb{P},\; p \equiv 1 \,(\mathrm{mod}\, m)\right\} \;=\; H_m^+ \cap \mathbb{P}(K)$$

όπου H_m^+ είναι η κύρια κλάση $mod\, m$ με στενή σημασία.

2. **Θεωρία κλάσεων σωμάτων**.

   (i) Χωρίς απόδειξη αναφέρουμε: Αν L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών, τότε υπάρχει $\mathfrak{m}$ ακέραιο ιδεώδες του K και $\mathcal{U}$ ομάδα με

   $$A_{\mathfrak{m}} \supseteq \mathcal{U} \supseteq H^{+}_{\mathfrak{m}}$$

   τέτοια ώστε

   $$\mathcal{A}_{L/K} = \mathcal{U} \cap \mathbb{P}(K).$$

   (ii) Σε κάθε υποομάδα $\mathcal{U}$ τέτοια ώστε

   $$A_{\mathfrak{m}} \supseteq \mathcal{U} \supseteq H^{+}_{\mathfrak{m}}$$

   υπάρχει ακριβώς μία αβελιανή επέκταση L/K με

   $$\mathcal{A}_{L/K} = \mathcal{U} \cap \mathbb{P}(K)$$

   με εξαίρεση το πολύ πεπερασμένου πλήθους πρώτων ιδεωδών P του K.

4.2 Αβελιανές L-σειρές

Έστω τώρα L/K μία επέκταση Galois αλγεβρικών σωμάτων αριθμών $G = \mathrm{Gal}(L/K)$. Έστω $P \in \mathbb{P}(K)$ και $Q \in \mathbb{P}(L)$, Q/P. Υπενθυμίζουμε ότι η ακολουθία

$$1 \longrightarrow G_T\left(Q/P\right) \longrightarrow G_Z\left(Q/P\right) \longrightarrow G\left(\overline{L}/\overline{K}\right) \longrightarrow 1$$

είναι ακριβής, όπου $\overline{L} = S/Q, \overline{K} = R/P$ είναι τα σωμάτα υπολοίπων των L, K αντίστοιχα (δες [2], σελίδα 161).

Αν P δεν διακλαδίζεται στην L/K τότε $G_T(Q/P) = \{1\}$, οπότε

$$G_Z(Q/P) \;\cong\; G(\overline{L}/\overline{K}) \;= \left\langle \left[\frac{L/K}{Q}\right] \right\rangle$$

Αν $\sigma \in G$ τότε

$$\begin{aligned} G_Z(\sigma Q/P) &= \sigma G_Z(Q/P)\sigma^{-1} \\ G_T(\sigma Q/P) &= \sigma G_T(Q/P)\sigma^{-1} \end{aligned}$$

και

$$\left[\frac{L/K}{\sigma(Q)}\right] \;=\; \sigma\left[\frac{L/K}{Q}\right]\sigma^{-1}$$

Αν G αβελιανή, τότε $G_Z\big(Q/P\big)$, $G_T\big(Q/P\big)$ και $\left[\frac{L/K}{Q}\right]$ εξάρτώνται μόνο από το P και θα γράφουμε $G_Z(P)$, $G_T(P)$ και $\left[\frac{L/K}{P}\right]$, αντίστοιχα.

Έστω τώρα $\chi \in \widehat{G}$. Στον χ αντιστοιχούμε έναν χαρακτήρα της ομάδας

$$I_K(D_K) \;:=\; \big\{A \in I_K \;\big|\; A \;\text{ πρώτο προς }\; D_K\big\}$$

$$(D_K \;\text{ είναι η διακρίνουσα του σώματος }\; K)$$

τον οποίο θα συμβολίζουμε πάλι με χ και τον ορίζουμε ως εξής:

Έστω, κατ' αρχήν, $P \in \mathbb{P}(K)$, $Q \in \mathbb{P}(L)$, $Q\big|P$ τα οποία τα κρατούμε σταθερά. Έστω σ_P ένα στοιχείο της $G_Z(P)$ το οποίο απεικονίζεται στον αυτομορφισμό του Frobenius

$$x \longmapsto x^{N(P)} \quad \text{στην} \quad G\big(\overline{L}/\overline{K}\big).$$

Κάθε άλλο στοιχείο που απεικονίζεται στον αυτομορφισμό είναι της μορφής

$$\sigma_P\sigma, \quad \text{όπου} \quad \sigma \in G_T(P).$$

Ορισμός 4.2.1 *Ορίζουμε*

$$\chi(P) \;:=\; \chi(\sigma_P)\cdot\frac{1}{e_P}\sum_{\sigma\in G_T(P)}\chi(\sigma)$$

όπου e_P είναι ο δείκτης διακλάδωσης του P στο L.

Παρατηρήσεις:

(1). Ο ορισμός εξαρτάται μόνο από το P και όχι από το σ_P.

(2). Αν $G_T(P) \not\subset \mathrm{Ker}(\chi)$ τότε $\chi(P) = 0$.

(3). Αν $G_T(P) \subset \mathrm{Ker}(\chi)$ τότε $\chi(P) = \chi(\sigma_P)$.

Η διαπίστωση αυτών των ιδιοτήτων αφήνεται σαν άσκηση στον αναγνώστη. Από παρατήρηση (3) έπεται ότι, όταν P δεν διακλαδίζεται στο L, τότε

$$\chi(P) \;=\; \chi\left(\left[\frac{L/K}{P}\right]\right).$$

Επεκτείνουμε τώρα τον ορισμό του χ πολλαπλασιαστικά στο I_K. Ο χ δηλαδή απεικονίζει την I_K στο $T \cup \{0\}$ όπου $T = \{z \in \mathbb{C} \mid |z| = 1\}$ και την $I_K(D_K)$ στο T. Ο χ είναι ένας **χαρακτήρας της $I_K(D_K)$ στο T**.

Ορισμός 4.2.2 *Σε κάθε χαρακτήρα χ, όπως τον ορίσαμε παραπάνω, ορίζουμε την* **αβελιανή L-συνάρτηση**

$$L(s, \chi, {}^{L}\!/_{K}) \;=\; \sum_{\substack{A \in I_K \\ A \text{ ακέραιο}}} \frac{\chi(A)}{N(A)^s}$$

με $Re(s) > 1$.

Χωρίς απόδειξη αναφέρουμε μερικές ιδιότητές της.

Θεώρημα 4.2.3

1. *Η $L(s, \chi, {}^{L}\!/_{K})$ συγκλίνει για $Re(s) > 1$ και παριστά ολόμορφη συνάρτηση σ΄ αυτό το ημιεπίπεδο.*

2. *Γινόμενο Euler*

$$L(s, \chi, {}^{L}\!/_{K}) \;=\; \prod_{P \in \mathbb{P}(K)} \left(1 - \frac{\chi(P)}{N(P)^s}\right)^{-1}, \quad (Re(s) > 1)$$

3. *Ισχύει*

$$\zeta_L(s) \;=\; \prod_{\chi \in \widehat{G}} L(s, \chi, {}^{L}\!/_{K}), \quad (Re(s) > 1)$$

4. *Η $L(s, \chi, {}^{L}\!/_{K})$ έχει* **αναλυτική επέκταση** *σαν* **μερόμορφη συνάρτηση** *του s.*
   Αν $\chi = \chi_0$ τότε η $L(s, \chi_0, {}^{L}\!/_{K})$ **έχει απλό πόλο στη θέση** *$s = 1$ και είναι* **ολόμορφη για όλα τα άλλα** *s.*
   Αν $\chi \neq \chi_0$ τότε $L(s, \chi, {}^{L}\!/_{K})$ είναι **ακέραια** *συνάρτηση του s.*
   Σημείωση: *Οι αποδείξεις μοιάζουν με αυτές που ήδη δώσαμε για τις σειρές του Dirichlet. Ο ενδιαφερόμενος αναγνώστης όμως μπορεί να δει [15], σελίδες 164-171.*
   Η (4) στηρίζεται σε δύσκολο αποτέλεσμα. Για $\chi = \chi_0$ έχουμε $L(s, \chi_0, {}^{L}\!/_{K}) = \zeta_K(s)$, οπότε οι προτάσεις 3. και 4. του θεωρήματος 4.2.3 δίνουν:

5. *${}^{\zeta_L(s)}\!/_{\zeta_K(s)}$ είναι* **ακέραια συνάρτηση**.

6. *Αν* $\chi \neq \chi_0$, *τότε* $L\big(1, \chi, {}^{L}\!/_{K}\big) \neq 0, \infty$.

   Απόδειξη: *Η πρόταση 4. του θεωρήματος 4.2.3 μας δίνει ότι* $L\big(1, \chi, {}^{L}\!/_{K}\big) \neq \infty$. *Επίσης* $L\big(1, \chi, {}^{L}\!/_{K}\big) \neq 0$ *διότι ο μηδενισμός κάποιας* L*-σειράς στην θέση* $s=1$ *θα αναιρούσε τον πόλο της* $L\big(s, \chi_0, {}^{L}\!/_{K}\big)$ *για* $s=1$ *οπότε η* $\zeta_L(s)$ *θα ήταν ολόμορφη για* $s=1$, *άτοπο.* □

Θεώρημα 4.2.4 (Θεώρημα του Dirichlet) *Αν* ${}^{L}\!/_{K}$ *είναι μία αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών και* $\sigma \in G = Gal\big({}^{L}\!/_{K}\big)$, *ορίζουμε*

$$A(\sigma) \;:=\; \left\{ P \in \mathbb{P}(K) \;\middle|\; \left[\frac{L/K}{P}\right] = \sigma \right\}.$$

Το $A(\sigma)$ *έχει πυκνότητα Dirichlet*

$$\delta(A(\sigma)) \;=\; \frac{1}{(L:K)} \;=\; \frac{1}{n}$$

όπου $n = (L:K)$.

Απόδειξη: Κατ' αρχήν κάνοντας χρήση του λήμματος 4.1.1 και του θεωρήματος 4.1.2 μπορεί κανείς να δει ότι: Αν A είναι κάποιο σύνολο πρώτων ιδεωδών του K τότε

$$\text{το } A \text{ έχει πυκνότητα Dirichlet } \delta(A) \iff \exists \lim_{s\to 1^+} \frac{\log \prod_{P\in A} (1 - N(P)^{-s})^{-1}}{\log \zeta_K(s)} \;=\; \delta(A).$$

Επομένως αρκεί να δείξουμε ότι

$$\lim_{s\to 1^+} \frac{\log \prod_{P\in A(\sigma)} (1 - N(P)^{-s})^{-1}}{\log \zeta_K(s)} \;=\; \frac{1}{n}.$$

Το αριστερό μέλος της παραπάνω σχέσης είναι ίσο με

$$\begin{aligned} &\lim_{s\to 1^+} \frac{-\sum_{P\in A(\sigma)} \log(1 - N(P)^{-s})}{\log \zeta_K(s)} \\ =\; &\lim_{s\to 1^+} \frac{\sum_{P\in A(\sigma)} \sum_{m=1}^{\infty} (m^{-1} N(P)^{-ms})}{\log \zeta_K(s)} \end{aligned} \tag{4.4}$$

Ορίζουμε τώρα

$$T(s) \;:=\; n^{-1} \sum_{\chi\in\widehat{G}} \chi(\sigma^{-1}) \log L\big(s, \chi, {}^{L}\!/_{K}\big)$$

και έχουμε

$$\lim_{s\to 1^+}\frac{T(s)}{\log\zeta_K(s)} \;=\; \frac{1}{n}+\lim_{s\to 1^+}\frac{n^{-1}\sum\limits_{\chi\neq\chi_0}\chi(\sigma^{-1})\log L\big(s,\chi,{}^{L}\!/_{K}\big)}{\log\zeta_K(s)} \;=\; \frac{1}{n}. \tag{4.5}$$

Από την άλλη μεριά

$$\begin{aligned} T(s) &= -n^{-1}\sum_{\chi\in\widehat{G}}\chi(\sigma^{-1})\sum_{P\in\mathbb{P}(K)}\sum_{m=1}^{\infty}\frac{\chi(P)}{mN(P)^{ms}} \\ &= -n^{-1}\sum_{P\in\mathbb{P}(K)}\sum_{m=1}^{\infty}m^{-1}N(P)^{-ms}\sum_{\chi\in\widehat{G}}\chi(\sigma^{-1})\chi(P). \end{aligned}$$

Για όλα σχεδόν τα P, έχουμε

$$\chi(P)=\left[\frac{L/K}{P}\right]$$

οπότε από τις γνωστές σχέσεις ορθογωνιότητας προκύπτει ότι

$$\sum_{\chi\in\widehat{G}}\chi\left(\,\sigma^{-1}\left[\frac{L/K}{P}\right]\,\right)=\begin{cases} n, & \text{όταν}\quad \left[\frac{L/K}{P}\right]=\sigma \\ 0, & \text{αλλιώς.}\end{cases}$$

Επομένως

$$\lim_{s\to 1^+}\frac{T(s)}{\log\zeta_K(s)} \;=\; \lim_{s\to 1^+}\frac{-\sum\limits_{m=1}^{\infty}\sum\limits_{P\in A(\sigma)}m^{-1}N(P)^{-ms}}{\log\zeta_K(s)} \tag{4.6}$$

οπότε οι σχέσεις (4.4), (4.5), (4.6) μας δίνουν το ζητούμενο. □

Πόρισμα 4.2.5 *Έστω* ${}^{L}\!/_{K}$ **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών και έστω* (f,r) *ένας τύπος ανάλυσης για την επέκταση* ${}^{L}\!/_{K}$*. Ικανή και αναγκαία συνθήκη για να υπάρχουν* **άπειρα πρώτα ιδεώδη** $P\in\mathbb{P}(K)$ **του τύπου** (f,r) *είναι η* G *να έχει ένα στοιχείο τάξης* f*. Αν τώρα*

$$n_f \;:=\; \#\big\{g\in G \;\big|\; ord(g)=f\big\}$$

τότε το σύνολο

$$\mathcal{A}_{L/K} \;=\; \big\{P\in\mathbb{P}(K) \;\big|\; P \text{ έχει τύπο ανάλυσης } (f,r)\big\}$$

έχει πυκνότητα Dirichlet

$$\delta(\mathcal{A}_{L/K}) \;=\; \frac{n_f}{n}.$$

Απόδειξη: Έστω $P \in \mathbb{P}(K)$ μη-διακλαδιζόμενο στην επέκταση L/K και έστω ότι ο βαθμός αδράνειας του P στην L/K είναι f. Τότε η G έχει τουλάχιστον ένα στοιχείο τάξης f, το $\left[\frac{L/K}{P}\right]$.
Αντίστροφα τώρα. Έστω $n_f \geq 1$ το πλήθος των στοιχείων της G τάξης f. Το θεώρημα (4.2.4) συνεπάγεται ότι το σύνολο όλων των πρώτων ιδεωδών του K που δεν διακλαδίζονται στην L/K και τέτοια ώστε $\left[\frac{L/K}{P}\right]$ να έχει τάξη f στην G έχει πυκνότητα Dirichlet ίση με $\frac{n_f}{n}$. Αλλά $\left[\frac{L/K}{P}\right]$ έχει τάξη f στην G σημαίνει ότι ο βαθμός αδράνειας του P στην G είναι f, δηλαδή ότι το ιδεώδες P είναι του τύπου (f, r). □

Πόρισμα 4.2.6 (Θεώρημα του Dirichlet για αριθμητικές προόδους) *Έστω $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. Τότε το σύνολο*

$$\{p \in \mathbb{P} \mid p \equiv a \,(mod\, m)\}$$

έχει πυκνότητα Dirichlet $\frac{1}{\varphi(m)}$. Ιδιαίτερα υπάρχουν άπειροι πρώτοι αριθμοί p, $p \equiv a \,(mod\, m)$.

Απόδειξη: Έστω $L = \mathbb{Q}(\zeta_m)$. Αν το $\sigma \in \mathrm{Gal}\left(L/\mathbb{Q}\right)$ ορίζεται από $\sigma(\zeta_m) = \zeta_m^a$ όπου $(a, m) = 1$, τότε (δες [2], σελίδα 146) έχουμε

$$\left[\frac{L/Q}{p\mathbb{Z}}\right] = \sigma \iff p \equiv a \,(\mathrm{mod}\, m).$$

Το πόρισμα είναι τώρα άμεση συνέπεια του θεωρήματος 4.2.4. □

Ο σκοπός μας είναι να γενικεύσουμε το θεώρημα 4.2.4 για επεκτάσεις του Galois όχι κατ' ανάγκη αβελιανές.

4.3 Το Θεώρημα πυκνότητας του Čebotarev.

Έστω L/K μία επέκταση του Galois αλγεβρικών σωμάτων αριθμών, $G := \mathrm{Gal}(L/K)$. Έστω $P \in \mathbb{P}(K)$ και $Q \in \mathbb{P}(L)$, $Q|P$. Αν $\sigma \in G$ τότε, ως γνωστό,

$$\left[\frac{L/K}{\sigma(Q)}\right] = \sigma \left[\frac{L/K}{Q}\right] \sigma^{-1}.$$

Επομένως, όταν το Q διατρέχει όλα τα πρώτα ιδεώδη του L τέτοια ώστε $Q|P$ όπου P μη διακλαδιζόμενο πρώτο ιδεώδες του K, τότε τα $\left[\frac{L/K}{Q}\right]$ διατρέχουν μία **κλάση συζυγίας** της G. Η κλάση αυτή συζυγίας θα λέγεται **σύμβολο του Artin στο** P και θα συμβολίζεται

(καταχρηστικά) πάλι με $\left[\frac{L/K}{P}\right]$.

Αν ${}^{L}\!/_{K}$ αβελιανή τότε το σύμβολο του Artin στο P είναι το γνωστό (μονοσύνολο !) $\left[\frac{L/K}{P}\right]$ (ο αυτομορφισμός του Forbenius στο P).

Έστω τώρα C μια κλάση συζυγίας της G με $c = \#C$. Θα αποδείξουμε το ακόλουθο

Θεώρημα 4.3.1 (Θεώρημα πυκνότητας του Čebotarev) *Αν*

$$\mathcal{A}_{{}^{L}\!/_{K},C} \;=\; \left\{ P \in \mathbb{P}(K) \;\middle|\; P \text{ μη διακλαδιζόμενο στην } {}^{L}\!/_{K} \text{ και } \left[\frac{L/K}{P}\right] = C \right\}$$

τότε το σύνολο $\mathcal{A}_{{}^{L}\!/_{K},C}$ έχει πυκνότητα Dirichlet

$$\delta(\mathcal{A}_{{}^{L}\!/_{K},C}) \;=\; \frac{c}{n}.$$

Απόδειξη: (McCluer, Acta Arithmetica, XV, 1969, 45-48)

Κατ' άρχήν αποδεικνύουμε το ακόλουθο

Λήμμα 4.3.2 *Έστω $Q \in \mathbb{P}(L)$, $Q \cap K = P$ και $e(Q/P) = 1$. Έστω M ενδιάμεσο σώμα $K \subseteq M \subseteq L$ τέτοιο ώστε* **κάθε** *$\mathcal{U} \in \mathbb{P}(M)$, $\mathcal{U} \cap K = P$,* **αδρανεί** *στην ${}^{L}\!/_{M}$. Έστω $\left[\frac{L/K}{Q}\right] = \sigma$. Τότε υπάρχουν $[Z_G(\sigma) : H]$ πρώτα ιδεώδη $\mathcal{U}$, $\mathcal{U} \,|\, P$ στην ${}^{M}\!/_{K}$ τέτοια ώστε $\left[\frac{M/K}{\mathcal{U}}\right] = \sigma$.*

($Z_G(\sigma)$ είναι ο centralizer του σ στην G και $H = \langle\sigma\rangle$.)

Απόδειξη του λήμματος: Έστω $\mathcal{U} \in \mathbb{P}(M)$, $\mathcal{U} \,|\, P$. Επειδή το $\mathcal{U}$ αδρανεί στην ${}^{L}\!/_{M}$ αρκεί να δείξουμε ότι

$$\exists\ [Z_G(\sigma) : H],\ Q \in \mathbb{P}(L),\ Q \,|\, P \text{ τέτοιο ώστε } \left[\frac{L/K}{Q}\right] = \sigma.$$

Κάθε τέτοιο ιδεώδες είναι της μορφής τQ, $\tau \in G$.

Τώρα

$$\left[\frac{L/K}{\tau(Q)}\right] = \sigma \iff \tau\sigma\tau^{-1} = \sigma \iff \tau \in Z_G(\sigma).$$

Από την άλλη μεριά

$$\tau_1(Q) = \tau_2(Q) \iff \tau_1\tau_2^{-1}(Q) = Q \iff \tau_1\tau_2^{-1} \in G_Z(Q/P).$$

Αλλά το P είναι μη διακλαδιζόμενο στην L/K, συνεπώς

$$G_Z(Q/P) \;=\; \left\langle \left[\frac{L/K}{Q}\right] \right\rangle \;=\; \langle\sigma\rangle \;=\; H.$$

Επομένως

$$\tau_1(Q) = \tau_2(Q) \iff \tau_1\tau_2^{-1} \in H$$

και συνεπώς υπάρχουν $[Z_G(\sigma) : H]$ τέτοια Q. □

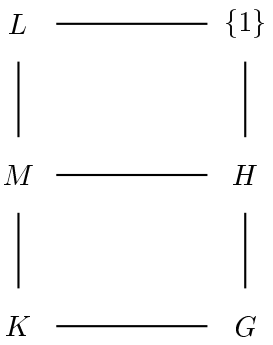
Προχωρούμε τώρα στην απόδειξη του θεωρήματος (4.3.1).

Αρκεί να αποδείξουμε ότι

$$\sum_{\left[\frac{L/K}{P}\right]=C} \frac{1}{NP^s} = -\frac{c}{n}\log(s-1) + O(1)$$

καθώς $s \to 1^+$.

Διαλέγουμε ένα $\sigma \in C$ και έστω $H = \langle\sigma\rangle \leq G$. Αν M το σώμα σταθερών στοιχείων της H τότε L/M κυκλική με $\mathrm{Gal}\left(L/M\right) = H$.



Επομένως, το Θεώρημα του Dirichlet (Θεώρημα 4.2.4) μας δίνει

$$\sum_{\left[\frac{L/M}{\mathcal{U}}\right]=\sigma} N\mathcal{U}^{-s} = -[H:1]^{-1}\cdot\log(s-1) + O(1)$$

όπου $\mathcal{U} \in \mathbb{P}(M)$ και $s \to 1^+$. Τώρα αν $f(\mathcal{U}/P) = 1$ τότε $N\mathcal{U} = NP$. Επειδή για $\mathcal{U} \in \mathbb{P}(M)$ με $f(\mathcal{U}/P) \neq 1$, τότε $\sum_{\mathcal{U}} \frac{1}{(N\mathcal{U})^s} = O(1)$ καθώς $s \to 1^+$, έχουμε

$$\sum_{\substack{\left[\frac{L/M}{\mathcal{U}}\right]=\sigma \\ f(\mathcal{U}/P)=1}} NP^{-s} = -[H:1]^{-1}\cdot\log(s-1) + O(1)$$

καθώς $s \to 1^+$.

Τώρα ισχυρίζομαι ότι το M πληρεί τις υποθέσεις του λήμματος (4.3.2) για κάθε $\mathcal{U} \in \mathbb{P}(M)$,

$\mathcal{U} \cap K = P$. Πράγματι αν $\left[\frac{L/M}{\mathcal{U}}\right] = \sigma$ τότε

$$G_Z\left(Q/\mathcal{U}\right) \;=\; \langle\sigma\rangle \;=\; H,$$

οπότε $[H : G_Z(Q/\mathcal{U})] = 1$ συνεπάγεται ότι υπάρχει **ακριβώς** ένα $Q \in \mathbb{P}(L)$ τέτοιο ώστε $Q \,|\, \mathcal{U}$ στην L/M. Επομένως από το λήμμα 4.3.2 συνεπάγεται

$$[Z_G(\sigma) : H] \cdot \sum_{\substack{\left[\frac{L/K}{P}\right]=C \\ f_P=1}} NP^{-s} \;=\; -[H:1]^{-1}\log(s-1) + O(1)$$

καθώς $s \to 1^+$, διότι $\left[\frac{L/M}{\mathcal{U}}\right] = \sigma \iff \left[\frac{L/K}{P}\right] = C$.
Επειδή (όπως και πιο μπροστά) το άθροισμα για $f_P > 1$ είναι της τάξης $O(1)$ έχουμε

$$\sum_{\left[\frac{L/K}{P}\right]=C} NP^{-s} \;=\; -\frac{1}{[Z_G(\sigma) : H][H:1]}\log(s-1) + O(1)$$

με $s \to 1^+$. Η σταθερά τέλος γράφεται

$$\frac{1}{[Z_G(\sigma) : H][H:1]} \;=\; \frac{1}{[Z_G(\sigma) : 1]} \;=\; \frac{[G : Z_G(\sigma)]}{[G:1]} \;=\; \frac{c}{n}. \quad \square$$

Παρατήρηση: Με μεγαλύτερο κόπο θα μπορούσε κανείς να αποδείξει ότι για $x \in \mathbb{R}$, αν

$$N_{\mathcal{A}_{L/K,C}}(x) = \#\left\{P \in \mathbb{P}(K) \;\middle|\; P \in \mathcal{A}_{L/K,C} \;\text{ με }\; N_{K/Q}(P) \le x\right\}$$

τότε

$$N_{\mathcal{A}_{L/K,C}}(x) \;=\; \left(\frac{c}{n} + o(1)\right) \cdot \frac{x}{\log x}.$$

Παράδειγμα: Έστω L/K **κυβική, όχι κανονική** επέκταση αλγεβρικών σωμάτων αριθμών. Αν $P \in \mathbb{P}(K)$ μή-διακλαδιζόμενο στην L/K τότε έχουμε τρείς δυνατότητες ανάλυσης σε γινόμενο πρώτων ιδεωδών στο L.

(1) $PS = Q_1Q_2Q_3$, με $f_i = f\left(Q_i/P\right) = 1$ για $i = 1,2,3$,

(2) $PS = Q_1Q_2$, με $f_1 = f\left(Q_1/P\right) = 1$, $f_2 = f\left(Q_2/P\right) = 2$,

(3) $PS = Q$, με $f = f\left(Q/P\right) = 3$.

Θέλουμε να υπολογίσουμε την πυκνότητα των πρώτων ιδεωδών P του K σε κάθε μία από τις παραπάνω περιπτώσεις. Έστω N η **κανονική θήκη** της επέκτασης L/K. Η N/K είναι κανονική επέκταση βαθμού 6 με ομάδα Galois την ομάδα S_3. Θα μελετήσουμε την ανάλυση του P στο N. Θυμόμαστε ότι τα πρώτα ιδεώδη του N που διαιρούν το P έχουν όλα τον ίδιο βαθμό. Έτσι αν P ανήκει στην περίπτωση (1), τότε η

$$(1') \quad PR_N = Q'_1 Q'_2 \dots Q'_6 \quad \text{με } f\left(Q'_i/P\right) = 1 \text{ για κάθε } i = 1,2,3,4,5,6, \quad \text{ή}$$
$$(1'') \quad PR_N = Q'_1 Q'_2 Q'_3 \quad \text{με } f\left(Q'_i/P\right) = 2 \text{ για κάθε } i = 1,2,3.$$

Η περίπτωση $(1'')$, λόγω του λήμματος 4.1.9, **δεν** μπορεί να συμβαίνει. Αν τώρα P ανήκει στην περίπτωση (2), θα πρέπει να έχουμε

$$(2') \quad PR_N = Q_2 Q'_1 Q'_2 \quad \text{με } f_1 = f\left(Q'_1/P\right) = f\left(Q'_2/P\right) = 2 \quad \text{και} \quad Q_1 R_N = Q'_1 Q'_2$$

(αφού θα πρέπει όλοι οι βαθμοί να είναι ίδιοι).
Αν P ανήκει στη περίπτωση (3) έχουμε:

$$(3') \quad PR_N = Q \quad \text{με } f(Q/P) = 6, \quad \text{ή}$$
$$(3'') \quad PR_N = Q'_1 Q'_2 \quad \text{με } f_i = f(Q'_i/P) = 3 \text{ για κάθε } i = 1,2.$$

Η $(3')$ δεν μπορεί να συμβεί διότι θα είχαμε στην S_3 ένα στοιχείο τάξης 6, το $\left[\frac{N/K}{Q}\right]$, άτοπο. Άρα ισχύει η $(3'')$.
Τώρα θυμόμαστε ότι η τάξη του $\left[\frac{N/K}{Q'}\right]$ είναι ίση με το βαθμό $f(Q'/P)$. Επομένως για κάθε Q' του $\mathbb{P}(N)$, $Q' \mid P$, έχουμε $\left[\frac{N/K}{Q'}\right]$ είναι στοιχείο τάξης $1,2,3$ ανάλογα με τις τρείς περιπτώσεις (1), (2) ή (3).

Στην S_3 υπάρχει μόνο ένα στοιχείο τάξης 1, υπάρχουν δύο στοιχεία τάξης 2, ενώ υπάρχουν τρία στοιχεία τάξης 3. Επομένως από το θεώρημα του Čebotarev προκύπτει ότι οι αντίστοιχες πυκνότητες είναι $\frac{1}{6}, \frac{1}{2}, \frac{1}{3}$.

Κεφάλαιο 5

Στοιχεία θεωρίας κλάσεων σωμάτων

5.1 Η απεικόνιση του Artin και η προβληματική της θεωρίας κλάσεων σωμάτων.

Έστω L/K **αβελιανή** επέκταση αλγεβρικών σωμάτων αριθμών, $\mathfrak{m}$ ένα **ακέραιο** ιδεώδες του K το οποίο περιέχει όλα τα πρώτα ιδεώδη του K που διακλαδίζονται στο L, δηλαδή, αν P διακλαδίζεται στο L τότε $P|\mathfrak{m}$. Με $I_K^{\mathfrak{m}}$ θα συμβολίζουμε την υποομάδα της I_K

$$I_K^{\mathfrak{m}} = \left\{ A \in I_K \;\middle|\; A \text{ πρώτο προς το } \mathfrak{m} \right\}.$$

Για κάθε $P \in \mathbb{P}(K)$, $P \in I_K^{\mathfrak{m}}$, μπορούμε να ορίσουμε το σύμβολο του Artin $\left[\frac{L/K}{P}\right]$, δηλαδή έχουμε κατ' άρχήν μία απεικόνιση

$$\varphi_{L/K} \;:\; \mathbb{P}(K) \cap I_K^{\mathfrak{m}} \longrightarrow G = \mathrm{Gal}(L/K)$$

όπου

$$\varphi_{L/K}(P) = \left[\frac{L/K}{P}\right].$$

Την επεκτείνουμε πολλαπλασιαστικά σ' όλο το $I_K^{\mathfrak{m}}$. Έτσι αν $A \in I_K$ και

$$A = \prod_{P \in \mathbb{P}(K)} P^{\nu_P(A)}$$

τότε

$$\varphi_{L/K}(A) \;:=\; \prod_{P \in \mathbb{P}(K)} \varphi_{L/K}(P)^{\nu_P(A)}.$$

Ορισμός 5.1.1 *Η απεικόνιση*

$$\varphi_{L/K}(A) \ : \ I_K^{\mathfrak{m}} \longrightarrow G = Gal(L/K)$$

λέγεται **απεικόνιση του Artin** *της* L/K.

Σημειώνουμε ότι ορίζεται μόνο για ακέραια ιδεώδη του K μη διακλαδιζόμενα στο L.

Θεώρημα 5.1.2 *Η απεικόνιση του Artin είναι* **επιμορφισμός** *ομάδων.*

Απόδειξη: Εξ ορισμού η $\varphi_{L/K}$ είναι ομομορφισμός ομάδων. Έστω

$$H := \varphi_{L/K}\,(I_K^{\mathfrak{m}}) < G$$

και F το σώμα των σταθερών στοιχείων που αντιστοιχεί στην H.

$$\begin{array}{ccc} L & \longleftrightarrow & \{1\} \\ | & & | \\ F & \longleftrightarrow & H \\ | & & | \\ K & \longleftrightarrow & G(L/K) \end{array}$$

Έστω $P \in \mathbb{P}(K) \cap I_K$. Ισχυρίζομαι ότι

$$\text{Αν} \quad \varphi_{L/K}(P) \in H \quad \text{τότε} \quad P \ \text{αναλύεται πλήρως στο} \ F. \tag{5.1}$$

Απόδειξη της (5.1): Αν $\varphi_{L/K}(P) \in H$ τότε συνεπάγεται ότι

$$\begin{aligned} & \forall \alpha \in F \quad \varphi_{L/K}(P)(\alpha) = \alpha \\ \Longrightarrow \quad & \forall \alpha \in F \quad \alpha \equiv \alpha^{N_{K/Q}(P)} \bmod Q, \ \text{όπου} \ Q \in \mathbb{P}(L), \ Q \cap K = P \\ \Longrightarrow \quad & \forall \alpha \in F \quad \alpha \equiv \alpha^{N_{K/Q}(P)} \bmod Q_F, \ \text{όπου} \ Q_F \in \mathbb{P}(F), \ Q \cap F = Q_F, \end{aligned}$$

οπότε

$$\#(R_F/Q_F) \ \leq \ N_{K/Q}(P).$$

Από την άλλη μεριά είναι προφανές ότι

$$\#(R_{_F}/Q_{_F}) \;=\; N_{_{F\!/\!Q}}(Q_{_F}) \;=\; N_{_{K\!/\!Q}}(P)^{f(Q_{_F}/P)} \;\geq\; N_{_{K\!/\!Q}}(P)$$

(Δες [2], σελίδα 119). Συνεπώς

$$N_{_{F\!/\!Q}}(Q_{_F}) = N_{_{K\!/\!Q}}(P),$$

δηλαδή

$$f = f(Q_{_F}/P) = 1.$$

Επειδή και $e = e(Q_{_F}/P) = 1$ άρα P αναλύεται πλήρως στο F και επομένως ισχύει η (5.1). Τώρα από το $\mathbb{P}(K) \cap I_K$ λείπουν μόνο πεπερασμένου πλήθους πρώτα ιδεώδη του K, δηλαδή

$$\delta\left(\mathbb{P}(K) \cap I_K^{\mathfrak{m}}\right) = 1.$$

Από την άλλη μεριά, λόγω της (5.1),

$$\varphi_{_{L\!/\!K}}(P) \in H \quad \Longrightarrow \quad f = f(Q_{_F}/P) = 1,$$

οπότε το Θεώρημα 4.1.6 μάς δίνει

$$\delta\left(\left\{P \in \mathbb{P}(K) \cap I_K^{\mathfrak{m}} \;\middle|\; P \text{ αναλύεται πλήρως στο } F\right\}\right) \;=\; 1.$$

Επομένως

$$\begin{aligned} 1 \quad &= \quad \delta\left(\mathbb{P}(K) \cap I_K^{\mathfrak{m}}\right) \\ &= \quad \delta\left(\left\{P \in \mathbb{P}(K) \cap I_K^{\mathfrak{m}} \;\middle|\; P \text{ αναλύεται πλήρως στο } F\right\}\right) \\ &\overset{\Theta.\,4.1.7}{=} \quad \frac{1}{(F:K)}, \end{aligned}$$

οπότε

$$\frac{1}{(F:K)} = 1 \;\Longrightarrow\; F = K \;\Longrightarrow\; H = G,$$

συνεπώς ο $\varphi_{_{L\!/\!K}}$ είναι επιμορφισμός. □

Το Θεώρημα 5.1.2 συνεπάγεται ότι

$$\begin{aligned} I_K^{\mathfrak{m}}\!/_{\operatorname{Ker}\varphi_{_{L\!/\!K}}} \quad &\cong \quad G(L/K), \\ A\,\operatorname{Ker}\varphi_{_{L\!/\!K}} \quad &\longmapsto \quad \varphi_{_{L\!/\!K}}(A). \end{aligned}$$

Παράδειγμα:

Έστω $K = \mathbb{Q}$ και $L = \mathbb{Q}(\zeta_m)$, $\zeta_m = e^{2\pi i/m}$ και $\mathfrak{m} = (m) = mR_{_L}$. Αν , A, ακέραιο ιδεώδες του $\mathbb{Q}$ πρώτο προς το $\mathfrak{m}$, $A = \mathbb{Z}\alpha$, $\alpha \in \mathbb{Z}$, $\alpha > 0$, τότε $\varphi_{_{L/K}}(A) = \sigma_\alpha$.

Από τα παραπάνω προκύπτει ότι η δομή της ομάδος $G(L/K)$, μας είναι γνωστή, αν γνωρίζουμε τον πυρήνα $\operatorname{Ker}\varphi_{_{L/K}}$. Ποιά όμως είναι η σημασία του πυρήνα; Μας δίνεται στο επόμενο

Θεώρημα 5.1.3 (Νόμος Ανάλυσης) *Έστω* $^{L}\!/_{K}$ **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών. Τότε ισχύει:*
Το $P \in \mathbb{P}(K) \cap I_K^{\mathfrak{m}}$ *έχει στο* L *την ανάλυση*

$$PR_{_L} = Q_1 Q_2 \dots Q_r$$

όπου $rf = n = (L : K)$ *με* $f = ord\Big(P \cdot Ker\,\varphi_{_{L/K}}\Big)$.

Απόδειξη: Ως γνωστόν,

$$\begin{aligned} f &= \operatorname{ord}\big(G_{_Z}(Q_1/P)\big) = \operatorname{ord}\big(\langle\varphi_{_{L/K}}(P)\rangle\big) \\ &= \operatorname{ord}(\varphi_{_{L/K}}(P)) = \operatorname{ord}\big(P \operatorname{Ker}\varphi_{_{L/K}}\big). \quad \square \end{aligned}$$

Παράδειγμα:

$K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_m)$, $\mathfrak{m} = \langle m\rangle = mR_{_L}$

$$K_m = \operatorname{Ker}\varphi_{_{L/K}} = \big\{x \;\big|\; x \in \mathbb{Z}\,,\; x \equiv 1 \bmod m\,,\; x > 0\big\}$$

Από το Θεώρημα 5.1.3 έχουμε ότι για κάθε πρώτο $p \nmid m$

$$f = \text{ ord } (\langle p\rangle K_m) = \text{ ord } (p \bmod m)$$

(Δες [2], σελίδα 184).
Αποδείξαμε ήδη τα εξής σημαντικά:

1. Ο $\operatorname{Ker}\varphi_{_{L/K}}$ **καθορίζει την** $G(L/K)$.
2. Ο $\operatorname{Ker}\varphi_{_{L/K}}$ **καθορίζει το Νόμο Ανάλυσης**.

Παρατήρηση 5.1.4 *Η* **αβελιανή** *επέκταση* L/K *καθορίζεται* **μονοσήμαντα** *από το σώμα* K *και τον πυρήνα* $Ker\,\varphi_{_{L/K}}$.

Απόδειξη: Το σύνολο $\mathrm{Ker}\,\phi_{L/K} \cap \mathbb{P}(K)$ περιέχει τα πρώτα ιδεώδη του K που αναλύονται πλήρως στο K εκτός από πεπερασμένου πλήθους, συνεπώς

$$\mathrm{Ker}\,\varphi_{L/K} \cap \mathbb{P}(K) \doteq \mathcal{A}_{L/K}.$$

Το συμπέρασμα τώρα είναι συνέπεια του λήμματος 4.1.12. □

Εντελως φυσιολογικά προκύπτει τώρα το **ερώτημα**: Έστω ότι L/K διατρέχει **όλες** τις **αβελιανές** επεκτάσεις του K. Ποιές υποομάδες της $I_K^{\mathfrak{m}}$ εμφανίζονται σαν $\mathrm{Ker}\,\varphi_{L/K}$ για κάποιο L;

Κατ' αρχήν θα "εκτιμήσουμε" τις $\mathrm{Ker}\,\varphi_{L/K}$ από κάτω.

Ορισμός 5.1.5 *Έστω L/K επέκταση αλγεβρικών σωμάτων αριθμών $\mathbb{Q} \in \mathbb{P}(K)$, $P = Q \cap K$. Ορίζουμε*

$$N_{L/K}(Q) := P^{f(Q/P)}$$

σχετική norm του Q ως προς K *και επεκτείνουμε πολλαπλασιαστικά.*

Για ιδιότητες της σχετικής norm παραπέμπουμε τον αναγνώστη στο βιβλίο [42], σελίδες 140-142. Εδώ απλά αναφέρουμε ότι ισχύει

$$N_{L/K}(\alpha\, R_L) = R_K\, N_{L/K}(\alpha) \quad \text{για κάθε } \alpha \in L.$$

Ορισμός 5.1.6

$$I_L^{\mathfrak{m}} := \left\{ A \in I_L \;\middle|\; \text{πρώτο προς το } R_L \cdot \mathfrak{m} \right\}$$

όπου $\mathfrak{m}$ ακέραιο ιδεώδες του K το οποίο περιέχει όλα τα πρώτα ιδεώδη του K που διακλαδίζονται στο L.

Θεώρημα 5.1.7 *Έστω L/K* **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών. Τότε ισχύει*

$$I_K^{\mathfrak{m}} \supseteq Ker\,\varphi_{L/K} \supseteq N_{L/K}(I_L^{\mathfrak{m}}).$$

Απόδειξη: Αρκεί να δείξουμε ότι:

$$\forall\, Q \in \mathbb{P}(L) \cap I_L^{\mathfrak{m}} \quad \text{ισχύει} \quad \varphi_{L/K}\big(N_{L/K}(Q)\big) = i\, d_L.$$

Πράγματι αν $P = Q \cap K$ τότε, από τον ορισμό, έχουμε

$$N_{L/K}(Q) \;=\; P^{f(Q/P)}.$$

Από την άλλη μεριά,

$$f(Q/P) \;=\; \#G_{_Z}(Q/P) \;=\; \mathrm{ord}\big(\varphi_{_{L/K}}(P)\big)$$

$$\begin{aligned}\Longrightarrow \varphi_{_{L/K}}\big(N_{_{L/K}}(Q)\big) \;&=\; \varphi_{_{L/K}}(P)^{f(Q/P)}\\ &=\; \varphi_{_{L/K}}(P)^{\,\mathrm{ord}\varphi_{_{L/K}}(P)} \;=\; i\,d_{_L}. \quad \square\end{aligned}$$

Στη συνέχεια θα προσπαθήσουμε να προσδιορίσουμε ακριβέστερα τον πυρήνα $\mathrm{Ker}\,\varphi_{_{L/K}}$. Το σύνολο

$$S^{+}_{\mathfrak{m}} \;:=\; H^{+}_{\mathfrak{m}} \;=\; \Big\{\langle\alpha\rangle = \alpha R_{_K} \;\Big|\; \alpha=\frac{\alpha_1}{\alpha_2},\ \alpha_i\in R_{_K},\ \alpha_i \text{ πρώτοι προς το } \mathfrak{m},\ \alpha_1\equiv\alpha_2\ (\mathrm{mod}\,\mathfrak{m}) \ \text{ και } \ \alpha\gg 0\Big\}$$

θα λέγεται **κλάση ακτίνας mod $\mathfrak{m}$** με τη στενή έννοια "engere Strahlklasse mod $\mathfrak{m}$".

Θεώρημα 5.1.8 (Η δεύτερη ανισότητα) *Έστω $^{L}\!/_{K}$ αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών και $\mathfrak{m}$ όπως πιο μπροστά. Αν οι εκθέτες των πρώτων ιδεωδών που περιέχονται στην ανάλυση του $\mathfrak{m}$ είναι αρκετά μεγάλοι, τότε*

$$Ker\,\varphi_{_{L/K}} \;\supseteq\; S^{+}_{\mathfrak{m}}.$$

Ιδιαίτερα, λόγω του θεωρήματος 5.1.7, έχουμε

$$\Big[I^{\mathfrak{m}}_{K} \;:\; N_{_{L/K}}\big(I^{\mathfrak{m}}_{L}\big)\cdot S^{+}_{\mathfrak{m}}\Big] \;\geq\; (L:K).$$

Πράγματι

$$I^{\mathfrak{m}}_{K} \;\supseteq\; Ker\,\varphi_{_{L/K}} \;\supseteq\; N_{_{L/K}}\big(I^{\mathfrak{m}}_{L}\big)\cdot S^{+}_{\mathfrak{m}}$$

και

$$\Big[I^{\mathfrak{m}}_{K} \;:\; Ker\,\varphi_{_{L/K}}\Big] \;=\; \big|G(L/K)\big| \;=\; (L:K).$$

Απόδειξη: Η απόδειξη ξεφεύγει κάπως από το στόχο του παρόντος βιβλίου. Χρησιμοποιούνται θεωρία συνομολογίας ομάδων και p-αδικές μέθοδοι. Ως εκ τούτου παραλείπεται. Ο ενδιαφερόμενος αναγνώστης μπορεί να δεί την απόδειξη σε οποιοδήποτε βιβλίο θεωρίας κλάσεων σωμάτων.

Ισχύει όμως και το

Θεώρημα 5.1.9 (η πρώτη ανισότητα) *Έστω* L/K **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών και* $\mathfrak{m}$ *όπως πριν. Τότε ισχύει*

$$\left[I_K^{\mathfrak{m}} \ : \ N_{L/K}\left(I_L^{\mathfrak{m}}\right) \cdot S_{\mathfrak{m}}^{+}\right] \leq (L:K).$$

Απόδειξη: Το θεώρημα θα αποδειχθεί στην επόμενη παράγραφο.

Παρατηρήσεις:

1. Δεν έχουμε θέσει κανένα περιορισμό στους **εκθέτες** των πρώτων ιδεωδών που διαιρούν το $\mathfrak{m}$.

2. Η **πρώτη ανισότητα** είναι σωστή και στην περίπτωση μη-αβελιανής επέκτασης του Galois. (Στην απόδειξη σπουδαίο ρόλο παίζει το θεώρημα του Ševotare).

Σαν άμεση συνέπεια των παραπάνω έχουμε το:

Θεμελιώδες Θεώρημα 5.1.10 *Έστω* L/K **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών και* $\mathfrak{m}$ *όπως παραπάνω. Αν οι εκθέτες των πρώτων ιδεωδών που εμφανίζονται στην ανάλυση του είναι αρκετά μεγάλοι τότε*

$$Ker\,\varphi_{L/K} \ = \ N_{L/K}\left(I_L^{\mathfrak{m}}\right) \cdot S_{\mathfrak{m}}^{+}.$$

Συνεπώς έχουμε αποδείξει το εξής: Έστω L/K αβελιανή επέκταση αλγεβρικών σωμάτων αριθμών. Υπάρχει ακέραιο ιδεώδες του K $\mathfrak{m}$ τέτοιο ώστε:

1. Αν P διακλαδίζεται στο L τότε $P \,|\, \mathfrak{m}$.

2. $I_K^{\mathfrak{m}} \ \supseteq \ \mathrm{Ker}\,\varphi_{L/K} \ \supseteq \ S_{\mathfrak{m}}^{+}$.

Αντίστροφα τώρα: Έστω $\mathfrak{m} \in I_K$ ακέραιο και $\mathcal{U}$ υποομάδα της $I_K^{\mathfrak{m}}$ τέτοια ώστε

$$I_K^{\mathfrak{m}} \ \supseteq \ \mathcal{U} \ \supseteq \ S_{\mathfrak{m}}^{+}.$$

Υπάρχει **αβελιανή** επέκταση L/K αλγεβρικών σωμάτων αριθμών με τις ιδιότητες

$$\begin{cases} (1) & \text{Αν } P \text{ διακλαδίζεται στο } L \text{ τότε } P \,|\, \mathfrak{m} \quad \text{και} \\ (2) & \mathrm{Ker}\,\varphi_{L/K} = \mathcal{U}\ ; \end{cases} \tag{5.2}$$

Παρατήρηση: Αν υπάρχει τέτοιο L τότε, λόγω της παρατήρησης 5.1.4, αυτό είναι **μοναδικό**.

Ορισμός 5.1.11 *Μία* **αβελιανή** *επέκταση* L/K *αλγεβρικών σωμάτων αριθμών με τις ιδιότητες (5.2) θα λέγεται* **σώμα κλάσεων** *της* $\mathcal{U}$.

Ορισμός 5.1.12 *Κάθε υποομάδα* $\mathcal{U}$ *της* $I_K^{\mathfrak{m}}$ *όπου* $I_K^{\mathfrak{m}} \supseteq \mathcal{U} \supseteq S_{\mathfrak{m}}^+$ *για κατάλληλα εκλεγμένο ακέραιο ιδεώδες* $\mathfrak{m} \in I_K$ *θα λέγεται* **ισοδυναμομάδα** *της* I_K *(Kongruenzuntergruppe von* I_K*).*

Επομένως το θεμελιώδες θεώρημα 5.1.10 γίνεται

Θεμελιώδες Θεώρημα 5.1.10′ *Κάθε* **αβελιανή** *επέκταση* L/K *αλγεβρικών σωμάτων αριθμών είναι σώμα κλάσεων μιάς ισοδυναμομάδας της* I_K.

Ισχύει όμως και το αντίστροφο:

Θεμελιώδες Θεώρημα 5.1.13 *Σε κάθε ισοδυναμομάδα του* I_K *υπάρχει (αντιστοιχεί)* **ακριβώς** *ένα σώμα κλάσεων.*

Απόδειξη: Κατ′ αρχήν αρκεί να δείξουμε την ύπαρξη σώματος κλάσεων ως προς την $S_{\mathfrak{m}}^+$, διότι ισχύει το

Θεώρημα 5.1.14 *Έστω* $\mathcal{U}, \mathcal{U}_0$ *ισοδυναμομάδες της* I_K *με*

$$I_K^{\mathfrak{m}} \supseteq \mathcal{U}_0 \supseteq \mathcal{U} \supseteq S_{\mathfrak{m}}^+$$

και έστω L *σώμα κλάσεων της* $\mathcal{U}$. *Τότε το σώμα σταθερών στοιχείων της* $\varphi_{L/K}(\mathcal{U}_0)$, *έστω* L_0, *είναι σώμα κλάσεων της* $\mathcal{U}_0$.

Απόδειξη: Αρκεί να δείξουμε ότι

$$\operatorname{Ker} \varphi_{L_0/K} \;=\; \mathcal{U}_0. \tag{5.3}$$

Ισχυρίζομαι ότι για κάθε $A \in I_K^{\mathfrak{m}}$ ισχύει

$$\varphi_{L_0/K}(A) \;=\; \varphi_{L/K}(A)\,\Big|_{L_0}\,. \tag{5.4}$$

Απόδειξη της (5.4): Αρκεί να περιοριστούμε σε πρώτα ιδεώδη $P \in \mathbb{P}(K) \cap I_K^{\mathfrak{m}}$. Πράγματι,

$$\varphi_{L_0/K}(P) \;=\; \left[\frac{L_0/K}{P}\right] \;=\; \left[\frac{L/K}{P}\right]\Big|_{L_0} \;=\; \varphi_{L/K}(P)\,\Big|_{L_0}\,.$$

Η μεσαία ισότητα είναι γνωστή ιδιότητα του συμβολισμού του Artin (δες [2], σελίδα 189). Τώρα προχωρούμε στην απόδειξη της (5.3):

$$\begin{aligned} A \in \operatorname{Ker} \varphi_{L_0/K} &\iff \varphi_{L_0/K}(A) = i\, d_{L_0} \\ &\overset{(5.4)}{\iff} \varphi_{L/K}(A)\Big|_{L_0} = \mathrm{id}_{L_0} \\ &\iff \varphi_{L/K}(A) \in \mathrm{Aut}\,(L/L_0) \\ &\iff \varphi_{L/K}(A) \in \varphi_{L/K}(\mathcal{U}_0) \\ &\iff A \in \mathcal{U}_0 \cdot \operatorname{Ker} \varphi_{L/K} = \mathcal{U}_0\mathcal{U} = \mathcal{U}_0. \end{aligned}$$

Επομένως

$$\operatorname{Ker} \varphi_{L/K} = \mathcal{U}_0. \quad \square$$

Απόδειξη του θεμελιώδους θεωρήματος 5.1.13 στην ειδική περίπτωση $K = \mathbb{Q}$.

Αρκεί να δείξουμε ότι $\forall\, m \in \mathbb{N}$ υπάρχει σώμα κλάσεων του $S^+_{\mathfrak{m}}$ όπου $\mathfrak{m} = \langle m \rangle$.

(1) Ισχυρίζομαι ότι $L = \mathbb{Q}(\zeta_m)$ είναι σώμα κλάσεων της $S^+_{(m)}$. Είναι γνωστό ότι, αν ο p διακλαδίζεται στο L, τότε $p \,\big|\, m$. Τώρα θα δείξουμε ότι

$$(2) \quad \left| \begin{array}{l} \text{Η } \varphi_{L/\mathbb{Q}} : I_{\mathbb{Q}}^{\langle m \rangle} \longrightarrow G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ \qquad\qquad a \longmapsto \varphi_{L/\mathbb{Q}}(a) \\ \text{έχει πυρήνα } \operatorname{Ker} \varphi_{L/\mathbb{Q}} = S^+_{\langle m \rangle}. \end{array} \right.$$

Για την απόδειξη της (2) χρειαζόμαστε την:

$$(3) \quad \left| \begin{array}{l} \text{Αν } \langle x \rangle \in I_{\mathbb{Q}}^m,\ x = \dfrac{x_1}{x_2},\ x_i \in \mathbb{Z},\ x_i \text{ πρώτα πρός το } m \text{ τότε:} \\ \varphi_{L/\mathbb{Q}}(\langle x \rangle) = \sigma_{|x_1|}\sigma_{|x_2|}^{-1}. \end{array} \right.$$

Απόδειξη της (3): Αρκεί να την αποδείξουμε για πρώτο $p \in \mathbb{P}$, $p \nmid m$, το οποίο όμως είναι γνωστό, καθ' όσον

$$\varphi_{L/\mathbb{Q}}(\langle p \rangle) = \sigma_p.$$

Απόδειξη της (2): '$\subseteq$' Έστω ότι $\langle x \rangle = xR_L$ ανήκει στον $\operatorname{Ker} \varphi_{L/\mathbb{Q}}$ και $x = x_1/x_2$ όπως στην (3). Θά έχουμε λοιπόν $\sigma_{|x_1|}\sigma_{|x_2|}^{-1} = 1_{\mathbb{Q}(\zeta_m)} \Rightarrow |x_1| = |x_2| \pmod m$, δηλαδή, $\langle x \rangle = xR_L = \left\langle \dfrac{|x_1|}{|x_2|} \right\rangle \in S^+_{(m)}$. Τώρα το αντίστροφο '$\supseteq$'. Έστω $\langle x \rangle = xR_L \in S^+_{(m)} \Rightarrow \langle x \rangle = \left\langle \dfrac{|x_1|}{|x_2|} \right\rangle$ όπου $x_1, x_2 > 0$, $x_1 \equiv x_2 \pmod m$. Λόγω της (3) έχουμε:

$$\varphi_{L/\mathbb{Q}}(\langle x \rangle) = \sigma_{x_1}\sigma_{x_2}^{-1} = 1_{\mathbb{Q}(\zeta_m)}$$

διότι $x_1 \equiv x_2 \pmod m$, και άρα $\langle x \rangle \in \operatorname{Ker} \varphi_{L/\mathbb{Q}}$. $\square$

Παρατηρήσεις: Αν $K = \mathbb{Q}$ κυρίαρχο ρόλο παίζει η (απλά) περιοδική **εκθετική συνάρτηση**.

Αν K είναι τετραγωνικό μιγαδικό τότε σπουδαίο ρόλο παίζουν οι **modular συναρτήσεις** (διπλά περιοδικές).

Παραδείγματος χάριν, για $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, d ελεύθερο τετραγώνου, $d \equiv 3 \pmod 4$, $\mathfrak{m} = \langle m \rangle$, $m \in \mathbb{N}$, τότε το σώμα κλάσεων της $S^+_{\mathfrak{m}}$ είναι το

$$K\left(j(\sqrt{-d}),\ \frac{\mathfrak{p}(\frac{1}{m}|\mathbb{Z}+\mathbb{Z}\sqrt{-d})}{\Delta(\sqrt{-d})} g_2(\sqrt{-d})\cdot g_3(\sqrt{-d})\right)$$

όπου:

$$\frac{\mathfrak{p}(\frac{1}{m}|\mathbb{Z}+\mathbb{Z}\sqrt{-d})}{\Delta(\sqrt{-d})}\cdot g_2(\sqrt{-d})\cdot g_3(\sqrt{-d})$$

m-στό σημείο διαίρεσης μιας ελλειπτικής καμπύλης και $j(\sqrt{-d})$ είναι η συνεισφορά μέσω των συντελεστών της ελλειπτικής καμπύλης.

5.2 Απόδειξη της πρώτης ανισότητας για επεκτάσεις του Galois: L/K

Θεώρημα 5.2.1 *Έστω $\mathfrak{m}$ ακέραιο ιδεώδες του K και $U \leq I_K^{\mathfrak{m}}$ με $(I_K^{\mathfrak{m}} : U) < \infty$ και την ακόλουθη ιδιότητα:*

$$\exists \lambda \in \mathbb{R}^+ \quad \text{τέτοιο ώστε γιά κάθε } \mathfrak{k} \in {}^{I_K^{\mathfrak{m}}}\!/_{U}$$

να ισχύει ότι

$$A_{\mathfrak{k}}(t) = \#\{A \in \mathfrak{k} | A \text{ακέραιο}, N(A) \leq t\} \tag{5.5}$$

$$= \lambda t + O(t^{1-\frac{1}{L:K}}), \quad \text{όταν } t \to \infty. \tag{5.6}$$

Για κάθε υποσύνολο S του $\mathbb{P}(K)\bigcap U$, για το οποίο **υπάρχει** *η πυκνότητα του Dirichlet, ισχύει:*

$$\delta(S) \leq \frac{1}{(I_k^{\mathfrak{m}} : U)}.$$

Παρατήρηση 5.2.2 *Οι υποθέσεις του θεωρήματος 5.2.1 ισχύουν για* **κάθε** *υποομάδα U όπου*

$$I_K^{\mathfrak{m}} \supseteq U \supseteq S^+_{\mathfrak{m}}.$$

(Δες Θεώρημα 2.1.19.)

Λήμμα 5.2.3 *Έστω U όπως στο θεώρημα 5.2.1. Για* **κάθε** *χαρακτήρα χ της $I_U^{\mathfrak{m}}/U$ η σειρά του Dirichlet*

$$L(s,\chi) = \sum_{A \text{ ακέραιο}} \frac{\chi(A)}{N(A)^s}, \quad \text{όπου } Re(s) > 1$$

συγκλίνει, *είναι* **διάφορη του μηδενός** *και* **ολόμορφη**. *Εδώ*

$$\chi(A) := \begin{cases} 0, & \text{αν } A \text{ όχι πρώτο προς το } \mathfrak{m} \\ \chi(AU), & \text{αλλιώς.} \end{cases}$$

Αν $\chi \neq \chi_0$, τότε η $L(s,\chi)$ επεκτείνεται ολόμορφα στο ημιεπίπεδο $Re(s) > 1 - \frac{1}{(K:\mathbb{Q})}$.

Απόδειξη: Σύγκλιση και ολομορφία είναι άμεσα συμπεράσματα (όπως ακριβώς το κάναμε πιο μπροστά σε ανάλογες L-σειρές). Το διάφορο του μηδενός είναι άμεση συνέπεια του γεγονότος ότι η $L(s,\chi)$ γράφεται σε μορφή γινομένου Euler.

Τώρα γράφουμε:

$$L(s,\chi) = \sum_{\mathfrak{k} \in I_{K/U}^{\mathfrak{m}}} \chi(\mathfrak{k}) \zeta(s,\mathfrak{k}),$$

όπου

$$\begin{aligned} \zeta(s,\mathfrak{k}) &= \sum_{\substack{A \text{ ακέραιο} \\ A \in \mathfrak{k}}} \frac{1}{N(A)^s} \\ &= \sum_{m=1}^{\infty} \frac{a_m(k)}{m^s} \end{aligned}$$

και

$$a_m(k) = \#\{A \text{ ακέραιο } \in \mathfrak{k} \mid N(A) = m\}.$$

Όπως και στην ζήτα συνάρτηση του Riemann, γράφουμε

$$\zeta(s,\mathfrak{k}) = \lambda \sum_{m=1}^{\infty} \frac{1}{m^s} + \sum_{m=1}^{\infty} \frac{a_m(k) - \lambda}{m^s}$$

Επειδή δε $\chi \neq \chi_0$, έπεται ότι

$$L(s,\chi) = \sum_{\mathfrak{k}} \chi(\mathfrak{k}) \sum_{m=1}^{\infty} \frac{a_m(\mathfrak{k}) - \lambda}{m^s}.$$

Αλλά

$$\begin{aligned}\sum_{m=1}^{M} \lambda - a_m(\mathfrak{k}) &= \lambda M - \#\{A \mid A \text{ ακέραιο}, A \in \mathfrak{k} \text{ και } N(A) \le M\} \\ &= O(M^{1-\frac{1}{(K:\mathbb{Q})}}).\end{aligned}$$

Συνεπώς από το θεώρημα 1.1.2 συνεπάγεται ότι η $L(s,\chi)$ για $\chi \neq \chi_0$ επεκτείνεται ολόμορφα στο ημιεπίπεδο

$$\mathrm{Re}(s) > 1 - \frac{1}{(K:\mathbb{Q})}. \quad \square$$

Απόδειξη του θεωρήματος 5.2.1: Όπως κάναμε και πιο μπροστά, σε ανάλογη περίπτωση,

$$\log\big(L(s,\chi)\big) \;=\; \sum_{\substack{P\in\mathbb{P}(K)\\ P\nmid\mathfrak{m}}} \frac{\chi(P)}{N(P)^s} + O(1), \quad \text{για } s \to 1^+.$$

Επομένως

$$\sum_{\chi} \log L(s,\chi) \;=\; \sum_{\substack{P\in\mathbb{P}(K)\\ P\nmid\mathfrak{m}}} \frac{1}{N(P)^s} \sum_{\chi\in\widehat{(I_K^{\mathfrak{m}}/U)}} \chi(P) + O(1).$$

Το εσωτερικό άθροισμα είναι ίσο προς $(I_K^{\mathfrak{m}} : \mathcal{U})$ αν $P \in \mathcal{U}$ και με μηδέν αλλιώς. Επομένως

$$\sum_{\chi} \log L(s,\chi) \;=\; (I_K^{\mathfrak{m}} : U) \cdot \sum_{\substack{P\in\mathbb{P}(K)\\ P\nmid\mathfrak{m}\\ P\in U}} \frac{1}{N(P)^s} + O(1), \quad \text{για } s \to 1^+ \tag{5.7}$$

Τώρα παίρνουμε s πραγματικό, $s > 1$.

Από το λήμμα 5.2.3 συνεπάγεται ότι η τιμή $L(s,\chi)$ υπάρχει για κάθε $\chi \neq \chi_0$ και $s \to 1^+$

$$\Longrightarrow \quad \log|L(s,\chi)| \;\le\; 0 + O(1), \quad \text{για } s \to 1^+,$$

οπότε, από (5.7), έχουμε

$$\log\big|L(s,\chi_0)\big| \;\ge\; (I_K^{\mathfrak{m}} : U) \sum_{P\in U} \frac{1}{N(P)^s} + O(1).$$

Στη συνέχεια περνούμε στα υπόλοιπα

$$\lim_{s\to 1^+} (s-1)L(s,\chi_0) \;=\; \mathrm{Res}_{s=1}\zeta_K(s) > 0$$

$$\begin{aligned}
&\Longrightarrow \quad \underbrace{\log((s-1)L(s,\chi_0))}_{O(1)} - \log(s-1) \;\geq\; (I_K^{\mathfrak{m}} : U) \sum_{P\in U} \frac{1}{N(P)^s} + O(1), \quad \text{για } s \to 1^+ \\
&\Longrightarrow \quad -\log(s-1) \;\geq\; (I_K^{\mathfrak{m}} : U) \sum_{P\in S} \frac{1}{N(P)^s} + O(1) \\
&\Longrightarrow \quad \frac{1}{(I_K^{\mathfrak{m}} : U)} \;\geq\; \lim_{s\to 1^+} \frac{\displaystyle\sum_{P\in S} \frac{1}{N(P)^s}}{\log(s-1)} \;=\; \delta(S).
\end{aligned}$$

Απόδειξη τώρα της **πρώτης ανισότητας:** Έστω L/K επέκταση του Galois, αλγεβρικών σωμάτων αριθμών,

$$U \;=\; N_{L/K}(I_L^{\mathfrak{m}}) \cdot S_{\mathfrak{m}}^{+},$$

$\mathfrak{m}$ ακέραιο ιδεώδες του K με τις γνωστές ιδιότητες που έχουμε υποθέσει από την αρχή του πέμπτου κεφαλαίου. Ισχυρίζομαι ότι το σύνολο

$$S \;:=\; \left\{ P \in \mathbb{P}(K) \cap I_K^{\mathfrak{m}} \;\middle|\; P \text{ αναλύεται πλήρως στο } L \right\} \;\subseteq\; \mathbb{P}(K) \cap U. \tag{5.8}$$

Αν δεχθούμε την αλήθεια της (5.8) τότε τελειώνουμε ως εξής:

Γνωστό: Το P αναλύεται πλήρως στο L εάν και μόνο εάν

$$\sigma_P = \left[\frac{L/K}{P}\right] \;=\; 1$$

και $\{1\}$ αποτελεί (προφανώς) μία κλάση συζυγίας της G. Το **Θεώρημα Čebotarev** τώρα μας δίνει

$$\delta(S) = \frac{1}{(L:K)}.$$

Από την άλλη μεριά το θεώρημα 5.2.1 συνεπάγεται ότι

$$\begin{aligned}
&\delta(S) \;\leq\; \frac{1}{(I_K^{\mathfrak{m}} : U)} \\
\Longrightarrow \quad &\frac{1}{(L:K)} \;\leq\; \frac{1}{(I_K^{\mathfrak{m}} : U)} \\
\Longrightarrow \quad &(I_K^{\mathfrak{m}} : U) \;\leq\; (L:K). \quad \square
\end{aligned}$$

Ακολουθεί η απόδειξη της (5.8):

Το ότι $P \in S$ συνεπάγεται ότι P αναλύεται πλήρως στο L

$$\begin{aligned}
&\Longrightarrow \quad \exists Q \in \mathbb{P}(L) \text{ τέτοιο ώστε } Q \,\middle|\, P \text{ και } f(Q/P) = 1 \\
&\Longrightarrow \quad N_{L/K}(Q) = P
\end{aligned}$$

και (επειδή $P \nmid \mathfrak{m}$, δηλαδή και $Q \nmid \mathfrak{m}m \implies Q \in I_L^{\mathfrak{m}}$)

$$\implies P = N_{L/K}(Q) \in N_{L/K}(I_L^{\mathfrak{m}}). \quad \square$$

Κεφάλαιο 6

Οι L-σειρές του Artin

6.1 Ορισμός των L-σειρών του Artin

Für die Untersuchung beliebiger, auch nicht Abelscher algebraischer Zahlkörper benötigt man eine Reihe neuer analytischer Funktionen, die mit FROBENIUSschen Gruppencharakteren gebildet sind und im Abelschen Falle mit den gewöhnlichen L-Reihen zusammenfallen. Ihrer Untersurchung sind die folgenden Zeilen gewidmet.

E. Artin, Über eine neue Art von L-Reihen, Abh. Math. Sem. Hamburg **3** (1923), p. 89

Προσπαθώντας να κατανοήσουμε την αριθμητική αλγεβρικών σωμάτων αριθμών και στην περίπτωση **κανονικών**, όχι κατ΄ ανάγκη αβελιανών, επεκτάσεων, σκεπτόμαστε (ο Artin και για μας!) να ορίσουμε L-σειρές, οι οποίες θα γενικεύουν φυσικά τις γνωστές αβελιανές. Ο ορισμός εδώ είναι εντελώς διάφορος των προηγουμένων και η θεωρία αναπτύχθηκε σε τρείς εργασίες του E. Artin. Πρώτη αυτή που μόλις αναφέραμε και επιπλέον οι: Beweis des allgemeinen Reziprozitätsgesetzes, Abh. Math. Sem. Hamburg **5** (1927) και Zur Theorie der L-Reihen mit allgemeinen Gruppencharakterenn Abh. Math. Sem. Hamburg **8** (1931).

Θεμελιώδεις έννοιες για τον ορισμό των L-σειρών του Artin είναι οι θεωρία χαρακτήρων (θεωρία παραστάσεων ομάδων) και ο αυτομορφισμός του Frobenius.

Έστω λοιπόν L/K μία πεπερασμένη επέκταση του Galois αλγεβρικών σωμάτων αριθμών.

Κατ' αρχάς υπενθυμίζουμε στον αναγνώστη μερικά γνωστά αποτελέσματα από την θεωρία παραστάσεων πεπερασμένων ομάδων. Για αποδείξεις παραπέμπουμε στα [3], [16]. Για $d \in \mathbb{N}$, $GL_d(\mathbb{C})$ θα συμβολίζει την ομάδα όλων των αντιστρεψίμων $d \times d$ πινάκων υπέρ το $\mathbb{C}$ και αν V διανυσματικός χώρος πεπερασμένης διάστασης d υπέρ το $\mathbb{C}$,

$$GL(V) = \{ f : V \to V \mid f \text{ είναι } \mathbb{C}\text{-γραμμική και αντιστρέψιμη} \}.$$

Ορισμός 6.1.1 Παράσταση *μιάς πεπερασμένης ομάδας G μέσω πινάκων υπέρ το $\mathbb{C}$ θα είναι κάθε ομομορφισμός ομάδων*

$$\rho : G \to GL_d(\mathbb{C})$$

*(***Παράσταση** *της G υπέρ τον V θα λέγεται κάθε ομομορφισμός $\rho : G \to GL(V)$.)*

Το d θα λέγεται **βαθμός της** ρ. Έτσι σε κάθε g αντιστοιχούμε έναν (αντιστρέψιμο) $d \times d$ πίνακα $M(g)$. **Χαρακτήρας της** ρ ορίζεται η απεικόνιση $\chi_\rho : G \to \mathbb{C}$ τέτοια ώστε

$$\chi_\rho(g) = \operatorname{tr}(M(g)) \quad \text{για κάθε } g \in G.$$

Προφανώς $\chi_\rho(g)$ εξαρτάται μόνο από την κλάση συζυγίας του g και όχι από το ίδιο το g.

Ορισμός 6.1.2 *Δύο παραστάσεις της G $\{M_1(g)\}_{g\in G}$, $\{M_2(g)\}_{g\in G}$ βαθμών d και d' αντίστοιχα θα λέγονται* **ισοδύναμες** *εάν και μόνο εάν $d = d'$ και $\exists\, P \in GL_d(\mathbb{C})$ τέτοιο ώστε $PM_1(g)P^{-1} = M_2(g)$ για κάθε $g \in G$.*

Ισχύει η

Πρόταση 6.1.3 *Δύο παραστάσεις ρ_1, ρ_2 της G είναι ισοδύναμες εάν και μόνο εάν $\chi_{\rho_1} = \chi_{\rho_2}$.*

Ορισμός 6.1.4 *Η παράσταση $\{M_1(g)\}_{g\in G}$ θα λέγεται* **όχι ανάγωγη** *(***reducible***) όταν είναι ισοδύναμη προς $\{M_2(g)\}_{g\in G}$ όπου*

$$M_2(g) = \begin{pmatrix} A_1(g) & 0 \\ 0 & A_2(g) \end{pmatrix}, \quad \text{για όλα τα στοιχεία } g \in G,$$

αλλιώς θα λέγεται **ανάγωγη**.

(Η G δρά στον V $g \cdot v = \rho(g) \cdot v$ και ο διανυσματικός χώρος V γίνεται G-module, οπότε η παράσταση ρ θα είναι ανάγωγη αν δεν έχει γνήσια G-υπομodules. Ακόμη $(\rho, V) \sim (\rho, V') \iff V \cong V'$ σαν G-modules.)

Θεώρημα 6.1.5 *Κάθε παράσταση (ρ, V) της G αναλύεται σε ευθύ άρθροισμα* **αναγώγων** *παραστάσεων (ρ_α, V_α). Αν μετρήσουμε και την πολλαπλότητα εμφάνισης r_α της ρ_α τότε γράφουμε $\rho \sim \sum_\alpha r_\alpha \rho_\alpha$.*

Ορισμός 6.1.6 *Ο χαρακτήρας χ_α μιάς ανάγωγης παράστασης ρ_α θα λέγεται* **ανάγωγος** *(ή* **απλός***).*

Από το θεώρημα 6.1.5 έπεται ότι αν $\rho \sim \sum_\alpha r_\alpha \rho_\alpha$ τότε

$$\chi_\rho \;=\; \sum_\alpha r_\alpha \chi_\alpha$$

όπου χ_α ανάγωγοι χαρακτήρες της G.

Πρόταση 6.1.7 *Το πλήθος των απλών χαρακτήρων της G είναι ίσο με τον αριθμό των κλάσεων συζυγίας της G.*

Θεώρημα 6.1.8 (σχέσεις ορθογωνιότητας)

$$\sum_{g\in G} \chi_1(g)\overline{\chi_2}(g) = \begin{cases} n, & \text{αν } \chi_1 = \chi_2 \\ 0, & \text{αν } \chi_1 \neq \chi_2 \end{cases}$$

Ιδιαίτερα,

$$\sum_{g\in G} \chi(g) = \begin{cases} n, & \text{αν } \chi = \chi_0 \\ 0, & \text{αλλιώς} \end{cases}$$

όπου χ_0 ο κύριος χαρακτήρας της G, δηλαδη αυτός που αντιστοιχεί στην παράσταση $M(g) = 1$ για όλα γα στοιχεία g της G.

Αν τώρα $\psi_1, \psi_2, \ldots, \psi_t$ είναι όλοι οι **απλοί** χαρακτήρες της G τότε

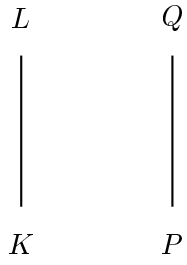
$$\sum_{i=1}^{t} \psi_i(g)\overline{\psi_i}(g') \;=\; \begin{cases} 0, & \text{αν } \langle g\rangle \neq \langle g'\rangle \\ \dfrac{\#G}{\#\langle g\rangle}, & \text{αν } \langle g\rangle = \langle g'\rangle \end{cases}$$

όπου $\overline{\psi_i}$ είναι ο μιγαδικός συζυγής του ψ_i και $\langle g\rangle$ είναι η κλάση συζυγίας του g.

Στην ειδική περίπτωση που $g = g' = 1$ έχουμε

$$\sum_{i=1}^{t} n_i^2 \;=\; \#G \;=\; n,$$

όπου $\psi_i(1) = n_i$ φυσικός αριθμός ο οποίος λέγεται βαθμός της ψ_i. Αν πάλι G αβελιανή, τότε επειδή για κάθε $g \in G$, $\#\langle g\rangle = 1$, έχουμε $t = n$, δηλαδή $n_i = 1$, οπότε οι $\psi_i : G \to \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ είναι **αβελιανοί χαρακτήρες**.



Τώρα έστω $P \in \mathbb{P}(K)$, μή-διακλαδιζόμενο στην L/K και $\left[\frac{L/K}{Q}\right]$ το σύμβολο του Frobenius.
Αν $\rho : G = \mathrm{Gal}\left(L/K\right) \longrightarrow \mathrm{GL}_d(\mathbb{C})$ μία παράσταση της G και

$$\rho\left(\left[\frac{L/K}{Q}\right]\right) = M\left(\left[\frac{L/K}{Q}\right]\right)$$

τότε θεωρούμε το "**χαρακτηριστικό**" **πολυώνυμο** στου πίνακα $M\left(\left[\frac{L/K}{Q}\right]\right)$

$$\det\left[I_d - M\left(\left[\frac{L/K}{Q}\right]\right)X\right].$$

Αν πάρουμε μία ισοδύναμη παράσταση της G, έστω ρ', τότε το $\rho'\left(\left[\frac{L/K}{Q}\right]\right) = M'\left(\left[\frac{L/K}{Q}\right]\right)$ είναι πίνακας **όμοιος** πρός τον $M\left(\left[\frac{L/K}{Q}\right]\right)$ και συνεπώς το "χαρακτηριστικό" πολυώνυμο δεν αλλάζει, δηλαδή εξαρτάται από τον **χαρακτήρα και όχι από την παράσταση**. Επίσης αν πάρουμε $Q' \in \mathbb{P}(L)$, $Q' \bigcap K = P$, τότε το $\left[\frac{L/K}{Q}\right]$ είναι συζυγές του $\left[\frac{L/K}{Q'}\right]$, δηλαδή και πάλι δεν μεταβάλλεται το χαρακτηριστικό πολυώνυμο, εξαρτάται λοιπόν από το P και όχι από τα Q.

Μπορούμε τώρα να θέσουμε όπου X, $N(P)^{-s}$ και να ορίσουμε (προσωρινά) την L-σειρά του Artin για μη-διακλαδιζόμενους πρώτους.

Ορισμός 6.1.9 (προσωρινός)

$$L\left(s, \chi, L/K\right) := \prod_{\substack{P \in \mathbb{P}(K) \\ P \nmid \mathfrak{D}(L/K)}} \det\left(I - M\left(\left[\frac{L/K}{Q}\right]\right) \cdot N(P)^{-s}\right)^{-1}$$

όπου $\mathfrak{D}\left(L/K\right)$ η (σχετική) διακρίνουσα της επέκτασης L/K.

Ο πλήρης ορισμός αυτών των L-σειρών δόθηκε από τον Artin στην εργασία τού 1931. Το πρόβλημα είναι τα διακλαδιζόμενα πρώτα ιδεώδη.

Γενικά λοιπόν τώρα έστω L/K επέκταση του Galois, $G = \mathrm{Gal}\left(L/K\right)$, V ένας $\mathbb{C}$-διανυσματικός χώρος πεπερασμένης διάστασης και

$$\rho : G\left(L/K\right) \longrightarrow \mathrm{GL}(V)$$

μία παράσταση της G με χαρακτήρα $\chi := \chi_\rho$. Συμβολίζουμε την δράση της G επί του V με σv και εννοούμε $\rho(\sigma)v$.

Έστω τώρα **οποιοδήποτε** (δηλαδή και διακλαδιζόμενο!) $P \in \mathbb{P}(K)$. Έστω κάποιο $Q \in \mathbb{P}(L)$, $Q \bigcap K = P$, $G_Z := G_Z\big({}^{Q}\!/_{P}\big)$, $G_T := G_T\big({}^{Q}\!/_{P}\big)$ οι ομάδες ανάλυσης και διακλαδώσεως αντίστοιχα. Είναι γνωστό ότι

$$ {}^{G_Z}\!/_{G_T} \cong \overline{G} = \mathrm{Gal}\big({}^{\overline{L}}\!/_{\overline{K}}\big) $$

όπου $\overline{L} = {}^{S}\!/_{Q}$ και $\overline{K} = {}^{R}\!/_{P}$. Αλλάζοντας και πάλι λίγο τους ορισμούς μας, κάθε στοιχείο της ${}^{G_Z}\!/_{G_T}$ που απεικονίζεται στον Frobenius της $\overline{G}$, δηλαδή στο $\overline{\sigma} : {}^{S}\!/_{Q} \ni \overline{s} = s + Q \mapsto \overline{s}^{N(\mathbb{P})} = s^{N(\mathbb{P})} + Q \in {}^{S}\!/_{Q}$ θα το λέμε ένα **αυτομορφισμό του Frobenius** των ${}^{Q}\!/_{P}$ και θα το συμβολίζουμε με $\varphi_{{}^{Q}\!/_{P}} \in G_Z$. Είναι προφανές ότι $\varphi_{{}^{Q}\!/_{P}}$ είναι ένας αντιπρόσωπος της πλευρικής ομάδας (coset) $\varphi_{{}^{Q}\!/_{P}} \cdot G_T({}^{Q}\!/_{P})$.

Ορίζουμε τώρα

$$ V^{G_T({}^{Q}\!/_{P})} := \Big\{ x \in V \;\Big|\; \rho(g)(x) = x \quad \forall\, g \in G_T\big({}^{Q}\!/_{P}\big) \Big\} $$

και

Ορισμός 6.1.10 (τελικός) *Έστω $s \in \mathbb{C}$ με $Re(s) > 1$. Η συνάρτηση*

$$ L\big(s, \chi, {}^{L}\!/_{K}\big) := \prod_{P \in \mathbb{P}(K)} \det\Big[\Big(1_V - NP^{-s} \cdot \rho(\varphi_{{}^{Q}\!/_{P}}) \Big) \,|V^{G_T} \Big]^{-1} $$

*θα λέγεται L-**σειρά του Artin** ως προς τον χαρακτήρα χ.*

Κατ' αρχήν παρατηρούμε ότι, αν $P \nmid \mathfrak{D}\big({}^{L}\!/_{K}\big)$ τότε $G_T = \{1\}$, $V^{G_T} = V$ και ο ορισμός ταυτίζεται με τον προηγούμενο.

Τώρα για να έχει ο ορισμός νόημα θα πρέπει να διαπιστώσουμε τα εξής:

(α′) $\rho(\varphi_{{}^{Q}\!/_{P}}) : V^{G_T} \longrightarrow V^{G_T}$.

Απόδειξη: Επειδή $G_T \lhd G_Z$, αν $g \in G_T$ τότε $\varphi^{-1} g \varphi = g' \in G_T$, δηλαδή υπάρχει $g' \in G_T$ τέτοιο ώστε $g\varphi = \varphi g'$, οπότε για **κάθε** $x \in V^{G_T}$ έχουμε $g\varphi(x) = \varphi(g'(x)) = \varphi(x)$ και αυτό προφανώς ισχύει για κάθε $g \in G_T$, δηλαδή $\varphi(x) \in V^{G_T}$ $(\varphi := \varphi_{{}^{Q}\!/_{P}})$. □

(β′) Αν φ' κάποιος άλλος αυτομορφισμός του Frobenius τότε προφανώς $\varphi' = \varphi \cdot g$, με $g \in G_T$, οπότε για κάθε $x \in V^{G_T}$ έχουμε $\varphi'(x) = (\varphi g)(x) = \varphi(g(x)) = \varphi(x)$, δηλαδή ο ορισμός μας **δεν** εξαρτάται από την επιλογή του φ. □

(γ′) $\rho(\varphi)\big|_{V^{G_T}}$ αντιστρέψιμος.

Απόδειξη: $\rho(\varphi)\big|_{V^{G_T}}$ είναι ένας ενδομορφισμός του διανυσματικού χώρου V^{G_T} **πεπερασμένης** τάξης. Επομένως οι ιδιοτιμές του είναι ρίζες της μονάδας. Συνεπώς το μηδέν **δεν** είναι ιδιοτιμή του

$$\left[1_V - NP^{-s}\cdot\rho(\varphi)\right]_{V^{G_T}}$$

για $s\in\mathbb{C}$ με $\mathrm{Re}(s)>0$. Επομένως είναι αυτομορφισμός. □

(δ′) Η **ορίζουσα** του αυτομορφισμού ανεξάρτητη της επιλογής του Q. $\big(Q\big|P\big)$

Απόδειξη: Έστω Q και $Q'\in\mathbb{P}(L)$. $Q\cap K=P=Q'\cap K$. Γνωρίζουμε ότι: $G_{Z'}=\sigma G_Z\sigma^{-1}$, $G_{T'}=\sigma G_T\sigma^{-1}$ και $\varphi'=\sigma\varphi\sigma^{-1}$ (δες [2], σελίδα 177), όπου $\sigma\in G\big(\frac{L}{K}\big)$ τέτοιο ώστε $\sigma(Q)=Q'$, δηλαδή ο φ' είναι **συζυγής** του φ και **συνεπώς** η ορίζουσα δεν αλλάζει τιμή. □

Τέλος ισχύει:

(ε′) Η ορίζουσα εξαρτάται **μόνο από τον χαρακτήρα** χ και **όχι από την παράσταση** ρ. Πράγματι, αν $\rho: G\big(\frac{L}{K}\big)\to GL(V)$ και $\rho': G\big(\frac{L}{K}\big)\to GL(V')$ δύο ισοδύναμες παραστάσεις τότε (εξ ορισμού) $\exists\, f: V\xrightarrow{\cong} V'$ με $f\circ\rho(g)=\rho'(g)\circ f$ για κάθε $g\in G$, οπότε

$$f\Big|_{V^{G_T}}: V^{G_T}\longrightarrow V'^{G_T}$$

ισομορφισμός και $f\circ\rho(\varphi)=\rho'(\varphi)\circ f$, συνεπώς

$$\rho'(\varphi)\Big|_{V'^{G_T}} \;=\; f\Big|_{V^{G_T}}\circ\rho(\varphi)\Big|_{V^{G_T}}\circ\Big(f\Big|_{V^{G_T}}\Big)^{-1}.$$

Από την τελευταία σχέση συζυγίας έπεται το αμετάβλητο της ορίζουσας. □

Συνολικά λοιπόν έχουμε: Η $L\big(s,\chi,\frac{L}{K}\big)$ είναι **καλά ωρισμένη** και **δεν εξαρτάται από την παράσταση που αντιστοιχεί στον χαρακτήρα** χ.

6.2 Ιδιότητες των L-σειρών του Artin

Θεώρημα 6.2.1 *Η* $L\big(s,\chi,\frac{L}{K}\big)$ **συγκλίνει απόλυτα** *στο ημιεπίπεδο* $Re(s)>1$ *και* **ομοιόμορφα** *σε συμπαγή υποσύνολά του.*

Απόδειξη: Έστω $\dim_{\mathbb{C}} V = m$. Για κάθε $P \in \mathbb{P}(K)$ έστω $\dim_{\mathbb{C}} V^{G_T} = m_P \leq m$, όπου $G_T = G_T\left({}^{Q}\!/_{P}\right)$ για κάποιο $Q \in \mathbb{P}(L)$, $Q|P$, και έστω $\varepsilon_{P,1}, \varepsilon_{P,2}, \ldots, \varepsilon_{P,m_P}$ οι ιδιοτιμές του ενδομορφισμού $\rho(\varphi_{Q/P})|_{V^{G_T}}$, οι οποίες, όπως παρατηρήσαμε πιο μπροστά, είναι ρίζες της μονάδος.

Επομένως

$$L\left(s, \chi, {}^{L}\!/_{K}\right) \;=\; \prod_{P \in \mathbb{P}(K)} \prod_{j=1}^{m_P} \left(1 - \frac{\varepsilon_{P,j}}{NP^s}\right)^{-1}.$$

Είναι γνωστό ότι αρκεί να αποδείξουμε τα συμπεράσματα του θεωρήματος για την σειρά

$$S \;:=\; \sum_{P \in \mathbb{P}(K)} \sum_{j=1}^{m_P} \left| \frac{\varepsilon_{P,j}}{NP^s} \right|.$$

Επειδή $|\varepsilon_{P,j}| = 1$ για κάθε $P \in \mathbb{P}(K)$ και για κάθε $j = 1, 2, \ldots, m_P$, και $m_P \leq m$ για κάθε $P \in \mathbb{P}(K)$, έχουμε:

$$S \;\leq\; m \sum_{P \in \mathbb{P}(K)} \frac{1}{|NP^s|} \;\leq\; m(K:Q) \cdot \sum_{p \in \mathbb{P}} \frac{1}{p^\sigma} \;\leq\; m(K:Q)|\zeta(s)| \;<\; \infty, \quad (s = \sigma + it)$$

οπότε έχουμε την απόλυτη σύγκλιση και την ομοιομορφία σε συμπαγή υποσύνολα του $\mathrm{Re}(s) > 1$, αφού αυτό ισχύει για την $\zeta(s)$. □

Θεώρημα 6.2.2 *Έστω τώρα ${}^{L}\!/_{K}$ πεπερασμένη* **αβελιανή** *επέκταση αλγεβρικών σωμάτων αριθμών και χ ένας* **πιστός** *χαρακτήρας της $G\left({}^{L}\!/_{K}\right) = G$. Με $\tilde{\chi}$ συμβολίζουμε τώρα τον αντίστοιχο αβελιανό χαρακτήρα της G (δες σελίδα 98, ορισμός 4.2.1). Τότε*

$$L\left(s, \chi, {}^{L}\!/_{K}\right) = L(s, \tilde{\chi}),$$

δηλαδή οι L-σειρές του Artin γενικεύουν τις αντίστοιχες αβελιανές L-σειρές.

Απόδειξη: Έστω ρ μία 1-διάστατη παράσταση $\rho : G\left({}^{L}\!/_{K}\right) \to GL(\mathbb{C})$ της $G\left({}^{L}\!/_{K}\right)$ με χαρακτήρα τον χ. Επειδή ρ μονοδιάστατη, έχουμε $\rho(g)(x) = \chi(g) \cdot x$ για κάθε $g \in G\left({}^{L}\!/_{K}\right)$. Αν τώρα $P \in \mathbb{P}(K)$ μη-διακλαδιζόμενο τότε $V = V^{G_T(Q/P)}$, οπότε

$$\begin{aligned} & \det\left[\left(1_V - NP^{-s}\rho(\varphi_{Q/P})\right)|V^{G_T}\right] \\ = \;& \det\left[\left(1_V - NP^{-s}\chi(\varphi_{Q/P})\right)|V\right] \\ = \;& 1 - \frac{\tilde{\chi}(P)}{NP^s}. \end{aligned}$$

Αν $P \in \mathbb{P}(K)$ διακλαδίζεται, τότε $V^{G_T} = \{0\}$ διότι, για κάθε $x \in V^{G_T}$ και $g \in G_T - \{1\}$ έχουμε $\chi(g) \neq 1$ και $x = \rho(g)(x) = \chi(g) \cdot x$, δηλαδή κατ' ανάγκη $x = 0$, οπότε

$$\det\left[(1_V - \rho(\varphi)NP^{-s})|V^{G_T}\right] = 1.$$

Από την άλλη μεριά,

$$\tilde{\chi}(P) \;=\; \chi(\varphi_{Q/P}) \cdot \frac{1}{e_P} \cdot \sum_{\tau \in G_T} \chi(\tau)$$

και επειδή $\chi \neq \chi_0$ έπεται ότι

$$\sum_{\tau \in G_T} \chi(\tau) = 0,$$

δηλαδή ότι $\tilde{\chi}(P) = 0$. □

Θεώρημα 6.2.3 *Αν $\chi = \chi_0$ ο μοναδικός χαρακτήρας της $G := G(L/K)$, τότε $L(s, \chi_0, L/K) = \zeta_K(s)$. Αυτό σημαίνει ότι οι L-σειρές του Artin γενικεύουν και τις ζήτα συναρτήσεις του Dedekind.*

Απόδειξη: Αν ρ είναι η τετριμμένη παράσταση $\rho : G \longrightarrow GL(\mathbb{C})$, $\rho(g) \equiv 1$ για κάθε $g \in G$, τότε

$$\det\left[1 - \rho(\varphi_{Q/P})NP^{-s}\right] = 1 - NP^{-s}, \quad \text{για κάθε } P \in \mathbb{P}(K). \quad \square$$

Θεώρημα 6.2.4 *Αν χ_1, χ_2 χαρακτήρες της $G(L/K)$ τότε*

$$L(s, \chi_1 + \chi_2 L/K) \;=\; L(s, \chi_1, L/K) \cdot L(s, \chi_2, L/K).$$

Απόδειξη: Έστω V_1, V_2 διανυσματικοί χώροι **πεπερασμένης** διάστασης και

$$\rho_1 : G(L/K) \longrightarrow GL(V_1),$$
$$\rho_2 : G(L/K) \longrightarrow GL(V_2)$$

παραστάσεις με χαρακτήρες χ_1, χ_2 αντίστοιχα. Έστω $V := V_1 \oplus V_2$. Επομένως

$$\rho := \rho_1 \oplus \rho_2 : G(L/K) \longrightarrow GL(V)$$

είναι μία παράσταση της $G\left(L/K\right)$ με χαρακτήρα τον $\chi_1+\chi_2$. Για κάθε $P\in\mathbb{P}(K)$ έχουμε

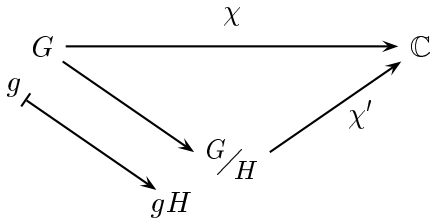
$$\begin{aligned} & \det\left[\left(1_V - NP^{-s}\rho(\varphi)\right)\big|V^{G_T}\right] \\ = \;& \det\left[\left(1_V - NP^{-s}\rho_1(\varphi)\oplus\rho_2(\varphi)\right)\big|V^{G_T}\right] \\ = \;& \det\left[\left(1_{V_1} - NP^{-s}\cdot\rho_1(\varphi)\right)\big|V_1^{G_T}\right]\cdot\det\left[\left(1_{V_2} - NP^{-s}\cdot\rho_2(\varphi)\right)\big|V_2^{G_T}\right], \end{aligned}$$

διότι

$$(V_1\oplus V_2)^{G_T} = V_1^{G_T}\oplus V_2^{G_T}$$

και συνεπώς το θεώρημα. □

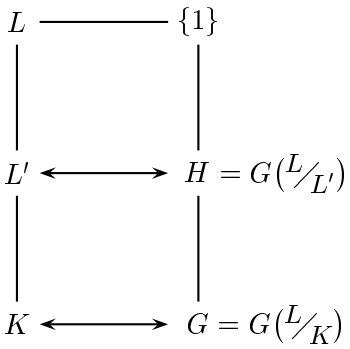
Θεώρημα 6.2.5 *Έστω L/K πεπερασμένη επέκταση του Galois και L' ένα ενδιάμεσο σώμα τέτοιο ώστε η επέκταση L'/K να είναι επίσης Galois. Έστω χ' ένας χαρακτήρας της $G\left(L'/K\right)$ και έστω χ ο χαρακτήρας (lifting) του χ', δηλαδή,*



$\chi(g) := \chi'(gH)$ *για κάθε* $g\in G$
όπου $H := G\left(L/L'\right)$

Τότε $L\left(s,\chi,L/K\right) = L\left(s,\chi',L'/K\right)$.

Απόδειξη:

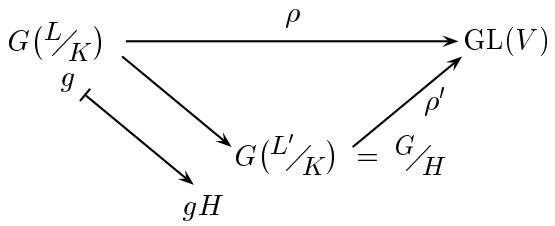


$$G\left(L'/K\right) \;\cong\; G/H$$

Έστω $Q\in\mathbb{P}(L)$. $Q\cap L' = Q'$, $Q\cap K = P$. Έστω $\varphi_{Q/P}$ ένας αυτομορφισμός του Frobenius της L/K για τα Q/P. Γνωστό ότι

$$\varphi_{Q'/P} \;=\; \varphi_{Q/P}\Big|_{L'}$$

είναι ένας αυτομορφισμός του Frobenius για Q'/P. Έστω V διανυσματικός χώρος πεπερασμένης διάστασης /$\mathbb{C}$ και $\rho' : G(L'/K) \longrightarrow \mathrm{GL}(V)$ μία παράσταση της $G(L'/K)$ με χαρακτήρα τον χ'. Η παράσταση της $G(L/K)$, ρ, που είναι lifting της ρ'



είναι μία παράσταση με χαρακτήρα του χ. Επειδή

$$G_T\left(Q'/P\right) \;=\; \left\{ g|_{L'} \;\middle|\; g \in G_T(Q/P) \right\}$$

έχουμε:

$$\begin{aligned} V^{G_T(Q/P)} &= \left\{ x \in V \,|\, \rho(g)(x) = x, \forall g \in G(Q/P) \right\} \\ &= \left\{ x \in V \,|\, \rho'(g|_{L'})(x) = x, \forall g \in G_T(Q/P) \right\} \\ &= \left\{ x \in V \,|\, \rho'(g')(x) = x, \forall g' \in G_T(Q'/P) \right\} \\ &= V^{G_T(Q'/P)}. \end{aligned}$$

Για όλα λοιπόν τα $P \in \mathbb{P}(K)$, ισχύει

$$\begin{aligned} & \det\left[\left(1_V - NP^{-s} \rho(\varphi_{Q/P}) \right) \,|\, V^{G_T(Q/P)} \right] \\ = \;& \det\left[\left(1_V - NP^{-s} \rho'(\varphi_{Q/P} | L') \right) \,|\, V^{G_T(Q/P)} \right] \\ = \;& \det\left[\left(1_V - NP^{-s} \cdot \rho'(\varphi_{Q'/P}) \right) \,|\, V^{G_T(Q'/P)} \right], \end{aligned}$$

δηλαδή το ζητούμενο. □

Στη συνέχεια θα αναφερθούμε σε μία πολύ σημαντική ιδιότητα των L-σειρών του Artin η οποία χρειάζεται περισσότερα στοιχεία από την θεωρία παραστάσεων πεπερασμένων ομάδων και ένα πολύ σημαντικό θεώρημα αυτής, το **θεώρημα του Brauer (ή Brauer-Tate)**.

Η σχέση ανάμεσα στους χαρακτήρες της G και στους χαρακτήρες των υποομάδων της H είναι θεμελιώδους σημασίας για την μελέτη της δομής της G. Αν ρ μία παράσταση της G $\rho : G \longrightarrow \mathrm{GL}(V)$, όπου V $\mathbb{C}$-διανυσματικός χώρος πεπερασμένης διάστασης και $H < G$. Ο

περιορισμός της ρ στην H $\rho\big|_H$ είναι, προφανώς, παράσταση της H. Αν χ ο χαρακτήρας της ρ τότε με $\chi|_H$ θα συμβολίζουμε και πάλι περιορισμό του χ στην H.

Προφανώς η απεικόνιση **περιορισμός** είναι γραμμική και διατηρεί το γινόμενο χαρακτήρων. Επομένως επάγει έναν φυσικό ομομορφισμό

$$\mathrm{res} : \hat{G} \longrightarrow \hat{H}.$$

Κάτι το οποίο δεν είναι τόσο προφανές είναι ότι υπάρχει επίσης μία απεικόνιση από $\hat{H} \to \hat{G}$ η οποία επίσης ορίζεται κατά εντελώς φυσιολογικό τρόπο.

Έστω g_i, $i \leq i \leq m$, ένα πλήρες σύστημα αντιπροσώπων των πλευρικών ομάδων της H ως προς την G και ψ μία παράσταση με πίνακες της H βαθμού d. Επεκτείνουμε τον ορισμό της ψ σε όλα τα στοιχεία της G θέτοντας

$$\psi(g) := [0]_{d\times d} \quad \forall g \in G - H.$$

Με την βοήθεια της ψ ορίζουμε τώρα μία απεικόνιση $\psi^* : G \longrightarrow M_{md}(\mathbb{C})$ ως εξής:

$$\psi^*(g) = \Big(\psi(g_i g g_j^{-1})\Big) \tag{6.1}$$

Ο $\psi^*(g)$ είναι λοιπόν ένας $m\times m$-πίνακας ο οποίος στην (i,j)-θέση του έχει τον $d\times d$-πίνακα $\psi(g_i g g_j^{-1})$. Ισχύει το:

Η απεικόνιση ψ^* όπως ορίζεται στην 6.1 είναι μία **παράσταση** της G βαθμού $[G:H]\cdot\deg\psi$ (δες [16], σελίδα 135).

Έστω τώρα $S = \{Hg_i \,|\, 1 \leq i \leq m\}$.

Η G δρά πάνω στο S ως εξής:

$$\pi_g(Hg_i) = Hg_i g \quad \text{για κάθε } g \in G.$$

Η δράση αυτή ορίζει μία μετάθεση του συνόλου S. Ακόμη ισχύει $\pi_x\pi_y = \pi_{xy}$ για $x, y \in G$. Επομένως η απεικόνιση

$$\pi_H(g) = \pi_g$$

είναι ομομορφισμός της G στην συμμετρική ομάδα S_m των στοιχείων του S. Αν $K = \mathrm{Ker}\pi_H$ τότε

$$\begin{aligned} g \in K &\iff g \text{ σταθεροποιεί } \textbf{κάθε } Hg_i \\ &\iff \forall i, 1 \leq i \leq m, Hg_i g = Hg_i \\ &\iff g \in g_i^{-1} H g_i \quad \forall i = 1, 2, \ldots, m, \end{aligned}$$

δηλαδή

$$K = \bigcap_{i=1}^{m} H^{g_i}.$$

Η $\pi_H(G) \cong {}^{G}\!/_{K}$ είναι ισόμορφη με μία **ομάδα μεταθέσεων** του S και δρά **μεταβατικά** επί του S. Γι' αυτό θα λέγεται η π_H η (μεταβατική) **παράσταση μεταθέσεων** της S. Γενικώτερα, κάθε ομομορφισμός της G μέσα στην συμμετρική ομάδα ενός συνόλου S θα λέγεται **παράσταση μεταθέσεων** της G επί του S.

Αν τώρα, **ειδικά**, $H = \{1\}$ (περίπτωση ιδιαίτερης σπουδαιότητας) τότε $K = \mathrm{Ker}\pi_H = \{1\}$ οπότε $\rho = \pi_H$ είναι ένας **ισομορφισμός** της G μέσα στην συμμετρική ομάδα των $|G|$-στοιχείων. Η παράσταση αυτή θα λέγεται ομαλή **(regular) παράσταση της** G.

Τώρα ισχύει το εξής:

Θεώρημα 6.2.6 *Έστω $H < G$ και ψ η* **τετριμμένη** *παράσταση της H. Η παράσταση ψ^* της G είναι η* **παράσταση μεταθέσεων** *του S ($S = \{Hg_i \,|\, 1 \le i \le m\}$). Ιδιαίτερα αν $H \triangleleft G$ τότε η ψ^* είναι η* **regular παράσταση της** ${}^{G}\!/_{H}$. *(Δες [16], σελίδα 135.)*

Ορισμός 6.2.7 *Η ψ^* θα λέγεται η παράσταση της G η* **επαγομένη** *από την παράσταση ψ της H. Συνήθως θα την συμβολίζουμε*

$$\psi^* = Ind_H^G \psi$$

Αν χ ο χαρακτήρας της ψ τότε θα συμβολίζουμε με $\chi^* = Ind_H^G \chi$ τον (επαγόμενο) χαρακτήρα της ψ^*.

Χωρίς απόδειξη πάλι αναφέρουμε μερικές ιδιότητες:

1. $\chi^*(g) := \dfrac{1}{[H:1]} \displaystyle\sum_{u \in G} \chi\left(ugu^{-1}\right)$, για κάθε $g \in G$

2. $\chi^*(g) = 0$, όταν το g δεν είναι συζυγές στοιχείου της H.

3. Αν $\mathrm{Ker}\,\chi \triangleleft G$ τότε $\mathrm{Ker}\,\chi \subseteq \mathrm{Ker}\,\chi^*$.

4. Αν $H \triangleleft G$, τότε $\mathrm{Ker}\,\chi^* \subseteq \mathrm{Ker}\,\chi$.

5. Ισοδύναμες παραστάσεις της H επάγουν τον ίδιο χαρακτήρα της G.

6. Αν $H \leq K \leq G$ και χ χαρακτήρας της H και έστω $\tilde{\chi}$ ο χαρακτήρας της K που επάγεται από τον χ, τότε

$$\chi^* = (\tilde{\chi})^* .$$

7. Στην $\hat{G}$ ορίζουμε **εσωτερικό γινόμενο**

$$\langle \chi_1, \chi_2 \rangle_G := \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi}_2(g).$$

Αλλά και στην H έχουμε το ίδιο.

Ο **νόμος αντιστροφής του Frobenius** μάς δίνει:

$$\langle \chi_1, \chi_2|_H \rangle_H = \langle \mathrm{Ind}_H^G \chi_1, \chi_2 \rangle_G .$$

Εδώ χ_1 είναι χαρακτήρας της H και χ_2 χαρακτήρας της G.

Τώρα είμαστε σε θέση να διατυπώσουμε το:

Θεώρημα 6.2.8 *Έστω μία L/K επέκταση του Galois αλγεβρικών σωμάτων αριθμών. Έστω $K \subseteq M \subseteq L$ ενδιάμεσο σώμα και έστω χ χαρακτήρας της $H := G(L/M)$ και $\chi^* =: Ind_H^G \chi$ ο από τον χ επαγόμενος χαρακτήρας της $G = G(L/K)$. Τότε ισχύει:*

$$L\big(s, Ind_H^G \chi, L/K\big) \;=\; L\big(s, \chi, L/M\big).$$

Απόδειξη: Όπως και πιο μπροστά, αν $P \in \mathbb{P}(K)$ και $Q \in \mathbb{P}(L)$ τέτοιο ώστε $Q \cap K = P$ οι ομάδες αναλύσεως και αδρανείας θα συμβολίζονται με $G_Z = G_Z(Q/P)$ και $G_T = G_T(Q/P)$ αντίστοιχα. Υπενθυμίζουμε ότι $G_Z/G_T \cong \overline{G} = \mathrm{Gal}(\overline{L}/\overline{K})$ όπου $\overline{L}$ και $\overline{K}$ τα σώματα υπολοίπων (residue fields) των L και K ως προς Q και P αντίστοιχα. Επίσης με $\varphi_{Q/P}$ θα συμβολίζουμε έναν αυτομορφισμό του Frobenius, $\varphi_{Q/P} \in G_Z$.

Έστω τώρα V κάποιος $\mathbb{C}$-διανυσματικός χώρος με $\dim_{\mathbb{C}} V = d < \infty$. Αν

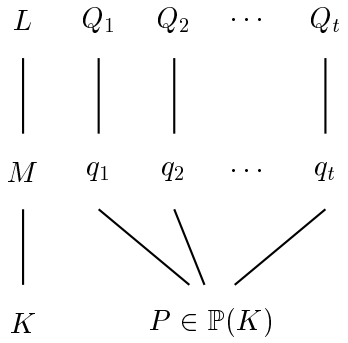
$$\rho : H \longrightarrow \mathrm{GL}(V)$$

είναι μία παράσταση της H η οποία έχει σαν χαρακτήρα τον δοσμένο χ και

$$\rho^* := \mathrm{Ind}_H^G \rho : G := G(L/K) \longrightarrow \mathrm{GL}(V^*)$$

η επαγομένη από τον ρ παράσταση της G, τότε η ρ^* έχει σαν χαρακτήρα τον $\chi^* := \mathrm{Ind}_H^G \chi$.

Αν τώρα $Q_1, Q_2, \dots, Q_t$ είναι οι πρώτοι του L οι οποίοι διαιρούν το $P \in \mathbb{P}(K)$ και q_i οι υποκείμενοι των Q_i πρώτοι του M, $q_i = Q_i \cap M$, τότε αρκεί να αποδείξουμε ότι:



$$\det\left[\left(\mathrm{Id}_{V^*} - NP^{-s}\cdot\rho^*(\varphi_{Q_{\diagup P}})\right) \;\middle|\; V^{*G_T(Q_{\diagup P})}\right] = \prod_{i=1}^{t}\det\left[\left(\mathrm{Id}_V - Nq_i^{-s}\cdot\rho(\varphi_{Q_{\diagup q_i}})\right) \;\middle|\; V^{G_T(Q_{\diagup q_i})}\right]. \qquad (6.2)$$

Η ιδέα για τον υπολογισμό της ρ^* είναι η επιλογή κατάλληλου συστήματος αντιπροσώπων των πλευρικών ομάδων της $G_{\diagup H}$. Για κάθε $j = 1, 2, \dots, t$ έστω $\sigma_j \in G$ τέτοιο ώστε $\sigma_j(Q_1) = Q_j$ (γνωρίζουμε ότι αυτό πάντοτε υπάρχει διότι η δράση της G στο σύνολο $\{Q_1, Q_2, \dots, Q_t\}$ είναι μεταβατική), και $m_j := e\left(Q_{j\diagup P}\right)\cdot f\left(Q_{j\diagup P}\right)$.

Θεωρούμε τις ομάδες ανάλυσης

$$G_{Z_j} := G_Z\left(Q_{j\diagup p}\right) \quad \text{και} \quad G'_{Z_j} := G_Z\left(Q_{j\diagup q_j}\right).$$

Είναι γνωστό ότι $G'_{Z_j} = G_{Z_j} \cap H$. Έστω $G_{Z_j} = \dot{\bigcup_{\nu=1}^{m_j}} G'_{Z_j}\cdot\gamma_{j\nu}$ η ανάλυση της G_{Z_j} σε δεξιές πλευρικές ομάδες ως προς την G'_{Z_j} ($\gamma_{j\nu} \in G_{Z_j}$).

Μία ανάλυση τώρα της G σε πλευρικές ομάδες της H είναι η ακόλουθη:

$$G = \dot{\bigcup_{j\in\{1,2,\dots,t\}}}\ \dot{\bigcup_{\nu\in\{1,2,\dots,m_j\}}} H\cdot\gamma_{j\nu}\cdot\sigma_j. \qquad (6.3)$$

Απόδειξη της (6.3).

Το πλήθος των πλευρικών ομάδων είναι $\sum_{j=1}^{t} m_j$. Επίσης, $[G : H] = (M : K) = \sum_{m=1}^{t} m_j$. Επομένως αρκεί να δείξουμε ότι οι $H\cdot\gamma_{j\nu}\cdot\sigma_j$ δίδουν ανά δύο διαφορετικές μεταξύ τους πλευρικές ομάδες. Πράγματι, έστω $H\cdot\gamma_{j\nu}\cdot\sigma_j = H\cdot\gamma_{k\mu}\cdot\sigma_k$. Αυτό σημαίνει ότι το στοιχείο

$$\sigma := \gamma_{j\nu}\sigma_j\sigma_k^{-1} \in H = G\left(L_{\diagup M}\right)$$

και συνεπώς

$$\sigma(q_k) = q_k. \qquad (6.4)$$

Από την άλλη μεριά,

$$\sigma(q_k) = \gamma_{j\nu}\sigma_j\sigma_k^{-1}\gamma_{k\mu}^{-1}(q_k).$$

Τώρα, επειδή $\gamma_{k\mu} \in G_{Z_k}$, έπεται ότι $\gamma_{k\mu}(q_k) = q_k$, οπότε

$$\sigma(q_k) = \gamma_{j\nu}\sigma_j\sigma_k^{-1}(q_k) = \gamma_{j\nu}\sigma_j(q_1) = \gamma_{j\nu}(q_j) = q_j. \tag{6.5}$$

Από τις σχέσεις (6.4) και (6.5) έπεται ότι $j = k$. Αυτό σημαίνει ότι

$$\sigma = \gamma_{j\nu}\gamma_{k\mu}^{-1} \in G_{Z_j} \cap H = G'_{Z_j}.$$

Επειδή όμως το σύνολο $\{\gamma_{j\nu}\}$ αποτελεί πλήρες σύστημα αντιπροσώπων των πλευρικών κλάσεων της G_{Z_j} ως προς την G'_{Z_j}, έπεται ότι $\nu = \mu$, δηλαδή η (6.3).

Έστω τώρα $R : H \longrightarrow \mathrm{GL}(d, \mathbb{C})$ μία παράσταση δια πινάκων της H η οποία αντιστοιχεί στην ρ. Λόγω της (6.3), η επαγόμενη παράσταση

$$R^* : G \longrightarrow \mathrm{GL}\big(d\cdot(M:K), \mathbb{C}\big)$$

ορίζεται ως εξής:

$$R^*(\sigma) \;=\; \big(R(\gamma_{k\mu}\sigma_k\sigma\sigma_j^{-1}\gamma_{j\nu})\big)_{(j,\nu),(k,\mu)}$$

και είναι μία παράσταση δια πινάκων της G που αντιστοιχεί στην ρ^*.

Εδώ (j,ν) είναι ο δείκτης των γραμμών, (k,μ) ο δείκτης των στηλών και $R(\sigma) = 0$ για κάθε $\sigma \in G - H$.

Από εδώ και κάτω με Q θα συμβολίζουμε τον πρώτο Q_1.

Για να προχωρήσουμε χρειαζόμαστε το ακόλουθο

Λήμμα 6.2.9 *Αν G περπερασμένη ομάδα και χ χαρακτήρας (όχι κατ' ανάγκη μονοδιάστατος!) και $\rho : G \longrightarrow GL(V)$ μία παράσταση της G στον (πεπερασμένης διάστασης) $\mathbb{C}$-διανυσματικό χώρο V, με χαρακτήρα χ, τότε η απεικόνιση $\Phi := \dfrac{1}{\#(G)} \cdot \displaystyle\sum_{\tau\in G} \rho(\tau)$ είναι μία* **προβολή** *του V στον*

$$V^G \;=\; \big\{x \in V \;\big|\; \rho(\sigma)(x) = x \;\; \textit{για κάθε } \sigma \in G\big\}.$$

Απόδειξη του λήμματος 6.2.9 Αν $v \in V$ τότε $x := \Phi(v) = \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\tau)(v)$, οπότε, για κάθε $\sigma \in G$, ισχύει:

$$\begin{aligned} \rho(\sigma)(x) &= \rho(\sigma)(\Phi(v)) = \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\sigma)(\rho(\tau)(v)) \\ &= \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\sigma\tau)(v) = \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(t)(v) = x, \end{aligned}$$

διότι, όταν το τ διατρέχει τα στοιχεία της G, το ίδιο κάνει και το $\sigma\tau$. Επομένως, η απεικόνιση Φ είναι ένας ενδομορφισμός του V στον $V^G \leq V$.

Θα αποδείξουμε ότι **ταυτοδύναμος**, δηλαδή ότι $\Phi^2 = \Phi$, πράγμα που συνεπάγεται ότι ο Φ είναι **προβολή**. Πράγματι,

$$\begin{aligned} (\Phi \circ \Phi)(v) &= \Phi(\Phi(v)) \\ &= \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\tau)(\Phi(v)) \\ &= \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\tau) \left(\frac{1}{\#G} \cdot \sum_{\sigma \in G} \rho(\sigma)(v) \right) \\ &= \frac{1}{\#G} \cdot \left(\frac{1}{\#G} \cdot \sum_{\tau \in G} \sum_{\sigma \in G} \rho(\sigma\tau)(v) \right). \end{aligned}$$

Πάλι, όταν το τ είναι σταθερό και το σ διατρέχει τα στοιχεία της G, τότε και το $\sigma\tau$ διατρέχει τα στοιχεία της G. Επομένως,

$$\sum_{\sigma \in G} \rho(\sigma\tau)(v) = \sum_{\sigma \in G} \rho(\sigma)(v),$$

οπότε και

$$\sum_{\tau \in G} \left(\sum_{\sigma \in G} \rho(\sigma)(x) \right) = \left|G\right| \cdot \sum_{\sigma \in G} \rho(\sigma)(x).$$

Τελικά, $\Phi^2 = \frac{1}{\#G} \cdot \sum_{\tau \in G} \rho(\tau)(v) = \Phi(v)$, δηλαδή η Φ είναι προβολή, και συνεπώς το λήμμα.

□

Σημείωση 6.2.10 *Επιπλέον ισχύει ότι* $\dim_{\mathbb{C}}^{G} = \chi(G)$, *όπου*

$$\chi(G) := \frac{1}{\#G} \cdot \sum_{\sigma \in G} \chi(\sigma).$$

Αυτό όμως δεν θα το χρειαστούμε στα επόμενα.

Από το λήμμα 6.2.9 τώρα έπεται ότι η $\Phi := \frac{1}{e(Q/P)} \cdot \sum_{\tau \in G_T(Q/P)} \rho^*(\tau)$ είναι **προβολή** του V^* στον $V^{*G_T(Q/P)}$. Επομένως,

$$\begin{aligned} & \det\left[\left(\mathrm{Id}_{V^*} - NP^{-s} \cdot \rho^*(\varphi_{Q/P})\right) \middle| (V^*)^{G_T(Q/P)}\right] \\ = \ & \det\left[\mathrm{Id}_{V^*} - \frac{1}{e(Q/P)} \cdot NP^{-s} \cdot \sum_{\tau \in G_T(Q/P)} \rho^*(\varphi_{Q/P} \cdot \tau)\right]. \end{aligned} \tag{6.6}$$

Ομοίως, αν

$$\Phi_j \ := \ \frac{1}{e(Q_j/q_j)} \cdot \sum_{\tau \in G_T(Q_j/q_j)} \rho(\tau)$$

τότε Φ_j προβολή του V στον $V^{G_T(Q_j/q_j)}$ $(j = 1, 2, \ldots, t)$. Επομένως,

$$\det\left[\left(\mathrm{Id}_V - Nq_j^{-s} \cdot \rho(\varphi_{Q_j/q_j})\right) \middle| V^{G_T(Q_j/q_j)}\right] \ = \ \det\left[\mathrm{Id}_V - Nq_j^{-s} \cdot \rho(\varphi_{Q_j/q_j}) \cdot \Phi_j\right]. \tag{6.7}$$

Αν $\tau \in G_T(Q/P)$, τότε έχουμε:

$$R^*(\varphi_{Q/P} \cdot \tau) \ = \ \left(R(\gamma_{k\mu}\sigma_k\varphi_{Q/P}\tau\sigma_j^{-1}\gamma_{j\nu}^{-1})\right)_{(j,\nu),(k,\mu)}.$$

Το $\sigma = \gamma_{k\mu}\sigma_k\varphi_{Q/P}\tau\sigma_j^{-1}\gamma_{jk}^{-1}$ απεικονίζει το Q_j στο Q_k, $\sigma(Q_j) = Q_k$.

Τώρα για $\sigma \in G \setminus H$, έχουμε $R(\sigma) = 0$ ενώ, αν $\sigma \in H$ τότε $\sigma(q_j) = q_j$. Επομένως $k = j$ και

$$R^*(\varphi_{Q/P} \cdot \tau) \ = \ \begin{bmatrix} A_{1,\tau} & & 0 \\ & \ddots & \\ 0 & & A_{t,\tau} \end{bmatrix} \tag{6.8}$$

όπου

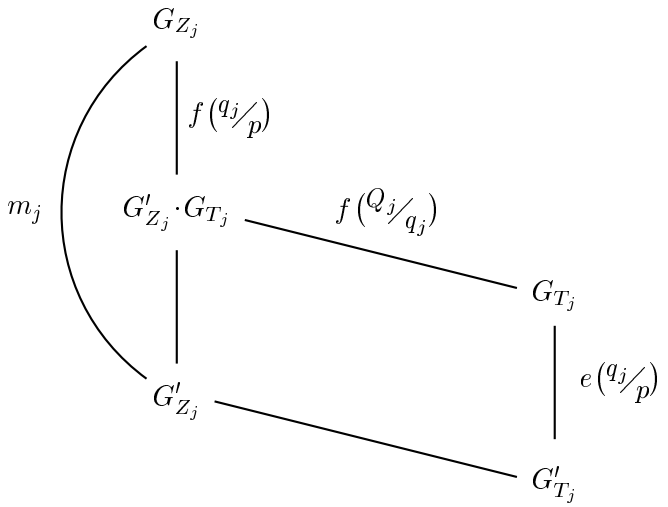
$$A_{j,\tau} \ = \ \left(R(\gamma_{j\mu}\sigma_j\varphi_{Q/P}\tau\sigma_j^{-1}\gamma_{j\nu}^{-1})\right)_{(\nu,\mu)}.$$

Στη συνέχεια θα **εκλέξουμε κατάλληλο** σύστημα συντεταγμένων (πλήρες σύστημα αντιπροσώπων των πλευρικών ομάδων) $\{\gamma_{j\nu}\}$ της G_{Z_j} ως προς την G'_{Z_j}.

Κατ' αρχήν υπενθυμίζουμε ότι

$$\varphi_{Q_j/P} \ = \ \sigma_j\varphi_{Q/P}\sigma_j^{-1}.$$

Έστω $\left\{\tau_{j,a} \middle| a \in \{1, 2, \ldots, e(q_i/p)\}\right\}$ ένα πλήρες σύστημα αντιπροσώπων των πλευρικών ομάδων της G_{T_j} ως προς την $G_T(Q_j/p)$.



Η ομάδα G_{Z_j}/G_{T_j} είναι κυκλική τάξης $f\left(Q_j/p\right)$ παραγομένη από τον αυτομορφισμό του Frobenius $\varphi_{Q_j/p}$. Συνεπώς και η $G_{Z_j}/G'_{Z_j}\cdot G_{T_j}$ είναι κυκλική τάξης $f(q_i/p)$.

Ένα πλήρες σύστημα αντιπροσώπων των πλευρικών ομάδων της G_{Z_j} ως προς την $G'_{Z_j}\cdot G_{T_j}$ είναι το

$$\left\{\varphi^{\ell}_{Q_j/p} \;\middle|\; \ell\in\{0,1,2,\dots,f(q_j/p)-1\}\right\}.$$

Επομένως, ένα πλήρες σύστημα αντιπροσώπων των πλευρικών ομάδων της G_{Z_j} ως προς την G'_{Z_j} θα είναι το σύνολο

$$\left\{\tau_{j,a}\cdot\varphi^{\ell}_{Q_j/p} \;\middle|\; a\in\{1,2,\dots,e(q_i/p),\ell\in\{0,1,2,\dots,f(q_i/p)-1\}\right\}.$$

Ως προς το "καινούργιο" αυτό σύστημα οι πίνακες $A_{j,\tau}$ γράφονται:

$$A_{j\tau} \;=\; \left(R(\tau_{j,a}\varphi^{l}_{Q_j/P}\sigma_j\varphi_{Q/P}\tau\sigma_j^{-1}\varphi^{-m}_{Q_j/P}\tau^{-1}_{j,b})\right)_{(a,l),(b,m)}$$

όπου το (a,l) είναι δείκτης γραμμής και το (b,m) δείκτης στήλης.

Όταν $\tau\in G_{T_1}=G_T\left(Q_1/p\right)$ διατρέχει την ομάδα G_{T_1} τα $\sigma_j\tau\sigma_j^{-1}$ διατρέχουν την ομάδα $G_{T_j}=G_T\left(Q_j/P\right)$. Επομένως,

$$A_j \;=\; \sum_{\tau\in G_{T_1}} A_{j,\tau} \;=\; \sum_{\tau\in G_{T_j}} \left(R(\tau_{j,a}\varphi^{l+1}_{Q_j/p}\tau\varphi^{-m}_{Q_j/p}\tau^{-1}_{j,b})\right)_{(a,l),(b,m)}.$$

Τώρα $G_{T_j}\trianglelefteq G_{Z_j}$, οπότε $\tau\cdot\varphi^{-m}_{Q_j/P}=\varphi^{-m}_{Q_j/P}\cdot\tau$ και, όταν το τ διατρέχει τα στοιχεία της G_{T_j}, το ίδιο κάνουν τόσο τα $\tau_{j,a}\tau$ όσο και τα $\tau_{j,a}\tau\tau^{-1}_{j,b}$.

Συνεπώς,

$$A_j = \sum_{\tau\in G_{T_j}} \left(R(\varphi_{Q_{j/p}}^{l+1-m})\cdot\tau\right)_{(a,l),(b,m)} \tag{6.9}$$

$$= \begin{bmatrix} B_j & \cdots & B_j \\ \vdots & & \vdots \\ B_j & \cdots & B_j \end{bmatrix}, \tag{6.10}$$

όπου

$$B_j = \left(\sum_{\tau\in G_{T_j}} R(\varphi_{Q_{j/P}}^{l+1-m})\cdot\tau\right)_{(l,m)}$$

είναι $e\left(q_j/P\right)\times e\left(q_j/P\right)$-blocks και $a,b\in\left\{1,2,\ldots,e\left(q_j/P\right)\right\}$.

Το $\tau\in G_{T_j}=G_T\left(Q_j/P\right)$ και το $\varphi_{Q_{j/P}}^{l+1-m}\in G_{Z_j}=G_Z\left(Q_j/P\right)$. Επομένως, $\varphi_{Q_{j/P}}^{l+1-m}\cdot\tau\in H$ αν και μόνο αν

$$\left\{\begin{array}{l} \varphi_{Q_{j/P}}^{l+1-m}\in G'_{Z_j}=G_Z\left(Q_j/q_j\right) \\ \qquad \text{και} \\ \tau\in G_{T_j}=G_T\left(Q_j/q_j\right) \end{array}\right\}.$$

Τώρα, $\varphi_{Q_{j/P}}^{l+1-m}\in G'_{Z_j}$ αν και μόνο αν $l+1-m\equiv 0\,(\mathrm{mod}\, f\left(q_i/P\right))$. Επομένως,

$$B_j = \begin{bmatrix} 0 & c_j & & & 0 \\ \vdots & 0 & c_j & & \\ & & \ddots & \ddots & \\ & 0 & & 0 & c_j \\ D_j & & & & 0 \end{bmatrix}.$$

Για $l:=f\left(q_j/P\right)-1$ και για $m=0$ παίρνουμε το

$$D_j = \sum_{\tau\in G'_{T_j}} R\left(\varphi_{Q_{j/q_j}}\tau\right) = R\left(\varphi_{Q_{j/q_j}}\right)\cdot c_j,$$

όπου $c_j=\sum_{t\in G'_{T_j}} R(\tau)$. (Υπενθυμίζουμε ότι χρησιμοποιήσαμε την γνωστή ιδιότητα Frobenius $\varphi_{Q_{j/P}}^{f(q_j/P)}=\varphi_{Q_{j/q_j}}$.)

Συνοψίζοντας όλα τα παραπάνω, έχουμε:

$$\det\left[\mathrm{Id}_{V^*}-\frac{1}{e\left(Q/P\right)}\cdot NP^{-s}\cdot\sum_{\tau\in G_T}\rho^*\left(\varphi_{Q/P}\cdot\tau\right)\right] \;=\; \prod_{j=1}^{t}\det\left(I-\frac{NP^{-s}}{e\left(Q/P\right)}\cdot A_j\right),$$

$$\det\left(I-\frac{NP^{-s}}{e\left(Q/P\right)}\cdot A_j\right) \;=\; \det\left(I-e\left(\frac{q_j}{P}\right)\cdot\frac{NP^{-s}}{e\left(Q/P\right)}\cdot B_j\right)$$

και

$$\det\left(I-e\left(q_j/P\right)\cdot\frac{NP^{-s}}{e\left(Q/P\right)}\cdot B_j\right) \;=\; \det\begin{bmatrix} I & -p_jc_j & & 0\\ & \ddots & \ddots & \\ & & \ddots & \ddots & \\ & 0 & & \ddots & -p_jc_j\\ -p_jD_j & 0 & \cdots\cdots & & I \end{bmatrix},$$

όπου $p_j:=\dfrac{NP^{-s}}{e\left(Q_j/q_j\right)}$ $\left(e\left(Q/P\right):=e\left(Q_j/P\right)=e\left(Q_j/q_j\right)\cdot e\left(q_j/P\right)\right)$. Τελικά,

$$\begin{aligned}
\det\left(I-\frac{NP^{-s}}{e\left(q/P\right)}\cdot A_j\right) &= \det\left(I-p_j\cdot D_j\cdot\left(p_j\cdot c_j\right)^{f(q_i/p)-1}\right)\\
&= \det\left(I-R(\varphi_{Q_j/q_j})\cdot\left(p_j\cdot c_j\right)^{f(q_j/p)}\right)\\
&= \det\left(I-Nq_j^{-s}\cdot R(\varphi_{Q_j/q_j})\cdot\left[\frac{1}{e\left(Q_j/q_j\right)}\cdot\sum_{\tau\in G'_{T_j}}R(\tau)\right]^{f(q_j/P)}\right)\\
&= \det\left(\mathrm{Id}_V-Nq_j^{-s}\cdot\rho(\varphi_{Q_j/q_j})\right)\cdot\Phi_j^{f(q_j/p)}\\
&= \det\left(\mathrm{Id}_V-Nq_j^{-s}\cdot\rho(\varphi_{Q_j/q_j})\circ\Phi_j\right),
\end{aligned}$$

δηλαδή το θεώρημα. □

Πόρισμα 6.2.11 *Έστω L/K μία επέκταση του Galois αλγεβρικών σωμάτων αριθμών. Ισχύει*

$$\zeta_L(s)=\zeta_K(s)\cdot\prod_{\substack{\chi\ \text{ανάγ.}\\ \chi\neq\chi_0}}L\left(s,\chi,L/K\right)^{\chi(1)},$$

όπου το χ διατρέχει όλους τους **ανάγωγους** *χαρακτήρες της $G\left(L/K\right)$, $\chi\neq\chi_0$.*

Απόδειξη: Έστω L' ενδιάμεσο σώμα τέτοιο ώστε $K \subseteq L' \subseteq L$ και L'/K Galois. Αν χ_0 ο τετριμμένος χαρακτήρας της $G(L/L')$, $\chi_0(g) = 1$ για κάθε $g \in G(L/L') = H$. Η L'/K είναι επέκταση του Galois. Επομένως η H είναι κανονική υποομάδα της $G = G(L/K)$.

Το θεώρημα 6.2.6 λοιπόν δίνει: Ο $\mathrm{Ind}_H^G \chi_0$ είναι ο χαρακτήρας που είναι lifted από τον **ομαλό** (regular) χαρακτήρα χ_r της $G/H = \mathrm{Gal}(L'/K)$. Επομένως,

$$\begin{aligned} \zeta_{L'}(s) &= \prod_{Q' \in \mathbb{P}(L')} \left(1 - NQ'^{-s}\right)^{-1} \\ &= L\big(s, \chi_0, L/L'\big) \\ &\overset{\vartheta.6.2.8}{=} L\big(s, \mathrm{Ind}_H^G \chi_0, L/K\big) \\ &\overset{\vartheta.6.2.5}{=} L\big(s, \chi_r, L'/K\big). \end{aligned}$$

Τώρα, έστω $L' = L, \Rightarrow \chi_r = \mathrm{Ind}_H^G \chi_0$ ο ομαλός (regular) χαρακτήρας της $G(L/K)$. Επομένως

$$\begin{aligned} \chi_r &= \sum_{\chi \text{ ανάγ.}} \chi(1) \cdot \chi \qquad \text{(δες [16], σελίδα 96, θεώρημα 6.1.4)} \\ \Longrightarrow \quad \zeta_L(s) &= L\big(s, \sum_{\chi \text{ ανάγ.}} \chi(1) \cdot \chi, L/K\big) \\ &\overset{\vartheta.6.2.4}{=} \prod_{\chi \text{ ανάγ.}} L\big(s, \chi, L/K\big)^{\chi(1)}. \end{aligned}$$

Αν χ_0 ο **κύριος** χαρακτήρας της $G(L/K)$ ($\chi_0(g) = 1 \ \forall g \in G$) έχουμε $\chi_0(1) = 1$, οπότε:

$$\begin{aligned} \zeta_L(s) &= L\big(s, \chi_0, L/K\big) \cdot \prod_{\substack{\chi \text{ ανάγ.} \\ \chi \neq \chi_0}} L\big(s, \chi, L/K\big)^{\chi(1)} \\ &= \zeta_K(s) \cdot \prod_{\substack{\chi \text{ ανάγ.} \\ \chi \neq \chi_0}} L\big(s, \chi, L/K\big)^{\chi(1)} \end{aligned}$$

□

Το αρχικό πρόβλημα που ενδιέφερε τον Artin ήταν αν είναι σωστή η εικασία ότι $\zeta_L(s)/\zeta_K(s)$ είναι ολόμορφη σ΄ όλο το μιγαδικό επίπεδο.

Το τελευταίο πόρισμα μάς δείχνει ότι η ολομορφία της $\zeta_L(s)/\zeta_K(s)$ θα ήταν άμεση συνέπεια της:

ΕΙΚΑΣΙΑΣ ΤΟΥ ARTIN: Για κάθε **ανάγωγο** χαρακτήρα $\chi \neq \chi_0$ η L-σειρά του Artin

$$L\big(s, \chi, L/K\big)$$

επεκτείνεται ολόμορφα σ΄ όλο το $\mathbb{C}$.

Τι γνωρίζουμε μέχρι σήμερα για την εικασία του Artin;

Κατ΄ αρχήν θα ήταν ίσως ευκταία η απόδειξη της **μερόμορφης επέκτασης** της $L(s,\chi,{}^{L}\!/_{K})$ σ΄ όλο το $\mathbb{C}$. Παρά την προσπάθειά του ο Artin δεν τα κατάφερε. Η απόδειξη ήρθε αργότερα από τον R. Brauer.

Το σύνολο των χαρακτήρων μιάς ομάδας G είναι κλειστό ως προς την **πρόσθεση** και ως προς τον **πολλαπλασιασμό**. Για λόγους ευκολίας ορίζουμε σαν "χαρακτήρα" και την **διαφορά** δύο χαρακτήρων. Τέτοιους χαρακτήρες θα τους λέμε **γενικευμένους χαρακτήρες**. Ένας γενικευμένος χαρακτήρας της G είναι λοιπόν μία συνάρτηση κλάσεων (class function) της G (μιγαδική, αφού εμείς δουλεύουμε στο $\mathbb{C}$). Το ερώτημα είναι: **Πότε** μία συνάρτηση κλάσεων (class function) θ της G είναι γενικευμένος χαρακτήρας της G; Εξ ορισμού, αν χ είναι ένας γενικευμένος χαρακτήρας της G και $H \leq G$ (τυχούσα) τότε $\chi\big|_H$ είναι επίσης γενικευμένος χαρακτήρας της G. Δηλαδή ο χ θα είναι γενικευμένος χαρακτήρας **κάθε** υποομάδας H της G. Το θεώρημα του Brauer βεβαιώνει και το αντίστροφο: Αν χ συνάρτηση κλάσεων (class function) της G τέτοια ώστε ο περιορισμός $\chi\big|_E$ είναι γενικευμένος χαρακτήρας της G για **όλες** τις στοιχειώδεις (elementary) υποομάδες της E, τότε ο χ είναι γενικευμένος χαρακτήρας της G.

Η αλήθεια της παραπάνω πρότασης είναι άμεση συνέπεια του:

Θεώρημα 6.2.12 (Θεμελιώδες θεώρημα του Brauer) *Κάθε χαρακτήρας της G είναι γραμμικός συνδυασμός χαρακτήρων της G με* **συντελεστές από το** $\mathbb{Z}$*, οι οποίοι χαρακτήρες* **επάγονται** *από* **γραμμικούς** *(μονοδιάστατους!) χαρακτήρες των στοιχειωδών (elementary) υποομάδων της G.*

Απόδειξη: (Δες [3], σελίδα 135, [16], σελίδες 160-170.) □

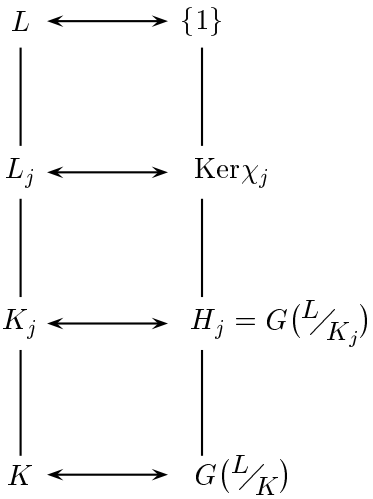
Ορισμός 6.2.13 *Μία ομάδα E θα λέγεται* **στοιχειώδης** *(elementary) όταν είναι ευθύ γινόμενο μιάς* **p-ομάδας** *και μιάς* **κυκλικής** **q-ομάδας**, $p,q \in \mathbb{P}$, $p \neq q$.

Έστω τώρα $\chi \neq \chi_0$ ανάγωγος χαρακτήρας της $G({}^{L}\!/_{K})$. Τον γράφουμε, σύμφωνα με το θεώρημα του Brauer, στην μορφή

$$\chi = \sum_{j=1}^{k} m_j \chi_j^*$$

όπου $m_j \in \mathbb{Z}$ και χ_j^* ο επαγόμενος χαρακτήρας του **γραμμικού** χαρακτήρα χ_j της στοιχείώδους (elementary) υποομάδας H_j της G.

Έστω K_j το σώμα σταθερών στοιχείων της H_j και L_j το σώμα των σταθερών στοιχείων του $\operatorname{Ker}\chi_j$.



Η επέκταση L_j/K_j είναι **κυκλική** και ο μονοδιάστατος χαρακτήρας της χ_j είναι **lifted** του **γραμμικού πιστού** χαρακτήρα,

$$\begin{aligned} \chi'_j : G(L_j/K_j) = H_j/\operatorname{Ker}\chi_j &\longrightarrow \mathbb{C} \\ \text{όπου} \quad \sigma\cdot\operatorname{Ker}\chi_j &\longmapsto \chi_j(\sigma). \end{aligned}$$

Λόγω των θεωρημάτων 6.2.4, 6.2.8 και 6.2.5 έχουμε:

$$\begin{aligned} L(s,\chi,L/K) &= \prod_{j=1}^{k} L(s,\chi_j^*,L/K)^{m_j} \\ &= \prod_{j=1}^{k} L(s,\chi_j,L/K_j)^{m_j} \\ &= \prod_{j=1}^{k} L(s,\chi'_j,L_j/K_j)^{m_j}. \end{aligned}$$

Τώρα L_j/K_j είναι **κυκλική** και χ'_j ένας χαρακτήρας της, άρα από το θεώρημα 6.2.2 συνεπάγεται ότι

$$L(s,\chi'_j,L_j/K_j) \;=\; L(s,\tilde{\chi}_j).$$

Τελικά έχουμε:

$$\boxed{L(s,\chi,L/K) \;=\; \prod_{j=1}^{k} L(s,\tilde{\chi}_j)^{m_j}}$$

δηλαδή το "θαύμα" οι L-σειρές του Artin να είναι γινόμενο δυνάμεων **αβελιανών L-σειρών** με **εκθέτες ακεραίους**.

Το παραπάνω θεώρημα σε συνδυασμό με το θεώρημα 4.2.3, 4., σελίδα 99 μας δίνει το

Θεώρημα 6.2.14 *Για κάθε* **ανάγωγο** *χαρακτήρα* χ *της* $G(L/K)$, $\chi \neq \chi_0$, *η* $L(s,\chi,L/K)$ **επεκτείνεται μερόμορφα σ' όλο το μιγαδικό επίπεδο**.

Σημείωση: Αν το θεώρημα του Brauer μάς εξασφάλιζε $m_j \in \mathbb{N}$, θα είχαμε σαν συμπέρασμα την εικασία του Artin. Εδώ ας σημειωθεί ότι η παράσταση $\chi = \sum m_j \chi_j^*$ **δεν** είναι μοναδική.

Ας επαναλάβουμε λοιπόν το ερώτημα: **Τί είναι γνωστό για την εικασία του Artin;**

(α′) Είναι γνωστή για παραστάσεις ρ **διάστασης** 1. Σ' αυτήν την περίπτωση ταυτίζονται οι L-σειρές του Artin μ' αυτές του Hecke για τις οποίες είναι γνωστή η ολόμορφη επέκταση. Τις σειρές του Hecke δεν θα τις ορίσουμε εδώ. Απλά μόνο θα υπενθυμίσουμε ότι η ταυτότητα αυτή είναι ο **νόμος αντιστροφής του Artin**. Οι Artin και Hecke, παρά το ότι εργάζονταν στο ίδιο πανεπιστήμιο (Hamburg), ουδέποτε συνειδητοποίησαν της διασυνδέσεις που είχαν τα ερευνητικά τους αποτελέσματα. Αυτό έγινε για πρώτη φορά από τον Langlands αρχής γενομένης από την δεκαετία του 60 του οποίου η "φιλοσοφία" έχει σαν στόχο την δημιουργία μιάς **μη-αβελιανής class field theory**.

(β′) Για μερικές παραστάσεις διάστασης 2, συγκεκριμένα για εκείνες που η προβολική εικόνα της $G(L/K)$ μέσω της ρ, $\tilde{\rho}(G(L/K)) \cong D_{2n}, A_4, S_4$,

$$\begin{array}{ccc} G & \xrightarrow{\ \rho\ } & \mathrm{GL}_2(\mathbb{C}) \\ & \searrow^{\tilde{\rho}} & \downarrow \\ & & P\mathrm{GL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^* \end{array}$$

(D_{2n} είναι η δίεδρη ομάδα τάξης $2n$.) Για τις A_4, S_4 τα αποτελέσματα είναι της δεκαετίας του 70, αρχές δεκαετίας του 80 και οφείλονται στους Langlands, Tunnell.

Μερικά συγκεκριμένα παραδείγματα είναι γνωστά στην περίπτωση του $\tilde{\rho}(G) = A_5$ και οφείλονται στον J. Buhler (Lecture Notes in Math. **654** (1978)). Επίσης παραπέμπουμε τον ενδιαφερόμενο αναγνώστη στο [12].

Ένα σημαντικό πρόσφατο αποτέλεσμα σχετικά με την εικασία του Artin είναι το ακόλουθο:

Θεώρημα 6.2.15 (K. Buzzard, M. Dickinson, N. Shepherd-Barron, R. Taylor) *Αν* $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{C})$ **ανάγωγη** *παράσταση Galois και* $\tilde{\rho} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow PGL_2(\mathbb{C})$ *η επαγόμενη προβολική παράσταση της* ρ *τέτοια ώστε*

1. *Η εικόνα της* $\tilde{\rho}$, $Im(\tilde{\rho})$, *να είναι ισόμορφη προς την ομάδα* A_5,

2. η $\tilde{\rho}$ να είναι μη-διακλαδιζομένη στους πρώτους 2 και 5, και

3. ο αυτομορφισμός του Frobenius της $\tilde{\rho}$ στον πρώτο 2 έχει τάξη 3

τότε η ρ **επαληθεύει την εικασία του Artin**.

Σημείωση 6.2.16 *Το αποτέλεσμα αυτό είναι υπό δημοσίευση. Ανακοινώθηκε στο Συνέδριο της Journees Arithmetiques τον Ιούλιο του 1999 στη Ρώμη.*

Θα πρέπει ακόμη να παρατηρήσουμε ότι η L-σειρά του Artin ορίζεται **τοπικά**, δηλαδή κατ' αρχήν για **κάθε** $P \in \mathbb{P}(K)$. Μία μη-τοπική προσέγγιση όπως στις αβελιανές L-σειρές **δεν** είναι μέχρι σήμερα γνωστή. Ίσως πάντως αυτός είναι ο λόγος που μας δημιουργεί δυσκολίες στην επέκτασή της σ' όλο το $\mathbb{C}$.

Τέλος θα πρέπει να πούμε ότι η L-σειρά του Artin πολλαπλασιασμένη με κατάλληλους "Γ-παράγοντες" δίνει την $\Lambda\left(s, \chi, {}^{L}\!/_{K}\right)$ για την οποία **έχουμε** μία **συναρτησιακή εξίσωση**

$$\Lambda\left(s, \chi, {}^{L}\!/_{K}\right) \;=\; W(x)\Lambda(1-s, \overline{\chi})$$

όπου $W(\chi)$ μία σταθερά με $|W(\chi)| = 1$ (Artin's **Wurzelzahl**), η οποία έχει θεμελιώδες αριθμητικό περιεχόμενο.

Θα κλείσουμε την παράγραφο με ένα **παράδειγμα**. Έστω $G = G\left({}^{L}\!/_{K}\right) \cong S_3$. Η S_3 έχει 3-κλάσεις συζυγίας: $C_1 : (1)$, $C_2 : (1,2,3), (3,2,1)$ και $C_3 : (1,2), (2,3), (3,1)$. Επομένως έχει 3-ανάγωγους χαρακτήρες. Έστω ψ_1 ο **κύριος**, ψ_2 αυτός που στέλνει τα στοιχεία του $C_1 \cup C_2$ στο $+1$ και τα στοιχεία της C_3 στο -1.

Οι ψ_1, ψ_2 είναι μονοδιάστατοι $1^2 + 1^2 + n_3^2 = \#\left|S_3\right| = 6 \implies n_3 = 2 \implies$ ο ψ_3 θα είναι διάστασης 2. Οι σχέσεις ορθογωνιότητας (θεώρημα (6.1.8), σελίδα 123) δίνουν:

$$\psi_1(g) + \psi_2(g) + 2\psi_3(g) = \begin{cases} 6, & \text{όταν } g = 1 \\ 0, & \text{αλλιώς.} \end{cases}$$

Πίνακας των χαρακτήρων

	ψ_1	ψ_2	ψ_3
C_1	1	1	2
C_2	1	1	-1
C_3	1	-1	0

Υπολογίζουμε τώρα τους επαγόμενους χαρακτήρες χ^* που αντιστοιχούν στους χαρακτήρες χ των υποομάδων της S_3.

(i) $H = A_3$

	χ_1^*	χ_2^*	χ_3^*
C_1	2	2	2
C_2	2	-1	-1
C_3	0	0	0

(ii) $H = \{1, (1,2)\}$

	χ_4^*	χ_5^*
C_1	3	3
C_2	0	0
C_3	1	-1

(iii) $H = \{1\}$

	χ_6^*
C_1	6
C_2	0
C_3	0

Από τους παραπάνω πίνακες βλέπει κανείς ότι έχουμε τις ακόλουθες σχέσεις:

$$\chi_1^* = \psi_1 + \psi_2, \qquad \chi_2^* = \chi_3^* = \psi_3,$$

$$\chi_4^* = \psi_1 + \psi_3, \qquad \chi_5^* = \psi_2 + \psi_3 \qquad \text{και}$$

$$\chi_6^* = \psi_1 + \psi_2 + 2\psi_3.$$

Η S_3 τώρα είναι η ομάδα του Galois κάθε μη-αβελιανής επέκτασης του Galois ${}^{L}\!/_{K}$ βαθμού 6. Αν K_1 και K_2 είναι τα σώματα σταθερών στοιχείων των A_3 και $\{1, (12)\}$ αντίστοιχα, τότε $[K_1 : K] = 2$ και $[K_2 : K] = 3$, επομένως ${}^{L}\!/_{K_1}$ και ${}^{L}\!/_{K_2}$ αβελιανές επεκτάσεις.

Ακόμη ${}^{K_1}\!/_{K}$ επίσης αβελιανή: Έχουμε λοιπόν

$$\begin{aligned}
\zeta_L(s) &= L\big(s, \chi_0, {}^{L}\!/_{L}\big) \\
&= L\big(s, \psi_1 + \psi_2 + 2\psi_3, {}^{L}\!/_{K}\big) \\
&= L\big(s, \psi_1, {}^{L}\!/_{K}\big) \cdot L\big(s, \psi_2, {}^{L}\!/_{K}\big) \cdot L\big(s, \psi_3, {}^{L}\!/_{K}\big)^2
\end{aligned}$$

$$\begin{aligned}
\zeta_{K_1}(s) &= L\big(s, \chi_0, {}^{L}\!/_{K_1}\big) \\
&= L\big(s, \psi_1 + \psi_2, {}^{L}\!/_{K_1}\big) \\
&= L\big(s, \psi_1, {}^{L}\!/_{K}\big) \cdot L\big(s, \psi_2, {}^{L}\!/_{K}\big)
\end{aligned}$$

$$\begin{aligned}
\zeta_{K_2}(s) &= L\big(s, \chi_0, {}^{L}\!/_{K_2}\big) \\
&= L\big(s, \psi_1 + \psi_3, {}^{L}\!/_{K}\big) \\
&= L\big(s, \psi_1, {}^{L}\!/_{K}\big) \cdot L\big(s, \psi_3, {}^{L}\!/_{K}\big)
\end{aligned}$$

και

$$\zeta_K(s) \;=\; L\big(s,\chi_0,{}^{L}\!/_{K}\big) = L\big(s,\psi_1,{}^{L}\!/_{K}\big).$$

Λόγω των γνωστών ιδιοτήτων τώρα έχουμε

$$L\big(s,\psi_2,{}^{L}\!/_{K}\big) \;=\; L\big(s,\chi_5,{}^{K_1}\!/_{K}\big)$$

και

$$L\big(s,\psi_3,{}^{L}\!/_{K}\big) = L\big(s,\chi_2,{}^{L}\!/_{K_1}\big)$$

Επομένως οι $L\big(s,\psi_2,{}^{L}\!/_{K}\big)$ και $L\big(s,\psi_3,{}^{L}\!/_{K}\big)$ είναι ολόμορφες συναρτήσεις. Συμπτωματικά, το παράδειγμα δείχνει ότι η εικασία του Artin είναι σωστή για $\mathrm{Gal}\big({}^{L}\!/_{K}\big) = S_3$.

Μέσω της παραπάνω θεωρίας βρίσκουμε σχέσεις ανάμεσα στις ζήτα συναρτήσεις αλγεβρικού σώματος αριθμών L και των υποσωμάτων αυτού. Σχέσεις ανάμεσα στις διακρίνουσες και του ομαλοποιητή (Regulator) του L και των υποσωμάτων μάς δίνουν **σχέσεις** ανάμεσα στους **αριθμούς κλάσεων**. Προς αυτή την κατεύθυνση έχουμε πολλές εργασίες.

Η πρώτη είναι η R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisscher Körpers, Math. Nach. **4** (1951), 158-174. Αναφέρουμε και μία πρόσφατη: Ch. Parry, Bicyclic Bicubic Fields, Can. J. Math. Vol XLII (1990), 491-507.

6.3 Δύο λόγια για τις εικασίες του Stark

Σε μία σειρά τεσσάρων πολύ σημαντικών εργασιών ο H. M. Stark στο Advances in Mathematics (από το 1971 μέχρι το 1980) επεξέτεινε την θεωρία και διατύπωσε εικασίες για τον σταθερό όρο του αναπτύγματος Taylor μιάς L-σειράς του Artin στην θέση $s = 0$. Τις εικασίες του αυτές απέδειξε στην περίπτωση που το σώμα $K = \mathbb{Q}$ ή τετραγωγικό μιγαδικό σώμα αριθμών. Σε ειδικές περιπτώσεις σημαντική είναι η συνεισφορά του Sands (δεκαετία του 80). Οι εικασίες μπορούν να θεωρηθούν σαν πολύ **πλατειά** και **βαθειά** γενίκευση του **τύπου για τον αριθμό κλάσεων του Dirichlet** και του **limit formula του Kronecker**. Ο Stark προτιμά την τιμή της L-σειράς στην θέση $s = 0$ και όχι $s = 1$. Τα επιχειρήματά του θα τα δείτε στο άρθρο του Values of Zeta and L-functions (Dedekinds Festschrift, Braunschweig 1981).

Φυσικά η μελέτη αυτή στην θέση $s=0$ δεν ήταν δυνατή την εποχή του Dedekind, διότι η συναρτησιακή εξίσωση της $\zeta_K(s)$ αποδείχθηκε για πρώτη φορά το 1917 από το Hecke και των L-σειρών του Artin στην δεκαετία του 1920.

Ξαναθυμίζουμε ότι, αν K αλγεβρικό σώμα αριθμών τότε

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot h_K\cdot \mathrm{Reg}K}{w\sqrt{|D_K|}}, \tag{1}$$

όπου $n=(K:\mathbb{Q})=r_1+2r_2$. Έστω τώρα

$$\xi_K(s) := \left(\frac{|D_K|}{2^{2r_2}\pi^n}\right)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s). \tag{2}$$

Η συναρτησιακή εξίσωση τότε είναι:

$$\xi_K(s) = \xi_K(1-s). \tag{3}$$

Από τις (1) και (2) συνεπάγεται ότι

$$\begin{aligned}\lim_{s\to 1}(s-1)\xi_K(s) &= \frac{|D_K|^{1/2}}{2^{r_2}\pi^{n/2}}\cdot\pi^{r_{1/2}}\cdot\frac{2^{r_1+r_2}\pi^{r_2}h_K\cdot R}{w\sqrt{|D_K|}}\\ \left.\begin{array}{c}\Gamma(1/2)=\sqrt{\pi}\\ \Gamma(1)=1\\ n/2=r_1/2+r_2\end{array}\right| &= 2^{r_1}\frac{h_K\cdot\mathrm{Reg}K}{w}.\end{aligned}$$

Η (3) συνεπάγετει ότι

$$\begin{aligned}\lim_{s\to 1}(s-1)\xi_K(s) &= \lim_{s\to 1}(s-1)\xi_K(1-s)\\ &= \lim_{s\to 0}(-s)\xi_K(s)\\ &= 2^{r_1}\cdot\frac{h_K\cdot\mathrm{Reg}_K}{w}\end{aligned}$$

Αλλά

$$\lim_{s\to 0}(-s)\xi_K(s) = \lim_{s\to 0}(-s)\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s).$$

Η $\zeta_K(s)$ είναι ολόμορφη στο $s=0$, η Γ-συνάρτηση όμως έχει στις θέσεις $-m, m\in\mathbb{N}_0$ πόλους πρώτης τάξης με υπόλοιπα

$$\lim_{z\to -m}(z+m)\Gamma(z)=\frac{(-1)^m}{m!}. \tag{4}$$

(δες [30], σελίδα 261).

Το υπόλοιπο στην θέση $s=0$ είναι λοιπόν 1, οπότε:

$$\begin{aligned}\lim_{s\to 0}(-s)\xi_K(s) &= \lim_{s\to 0}\frac{\zeta_K(s)}{s^{r_1r_2-1}}\cdot\frac{1}{2^{r_1}}\cdot\left[\frac{s}{2}\Gamma\left(\frac{s}{2}\right)\right]^{r_1}\cdot[s\cdot\Gamma(s)]^{r_2}\\ &= -\frac{1}{2^{r_1}}\cdot\lim_{s\to 0}\frac{\zeta_K(s)}{s^r}\end{aligned}$$

με $r := r_1 + r_2 - 1$. Έχουμε λοιπόν:

$$\boxed{\lim_{s\to 0} \frac{\zeta_K(s)}{s^r} = -\frac{h_K \cdot \mathrm{Reg}_K}{w}} \tag{5}$$

Έστω τώρα L/K επέκταση του Galois αλγεβρικών σωμάτων αριθμών, $G = G\left(L/K\right)$, και χ ένας χαρακτήρας κάποιας παράστασης της G.

Ξαναθυμούμαστε αυτό που είπαμε, και δεν αποδείξαμε πιό μπροστά, ότι αν

$$\xi(s,\chi) \;=\; \big(\text{κατάλληλοι } \Gamma\text{-παράγοντες}\big)\cdot L\big(s,\chi,L/K\big)$$

τότε

$$\xi(1-s,\overline{\chi}) \;=\; W(\chi)\xi(s,\chi) \tag{6}$$

όπου $\big|W(\chi)\big| = 1$.

Για τους προσεκτικούς και ακριβολόγους,

$$\xi(s,\chi) = \left(|D_K|\cdot N\mathfrak{f}/\pi^{n(K)\chi(1)}\right)^{s/2}\Gamma\left(\frac{s}{2}\right)^a\left(\Gamma\left(\frac{s+1}{2}\right)^b\cdot L\big(s,\chi,L/K\big)\right)$$

όπου $\mathfrak{f}$ είναι ο **οδηγός** του χ ως προς το K, $n(K) = (K:Q)$ και $a+b = n(K)\cdot\chi(1)$.

Εικασία του Stark

Έστω ότι ο χ **δεν** περιέχει τον χ_1 στην ανάλυσή του σε ανάγωγους. Τότε

$$L\big(1,\chi,L/K\big) \;=\; \frac{W(\overline{\chi})\cdot 2^a\cdot\pi^b}{(|D_K|N\mathfrak{f})^{1/2}}\cdot\Theta(\overline{\chi})\cdot R(\overline{\chi})$$

ή ισιδύναμα,

$$\lim_{s\to 0}\frac{L\big(s,\chi,L/K\big)}{s^\alpha} \;=\; \Theta(x)\cdot R(x)$$

όπου $\Theta(\chi)\in\tilde{\mathbb{Q}}$ (αλγεβρικός αριθμός) και $R(\chi)$ η **ορίζουσα** ενός $a\times a$ πίνακα του οποίου τα στοιχεία είναι **γραμμικές μορφές από λογαρίθμους απολύτων τιμών μονάδων του σώματος K και των συζυγών του**.

Έστω τώρα $K = \mathbb{Q}$ και $\sigma_0 \in \mathrm{Gal}\big(L/\mathbb{Q}\big)$ ο $\mathbb{Q}$-αυτομορφισμός του L που στέλνει τα στοιχεία του L στα μιγαδικά συζυζή τους αν $L \not\subseteq \mathbb{R}$ και $\sigma_0 = 1$ αλλιώς.

Έστω $A(\sigma) = (a_{ij}(\sigma))$, $\sigma\in G$, μία παράσταση με πίνακες της $G\big(L/\mathbb{Q}\big)$ η οποία έχει σαν χαρακτήρα τον χ. Μπορούμε να υποθέσουμε ότι ο $A(\sigma)$ εκλέχτηκε έτσι ώστε

$$A(\sigma_0) = \begin{pmatrix} I_a & 0 \\ 0 & -I_b \end{pmatrix}$$

Υπάρχει μία μονάδα ε του L τέτοια ώστε $\sigma_0(\varepsilon) = \varepsilon$ και υπάρχει ακριβώς μία σχέση ανάμεσα στις $r(L)+1$ μονάδες $\varepsilon^{\sigma-1}$ για $\sigma \in G_0$, όπου G_0 πλήρες σύστημα αριστερών αντιπροσώπων της G, G modulo την υποομάδα $\{1, \sigma_0\}$, και η σχέση αυτή είναι

$$\prod_{\sigma \in G_0} \varepsilon^{\sigma^{-1}} = \pm 1.$$

Έστω τώρα

$$\left| \begin{array}{l} c_{ij} := \sum_{\sigma \in G} a_{ij}(\sigma) \log |\varepsilon^{\sigma}| \\ 1 \leq i \leq a \\ 1 \leq j \leq b \end{array} \right. \tag{7}$$

Με τα c_{ij} όπως στην (7) έχουμε

Θεώρημα 6.3.1 (Θεώρημα του Stark) *Έστω χ* **ρητός** *χαρακτήρας. Τότε η εικασία ισχύει για*

$$R(\chi) = R(\chi, \varepsilon) = \det(c_{ij}).$$

Ορισμός 6.3.2 *Ο χαρακτήρας χ θα λέγεται* **ρητός** *όταν παίρνει τιμές στο $\mathbb{Q}$, δηλαδή όταν για κάθε σ της ομάδας του Galois $G(L/K)$ ισχύει $\chi^{\sigma} = \chi$.*

Ένα σπουδαίο βιβλίο για κάποιο ανάλογο σεμινάριο είναι το [39]. Τέλος αναφέρουμε και το πιο πρόσφατο [32].

ΤΕΛΟΣ

Βιβλιογραφία

[1] Lars V. Ahlfors, *Complex Analysis*, McGraw-Hill, London 1979.

[2] Γιάννη Α. Αντωνιάδη, *Θεωρία Αριθμών Ι, Αλγεβρική Θεωρία Αριθμών*, Σημειώσεις, Πανεπιστήμιο Κρήτης, Ηράκλειο 1988.

[3] Γιάννη Α. Αντωνιάδη, *Θεωρία Παραστάσεων Πεπερασμένων Ομάδων*, Έκδοση ΕΠΕΑΕΚ "Προμηθέας", Πανεπιστήμιο Κρήτης, Ηράκλειο 1998.

[4] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York 1976.

[5] Tom M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Springer-Verlag, New York 1976.

[6] Emil Artin, *The Gamma Function*, Holt-Rinehart-Winston, New York 1964.

[7] Emil Artin, John Tate, *Class Field Theory*, W. A. Benjamin, London, 1967.

[8] Senon I. Borewicz, Igor R. Šafarevič, *Zahlentheorie*, Birkhäuser, Basel, 1966.

[9] J. W. S. Cassels, A. Fröhlich (editors), *Algebraic Number Theory*, Academic Press, London 1967.

[10] Komaravolu Chandrasekharan, *Introduction to Analytic Number Theorey*, Springer-Verlag, Berlin 1968.

[11] David A. Cox, *Primes of the Form $x^2 + ny^2$, Fermat, Class Field Theory and Complex Multiplication*, John Wiley and Sons, New York 1989.

[12] Gerhard Frey (editor), *On Artin's Conjecture for Odd 2-Dimensional Representations*, L.N.M. 1585, Springer-Verlag, Berlin 1994.

[13] A. Fröhlich (editor), *Algebraic Number Fields, L-Functions and Galois Properties*, Academic Press, London 1977.

[14] A. Fröhlich, M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, Cambridge 1993.

[15] Larry J. Goldstein, *Analytic Number Theory*, Prentice-Hall, Englewood Cliffs 1971.

[16] Daniel Gorenstein, *Finite Groups*, Chelsea, New York 1980.

[17] Helmut Hasse, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg 1967.

[18] Helmut Hasse, *Zahlbericht*, Physica-Verlag, Würzburg 1970.

[19] Erich Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, New York 1981.

[20] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York 1990.

[21] Shokichi Iyanaga (editor), *The Theory of Numbers*, North-Holland, 1975.

[22] Gerald J. Janusz, *Algebraic Number Fields, Second Edition*, American Mathematical Society 1996.

[23] Serge Lang, *Algebraic Number Theory*, Addison-Wesley, New York 1970.

[24] Serge Lang, *Cyclotomic Fields*, Springer-Verlag, New York 1978.

[25] Serge Lang, *Cyclotomic Fields II*, Springer-Verlag, New York 1980.

[26] M. J. Lighthill, *Einführung in die Theorie der Fourier Analysis*, Bibliographisches Institut, Mannheim 1966.

[27] Robert Long, *Algebraic Number Theory*, Marcel Dekker, New York 1977.

[28] Falko Lorenz, *Algebraische Zahlentheorie*, Bibliographisches Institut, Mannheim 1993.

[29] Daniel A. Marcus, *Number Fields*, Springer-Verlag, Berlin 1977.

[30] A. I. Markushevich, *The Theory of Analytic Functions: A Brief Course*, Mir Publishers, Moscow 1983.

[31] Curt Meyer, *Einführung in die Theorie der Gammafunction*, παραδόσεις, χειμερινό εξάμηνο 1983/84, Κολωνία 1984.

[32] Ram M. Murty, Kumar V. Murty, *Non-Vanishing of L-functions and Applications*, Birkhäuser, Basel 1997.

[33] Jürgen Neukirch, *Klassenkörpertheorie*, Bibliographishes Institut, Mannheim 1969.

[34] Jürgen Neukirch, *Class Field Theory*, Springer-Verlag, Berlin 1986.

[35] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin 1992.

[36] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York 1973.

[37] Stephen S. Shatz, *Profinite Groups, Arithmetic, and Geometry*, Princeton University Press, Princeton 1972.

[38] Ian Stewart, David Tall, *Algebraic Number Theory*, Chapman and Hall, London 1979.

[39] John Tate, *Les Conjectures de Stark sur les Fonctions L d' Artin en* $s = 0$, Birkhäuser, Basel 1984.

[40] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York 1982.

[41] E. T. Whittaker, G. W. Watson, *A Course in Modern Analysis, 4th edition*, Cambridge University Press, Cambridge 1937.

[42] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa 1974.

[43] Wladyslaw Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag, Berlin 1990.

[44] Don B. Zagier, *Zetafunktionen und Quadratische Körper (Eine Einführung in die höhere Zahlentheorie)*, Springer-Verlag, Berlin 1981.