Μια Εισαγωγή στη Θεωρία Iwasawa

Δημήτριος Νούλας

Δεκέμβριος 2022

Ομάδες Κλάσεων Ιδεωδών

Μια αναδρομή από αλγεβρική θεωρία αριθμών

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$$

Σε ιδεώδη:

$$\begin{aligned}(2)(3) &= (1 - \sqrt{-5})(1 + \sqrt{-5}) \\ &= (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})\end{aligned}$$

$2\mathbb{Z}[\sqrt{-5}] = (2, 1+\sqrt{-5})^2 \qquad 3\mathbb{Z}[\sqrt{-5}] = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$

Ομάδες Κλάσεων Ιδεωδών

Κλασματικά Ιδεώδη

π.χ.

$$\frac{1}{3}\mathbb{Z} \subseteq \mathbb{Q}$$

Για K σώμα αριθμών ο δακτύλιος ακεραίων $\mathcal{O}_K$ είναι περιοχή Dedekind, δηλαδή όλα τα κλασματικά ιδεώδη είναι αντιστρέψιμα

$$I\{x \in K : xI \subseteq \mathcal{O}_K\} = (1)$$

$$C_K = \frac{\text{κλασματικά ιδεώδη}}{\text{κύρια ιδεώδη}}$$

Ομάδες Κλάσεων Ιδεωδών

Κλασματικά Ιδεώδη

π.χ.

$$\frac{1}{3}\mathbb{Z} \subseteq \mathbb{Q}$$

Για K σώμα αριθμών ο δακτύλιος ακεραίων $\mathcal{O}_K$ είναι περιοχή Dedekind, δηλαδή όλα τα κλασματικά ιδεώδη είναι αντιστρέψιμα

$$I\{x \in K : xI \subseteq \mathcal{O}_K\} = (1)$$

$$C_K = \frac{\text{κλασματικά ιδεώδη}}{\text{κύρια ιδεώδη}}$$

Iwasawa: $h_n = |C_K|$ κυρίως για $\mathbb{Z}_p$-επεκτάσεις.

P-adic L-functions

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

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

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

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

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

$\mathbb{Z}_p$-Επεκτάσεις

Ύπαρξη

$\mathbb{Q}_\infty \subseteq \mathbb{Q}(\zeta_{p^\infty})$:

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

και

$$\mathbb{Q}_\infty = \cup_n \mathbb{Q}_n \qquad \mathbb{Q}_n := \mathbb{Q}(\zeta_{p^{n+1}})^{(\mathbb{Z}/p\mathbb{Z})^\times}$$

με

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$$

$\mathbb{Z}_p$-Επεκτάσεις

Ύπαρξη

$\mathbb{Q}_\infty \subseteq \mathbb{Q}(\zeta_{p^\infty})$:

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

και

$$\mathbb{Q}_\infty = \cup_n \mathbb{Q}_n \qquad \mathbb{Q}_n := \mathbb{Q}(\zeta_{p^{n+1}})^{(\mathbb{Z}/p\mathbb{Z})^\times}$$

με

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$$

Για K τυχαίο σώμα αριθμών $K_\infty = K\mathbb{Q}_\infty$

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

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

Θεώρημα Iwasawa

Θεώρημα

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

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

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

Θεώρημα Iwasawa

Θεώρημα

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

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

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

Ιδέα: p-Sylow υποομάδα του C_{K_n} ως πεπερασμένα παραγόμενο Λ-πρότυπο, όπου $\Lambda := \mathbb{Z}_p[[T]]$ η άλγεβρα του Iwasawa.

- Αλγεβρική δομή των δακτυλίων $\Lambda_{\mathcal{O}} := \mathcal{O}_K[[T]]$ για $K/\mathbb{Q}_p$ πεπερασμένη επέκταση.
- «Κολλώντας» την πληροφορία που δίνει η θεωρία κλάσεων σωμάτων σε κάθε πεπερασμένο στρώμα βλέποντας το Λ ως προβολικό όριο ομαδοδακτυλίων.

Νόμος Αντιστροφής

Έστω K σώμα αριθμών, τότε υπάρχει το σώμα H_K που είναι η μέγιστη αβελιανή αδιακλάδιστη επέκταση του K και

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

Πρόταση (Αλγόριθμος Διαίρεσης)

Έστω $f, g \in \Lambda_{\mathcal{O}}$ *με* $f = a_0 + a_1 T + \cdots$ *με* $a_i \in \mathfrak{p} = (\pi)$ *για κάθε* $0 \leq i \leq n-1$ *και* $a_n \in \mathcal{O}_K^{\times}$. *Τότε υπάρχουν μοναδικά* $q \in \Lambda_{\mathcal{O}}$ *και* $r \in \mathcal{O}_K[T]$ *με βαθμό* $\deg r \leq n-1$ *έτσι ώστε*

$$g = qf + r$$

Πρόταση (Αλγόριθμος Διαίρεσης)

Έστω $f, g \in \Lambda_{\mathcal{O}}$ *με* $f = a_0 + a_1 T + \cdots$ *με* $a_i \in \mathfrak{p} = (\pi)$ *για κάθε* $0 \leq i \leq n-1$ *και* $a_n \in \mathcal{O}_K^{\times}$*. Τότε υπάρχουν μοναδικά* $q \in \Lambda_{\mathcal{O}}$ *και* $r \in \mathcal{O}_K[T]$ *με βαθμό* $\deg r \leq n-1$ *έτσι ώστε*

$$g = qf + r$$

Απόδειξη.

Τελεστής $\tau_n : \Lambda_{\mathcal{O}} \longrightarrow \Lambda_{\mathcal{O}}$

$$b_0 + b_1 T + b_2 T^2 + \cdots \longmapsto b_n + b_{n+1} T + b_{n+2} T^2 + \cdots$$

$$\tau_n(g) = \tau_n(qf)$$

$\square$

Distinguished Πολυώνυμα

Ορισμός

Έστω $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathcal{O}_K[T]$. *Θα λέμε το* $P(T)$ *είναι distinguished αν* $a_i \in (\pi)$ *για τα* $0 \leq i \leq n-1$.

Θεώρημα Προπαρασκευής του Weierstrass

Θεώρημα (p-adic Weierstrass Preparation Theorem)

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

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

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

$$f(T) = \pi^{\mu} P(T)U(T).$$

Περιοχή Μοναδικής Παραγοντοποίησης

$$\Lambda_{\mathcal{O}} : \mathrm{UFD}$$

ανάγωγα: π, ανάγωγα distinguished $P(T) \in \mathcal{O}[T]$

αντιστρέψιμα : $U(T) \in \Lambda_{\mathcal{O}}^{\times}$ αν $U(0) \in \mathcal{O}^{\times}$

Αλγεβρική Δομή

Περιοχή Μοναδικής Παραγοντοποίησης

$$\Lambda_{\mathcal{O}} : \mathrm{UFD}$$

$$\text{ανάγωγα:} \quad \pi, \text{ ανάγωγα distinguished } P(T) \in \mathcal{O}[T]$$

$$\text{αντιστρέψιμα :} \quad U(T) \in \Lambda_{\mathcal{O}}^{\times} \text{ αν } U(0) \in \mathcal{O}^{\times}$$

Λήμμα

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

Αλγεβρική Δομή

Περιοχή Μοναδικής Παραγοντοποίησης

$$\Lambda_{\mathcal{O}} : \text{UFD}$$

$$\text{ανάγωγα:} \quad \pi, \text{ ανάγωγα distinguished } P(T) \in \mathcal{O}[T]$$

$$\text{αντιστρέψιμα} : \quad U(T) \in \Lambda_{\mathcal{O}}^{\times} \text{ αν } U(0) \in \mathcal{O}^{\times}$$

Λήμμα

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

Λήμμα

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

Πρόταση

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

Αλγεβρική Δομή

Πρόταση

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

Απόδειξη.

Έχουμε τους ισομορφισμούς:

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

Κάθε άλλη περίπτωση ανάγεται σε αυτές. □

Άλγεβρική Δομή

Λήμμα

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

1. *Η φυσική απεικόνιση*

$$\Lambda_{\mathcal{O}}/(fg) \longrightarrow \Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g)$$

   είναι μονομορφισμός με πεπερασμένο συνπυρήνα.

2. *Υπάρχει εμφύτευση*

$$\Lambda_{\mathcal{O}}/(f) \oplus \Lambda_{\mathcal{O}}/(g) \longrightarrow \Lambda_{\mathcal{O}}/(fg)$$

   με πεπερασμένο συνπυρήνα.

Ψευδο-ισομορφισμός

Ορισμός

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

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

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

Ψευδο-ισομορφισμός

Ορισμός

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

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

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

Όχι Σχέση Ισοδυναμίας

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

$$(\pi, T) \sim \Lambda_{\mathcal{O}} \text{ αλλά } \Lambda_{\mathcal{O}} \nsim (\pi, T).$$

Θεώρημα Δομής

Θεώρημα (Δομής Πεπερασμένα Παραγόμενων $\Lambda_{\mathcal{O}}$-Προτύπων)

Έστω M ένα πεπερασμένα παραγόμενο $\Lambda_{\mathcal{O}}$-πρότυπο. Τότε

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

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

Στρώνουμε το έδαφος

Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση, για κάθε $n \geq 1$ η επέκταση K_∞/K_n παραμένει $\mathbb{Z}_p$-επέκταση. Θέτουμε

$$\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$$

και έστω $\gamma_0 \in \Gamma$ ένας τοπολογικός γεννήτορας.

$$x \in \mathbb{Z}_p \longmapsto \gamma_0^x \in \Gamma$$

Στρώνουμε το έδαφος

Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση, για κάθε $n \geq 1$ η επέκταση K_∞/K_n παραμένει $\mathbb{Z}_p$-επέκταση. Θέτουμε

$$\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$$

και έστω $\gamma_0 \in \Gamma$ ένας τοπολογικός γεννήτορας.

$$x \in \mathbb{Z}_p \longmapsto \gamma_0^x \in \Gamma$$

Έστω για κάθε K_n θεωρούμε ως L_n την μέγιστη αβελιανή αδιακλάδιστη p-επέκταση και θέτουμε $L = \cup_n L_n$

Στρώνουμε το έδαφος

Έστω K_∞/K μια $\mathbb{Z}_p$-επέκταση, για κάθε $n \geq 1$ η επέκταση K_∞/K_n παραμένει $\mathbb{Z}_p$-επέκταση. Θέτουμε

$$\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$$

και έστω $\gamma_0 \in \Gamma$ ένας τοπολογικός γεννήτορας.

$$x \in \mathbb{Z}_p \longmapsto \gamma_0^x \in \Gamma$$

Έστω για κάθε K_n θεωρούμε ως L_n την μέγιστη αβελιανή αδιακλάδιστη p-επέκταση και θέτουμε $L = \cup_n L_n$
και

$$X = \mathrm{Gal}(L/K_\infty)$$

$$G = \mathrm{Gal}(L/K)$$

Στρώνουμε το έδαφος

$$X_n = \mathrm{Gal}(L_n/K_n)$$

Στρώνουμε το έδαφος

$$X_n = \mathrm{Gal}(L_n/K_n)$$

είναι ισόμορφη με την p-Sylow υποομάδα της C_{K_n}.

Είτε ξεκινήσουμε από την K_∞/K ή την K_∞/K_n παίρνουμε το ίδιο X!

Λήμμα

Οι ομάδες διάσπασης και αδράνειας για άπειρη Galois επέκταση είναι κλειστές ως προς την τοπολογία Krull.

Λήμμα

Οι ομάδες διάσπασης και αδράνειας για άπειρη Galois επέκταση είναι κλειστές ως προς την τοπολογία Krull.

Υπενθυμίζουμε ότι για μια άπειρη Galois επέκταση M/N λέμε ότι ένας πρώτος $\mathfrak{p}$ του N διακλαδίζεται πλήρως αν υπάρχει μοναδικός πρώτος $\mathfrak{q}$ του M έτσι ώστε $I_{\mathfrak{q}} = I_{\mathfrak{q}|\mathfrak{p}} = \mathrm{Gal}(M/N)$.

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

Λήμμα

Οι ομάδες διάσπασης και αδράνειας για άπειρη Galois επέκταση είναι κλειστές ως προς την τοπολογία Krull.

Υπενθυμίζουμε ότι για μια άπειρη Galois επέκταση M/N λέμε ότι ένας πρώτος $\mathfrak{p}$ του N διακλαδίζεται πλήρως αν υπάρχει μοναδικός πρώτος $\mathfrak{q}$ του M έτσι ώστε $I_{\mathfrak{q}} = I_{\mathfrak{q}|\mathfrak{p}} = \mathrm{Gal}(M/N)$.

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

Πρόταση

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

Πρόταση

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

Πρόταση

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

Πρόταση

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

Πρόταση

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

Πρόταση

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

$$\mathrm{Gal}(L_nK_{n+1}/K_{n+1}) \cong \mathrm{Gal}(L_n/K_n)$$

$$L_nK_{n+1} \subset L_{n+1}$$

$$X_{n+1} \longrightarrow X_n$$

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

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

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

Δράση Συζυγίας

$$\Gamma_n := \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z} \cong \mathrm{Gal}(K_n/K)$$

$\gamma_n \in \Gamma_n$ δρα στο X_n εφόσον ανυψώσουμε σε $\tilde{\gamma}_n \in \mathrm{Gal}(L_n/K)$

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

Το X_n γίνεται $\mathbb{Z}_p[\Gamma_n]$-πρότυπο

Θεώρημα

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

$$1 + T \longleftrightarrow \gamma_0$$

Θεώρημα

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

$$1 + T \longleftrightarrow \gamma_0$$

Απόδειξη.

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

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

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

□

Δράση Συζυγίας

$$\Lambda \cong \varprojlim \mathbb{Z}_p[\Gamma_n]$$

δρα στο

$$X \cong \varprojlim X_n$$

«κατά συντεταγμένη», δηλαδή για $\gamma \in \Gamma$ και $x \in X$

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

όπου ανυψώνουμε σε $\tilde{\gamma} \in \mathrm{Gal}(L/K_m)$ για το m από πριν.

$$X \text{ είναι } \Lambda\text{-πρότυπο}$$

X_n ως πηλίκο του X

Θεωρούμε ότι $m = 0$.

Βάση Επαγωγής

$\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ οι πρώτοι που διακλαδίζονται στην επέκταση K_∞/K. Σταθεροποιούμε έναν πρώτο $\mathfrak{q}_i$ του L που στέκεται πάνω από το $\mathfrak{p}_i$.

$$I_i = I(\mathfrak{q}_i \mid \mathfrak{p}_i), \quad L/K_\infty \text{ αδιακλάδιστη}$$

$$I_i \cap X = 1$$

$$I_i \hookrightarrow G/X \cong \Gamma \text{ επιμορφισμός}$$

$$G = I_i X = X I_i$$

$$\gamma_0 \longleftrightarrow \sigma_i \in I_i, \quad \sigma_i = a_i \sigma_1, \quad a_i \in X$$

X_n ως πηλίκο του X

Λήμμα

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

Βάση Επαγωγής

Θέτουμε Y_0 να είναι το $\mathbb{Z}_p$-υποπρότυπο του X που παράγεται από τα TX και $\{a_i : \ 2 \leq i \leq s\}$.

$$\nu_n := 1 + \gamma_0 + \cdots + \gamma_0^{p^n - 1} = \frac{\gamma_0^{p^n} - 1}{\gamma_0 - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

$$Y_n = \nu_n \cdot Y_0$$

X_n ως πηλίκο του X

Λήμμα

Για $n \geq 0$ *έχουμε*

$$X_n \cong X/Y_n$$

X_n ως πηλίκο του X

Λήμμα

Για $n \geq 0$ *έχουμε*
$$X_n \cong X/Y_n$$

Απόδειξη.

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

αλλαγές: $\sigma_i \to \sigma_i^{p^n}$, $a_i \to \nu_n \cdot a_i$,

$$(\gamma_0 - 1)X \to (\gamma_0^{p^n} - 1)X = \nu_n(\gamma_0 - 1)X$$

X πεπερασμένα παραγόμενο Λ-πρότυπο

Λήμμα

Έστω M ένα συμπαγές Λ-πρότυπο. Αν το $M/(p, T)M$ είναι πεπερασμένα παραγόμενο, τότε το M είναι πεπερασμένα παραγόμενο Λ-πρότυπο.

X πεπερασμένα παραγόμενο Λ-πρότυπο

Λήμμα

Έστω M ένα συμπαγές Λ-πρότυπο. Αν το $M/(p, T)M$ είναι πεπερασμένα παραγόμενο, τότε το M είναι πεπερασμένα παραγόμενο Λ-πρότυπο.

Πόρισμα

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

X πεπερασμένα παραγόμενο Λ-πρότυπο

Λήμμα

Έστω M ένα συμπαγές Λ-πρότυπο. Αν το $M/(p,T)M$ είναι πεπερασμένα παραγόμενο, τότε το M είναι πεπερασμένα παραγόμενο Λ-πρότυπο.

Πόρισμα

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

Απόδειξη.

$$\nu_1 = ((1+T)^p - 1)/T \in (p,T)$$

$$Y_0/(p,T)Y_0 \text{ πηλίκο του } Y_0/\nu_1 \cdot Y_0 = Y_0/Y_1 \subset X/Y_1 = X_1$$

$$\implies Y_0 \text{ πεπερασμένα παραγόμενο }, \quad X/Y_0 = X_0$$

$$\implies X \text{ πεπερασμένα παραγόμενο}$$

□

X_n ως πηλίκο του X

Διόρθωση

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

Εφόσον $\mathrm{Gal}(K_\infty/K_m) \cong \Gamma^{p^m}$ παράγεται από γ^{p^n}.

Διόρθωση

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

Εφόσον $\mathrm{Gal}(K_\infty/K_m) \cong \Gamma^{p^m}$ παράγεται από γ^{p^n}.

Λήμμα

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

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

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

Θεώρημα Δομής

Δομή του X

$$X/Y_m \cong \frac{X_m}{Y_m/\nu_{n,m}Y_m} \text{ πεπερασμένο}$$

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

Υπολογίζουμε την τάξη του $M/\nu_{n,m}M$ για κάθε συνιστώσα M.

Θεώρημα Δομής

Δομή του X

$$X/Y_m \cong \frac{X_m}{Y_m/\nu_{n,m}Y_m} \text{ πεπερασμένο}$$

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

Υπολογίζουμε την τάξη του $M/\nu_{n,m}M$ για κάθε συνιστώσα M.

$$\begin{cases} M = \Lambda : & \Lambda/(\nu_{n,m}) \text{ άπειρο} \implies r = 0. \\ M = \Lambda/(p^k) : & \Lambda/(p^k, \nu_{n,m}) \implies (p^k)^{p^n - p^m} = p^{kp^n + c} \\ M = \Lambda/(f(T)^k) : & p^{dn+c},\ d = \deg f(T)^r, n > n_0 \end{cases}$$

Πρόταση

Υποθέτουμε ότι

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

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

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

για κάθε $n \geq n_0$.

Πρόβλημα

$$\text{Ξέρουμε την τάξη του } N/\nu_{n,m}N \quad \forall n \geq n_0$$

$$Y_m \sim N$$

$$\text{Θέλουμε την τάξη του } Y_m/\nu_{n,m}Y_m \quad \forall n \geq n_0$$

Πρόβλημα

$$\text{Ξέρουμε την τάξη του } N/\nu_{n,m}N \quad \forall n \geq n_0$$

$$Y_m \sim N$$

$$\text{Θέλουμε την τάξη του } Y_m/\nu_{n,m}Y_m \quad \forall n \geq n_0$$

Λήμμα

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

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

για κάθε $n \geq n_0$.

$$
\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \ker \phi_n' \arrow[d] & \ker \phi \arrow[d] & \ker \phi_n'' \arrow[d] & \\
0 \arrow[r] & \nu_{n,m}M \arrow[r] \arrow[d, "\phi_n'"] & M \arrow[r] \arrow[d, "\phi"] & M/\nu_{n,m}M \arrow[r] \arrow[d, "\phi_n''"] & 0 \\
0 \arrow[r] & \nu_{n,m}N \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N/\nu_{n,m}N \arrow[r] \arrow[d] & 0 \\
 & \operatorname{coker} \phi_n' \arrow[d] & \operatorname{coker} \phi \arrow[d] & \operatorname{coker} \phi_n'' \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

Θεώρημα (Iwasawa)

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

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

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

Απόδειξη.

$$\begin{aligned} p^{e_n} &= |X_n| \\ &= |X/Y_m| \cdot |Y_m/\nu_{n,m} Y_m| \\ &= p^b \cdot |N/\nu_{n,m} N| \\ &= p^{\lambda n + \mu p^n + \nu} \end{aligned}$$

για κάθε $n \geq n_0$. $\square$

p-αδικός χαρακτήρας Artin

Συνεχής ομομορφισμός ομάδων με πεπερασμένη εικόνα:

$$\chi : \mathrm{Gal}(F^{\mathrm{sep}}/F) \longrightarrow \overline{\mathbb{Q}}_p^\times$$

$$\chi : \mathrm{Gal}(F^{\chi}/F) \longrightarrow \langle \zeta_n \rangle \subseteq \overline{\mathbb{Q}}_p^\times$$

Τύπου S αν $F^{\chi} \cap F_\infty = F$.
Τύπου W αν $F^{\chi} \subset F_\infty$.

$$F_\infty^{\chi} = F_\infty F^{\chi} = \cup_n F_n^{\chi}$$

Αν χ τύπου S τότε έχουμε τους ισομορφισμούς:

$$\Gamma = \mathrm{Gal}(F_\infty^{\chi}/F^{\chi}) \longrightarrow \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p$$

$$\Delta = \mathrm{Gal}(F_\infty^{\chi}/F_\infty) \longrightarrow \mathrm{Gal}(F^{\chi}/F)$$

$$
\begin{tikzcd}[arrows=dash]
 & F_\infty^{\chi} \arrow[dl, "\Gamma"'] \arrow[dr, "\Delta"] & \\
F^{\chi} \arrow[dr] & & F_\infty \arrow[dl, "\mathbb{Z}_p"] \\
 & F &
\end{tikzcd}
$$

Όμοια με πριν

L_n μέγιστη αδιακλάδιστη αβελιανή p-επέκταση του F_n^{χ}.
$X_n = \mathrm{Gal}(L_n/F_n^{\chi})$ ισόμορφο με την p-Sylow υποομάδα της ομάδας κλάσεων του F_n^{χ}.

$$L = \cup L_n F_\infty^{\chi}$$

$$X \cong \varprojlim X_n$$

$$
\begin{tikzcd}
& & L & & \\
& L_n \arrow[ur, dash] & & F_\infty^\chi \arrow[ul, dash, "X"'] & \\
L_0 \arrow[ur, dash] & & F_n^\chi \arrow[ul, dash, "X_n"'] \arrow[ur, dash, "\Gamma^{p^n}"'] & & F_\infty \arrow[ul, dash, "\Delta"'] \\
& F^\chi \arrow[ul, dash, "X_0"] \arrow[ur, dash, "\Gamma/\Gamma^{p^n}"'] & & F_n \arrow[ul, dash] \arrow[ur, dash, "p^n\mathbb{Z}_p"'] & \\
& & F \arrow[ul, dash] \arrow[ur, dash, "\mathbb{Z}/p^n\mathbb{Z}"'] & &
\end{tikzcd}
$$

X ως $\mathbb{Z}_p[[\Gamma]]$-πρότυπο

$\Gamma \times \Delta$ δρα με συζυγίες στο X

X γίνεται $\mathbb{Z}_p[[\Gamma \times \Delta]]$ – πρότυπο

Θεώρημα Δομής

$$X \sim \left(\bigoplus_i \Lambda/(p^{\mu_i}) \right) \oplus \left(\bigoplus_j \Lambda/(f_j(T)^{m_j}) \right)$$

$$V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p \cong \bigoplus \overline{\mathbb{Q}}_p[T]/(f_j(T)^{m_j})$$

$$f_X(T) = \prod f_j(T)^{m_j}$$

χαρακτηριστικό πολυώνυμο της δράσης του $\gamma_0 - 1$ στο V.

$$V = \bigoplus_{\psi \in \Delta^\wedge} \varepsilon_\psi V \quad \text{ως } \overline{\mathbb{Q}}_p[\Delta]\text{-πρότυπο}$$

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

$f_\chi(T)$ χαρακτηριστικό πολυώνυμο της δράσης του $\gamma_0 - 1$ στο V^χ

P. Deligne & K. Ribet

Έστω ψ χαρακτήρας του F τέτοιος ώστε το F^{ψ} να είναι πλήρως πραγματικό. Τότε υπάρχει η αντίστοιχη p-αδική L-συνάρτηση $\mathcal{L}_p(s,\psi)$.

$$H_{\psi}(T) = \begin{cases} \psi(\gamma_0)(1+T)-1, & \psi \text{ είναι τύπου } W \text{ ή τετριμμένο}, \\ 1, & \text{διαφορετικά}. \end{cases}$$

Για $\mathcal{O}_{\psi} := \mathbb{Z}_p[\psi]$ υπάρχει $G_{\psi}(T) \in \mathcal{O}_{\psi}[[T]]$ έτσι ώστε

$$\mathcal{L}_p(1-s,\psi) = \frac{G_{\psi}((1+p)^s-1)}{H_{\psi}((1+p)^s-1)}$$

ρ χαρακτήρας τύπου W: $G_{\psi\rho}(T) = G_{\psi}(\rho(\gamma_0)(1+T)-1)$

χ περιττός, $\psi = \chi^{-1}\omega$

Θ. Προπαρασκευής: $G_{\psi}((1+p)(1+T)^{-1}-1) = \pi^{\mu_{\chi}} g_{\psi}(T) u_{\psi}(T)$

Θεώρημα (Κύρια Εικασία της Θεωρίας Iwasawa)

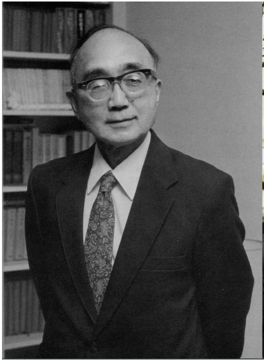
Για χ *περιττό χαρακτήρα τύπου* S *και* p *έναν περιττό πρώτο έχουμε*

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

Θεώρημα (Κύρια Εικασία της Θεωρίας Iwasawa)

Για χ περιττό χαρακτήρα τύπου S και p έναν περιττό πρώτο έχουμε

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




Σας ευχαριστώ πολύ!

Απόσπασμα από το Fermat's Last Theorem του Simon Singh

Iwasawa theory on its own had been inadequate. The Kolyvagin-Flach method on its own was also inadequate. Together they complemented each other perfectly. It was a moment of inspiration that Wiles will never forget. As he recounted these moments the memory was so powerful that he was moved to tears: "It was so indescribably beautiful; it was so simple and so elegant. I couldn't contain myself, I was so excited. It was the most important moment of my working life. Nothing I ever do again will mean as much."