



Greither unit undex

Giacomo Borin

19 aprile 2021

Introduzione

In questo lavoro ho rielaborato l'articolo:


Cornelius Greither. "Improving Ramachandra's and Levesque's unit index". English. In: *Number theory. Fifth conference of the Canadian Number Theory Association, Ottawa, Ontario, Canada, August 17–22, 1996*. Providence, RI: American Mathematical Society, 1999, pp. 111–120. ISBN: 0-8218-0964-4/pbk

Completando i prerequisiti richiesti per la comprensione e implementando alcuni calcoli in 





Introduzione

In questo lavoro ho rielaborato l'articolo:

Cornelius Greither. "Improving Ramachandra's and Levesque's unit index". English. In: *Number theory. Fifth conference of the Canadian Number Theory Association, Ottawa, Ontario, Canada, August 17–22, 1996*. Providence, RI: American Mathematical Society, 1999, pp. 111–120. ISBN: 0-8218-0964-4/pbk

Completando i prerequisiti richiesti per la comprensione e implementando alcuni calcoli in 

Bibliografia

-  Cornelius Greither. "Improving Ramachandra's and Levesque's unit index". English. In: *Number theory. Fifth conference of the Canadian Number Theory Association, Ottawa, Ontario, Canada, August 17–22, 1996*. Providence, RI: American Mathematical Society, 1999, pp. 111–120. ISBN: 0-8218-0964-4/pbk.
-  K. Ramachandra. "On the units of cyclotomic fields". English. In: *Acta Arith.* 12 (1966), pp. 165–173. ISSN: 0065-1036; 1730-6264/e.
-  Paulo Ribenboim. *Classical theory of algebraic numbers*. English. New York, NY: Springer, 2001, pp. xxiv + 681. ISBN: 0-387-95070-2/hbk.
-  W. Sinnott. *On the Stickelberger ideal and the circular units of an abelian field*. English. *Theorie des nombres, Semin.*



Prerequisiti

Il gruppo delle unità

Primo oggetto di interesse: E_K

Il gruppo delle unità di K , il sottocampo reale massimo di $\mathbb{Q}(\zeta_n)$

- ζ_n l' n -esima radice ciclotomica (con $n \not\equiv 2 \pmod{4}$)
- $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
- $O_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$
- $E_K = O_K^*$, cioè l'insieme degli elementi invertibili

Il gruppo delle unità

Primo oggetto di interesse: E_K

Il gruppo delle unità di K , il sottocampo reale massimo di $\mathbb{Q}(\zeta_n)$

- ζ_n l' n -esima radice ciclotomica (con $n \not\equiv 2 \pmod{4}$)
- $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
- $O_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$
- $E_K = O_K^*$, cioè l'insieme degli elementi invertibili

Il gruppo delle unità

Primo oggetto di interesse: E_K

Il gruppo delle unità di K , il sottocampo reale massimo di $\mathbb{Q}(\zeta_n)$

- ζ_n l' n -esima radice ciclotomica (con $n \not\equiv 2 \pmod{4}$)
- $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
- $O_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$
- $E_K = O_K^*$, cioè l'insieme degli elementi invertibili

↗ Salta dimostrazione

Il gruppo delle unità

Primo oggetto di interesse: E_K

Il gruppo delle unità di K , il sottocampo reale massimo di $\mathbb{Q}(\zeta_n)$

- ζ_n l' n -esima radice ciclotomica (con $n \not\equiv 2 \pmod{4}$)
- $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
- $O_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$
- $E_K = O_K^*$, cioè l'insieme degli elementi invertibili

↗ Salta dimostrazione

Il gruppo delle unità

Primo oggetto di interesse: E_K

Il gruppo delle unità di K , il sottocampo reale massimo di $\mathbb{Q}(\zeta_n)$

- ζ_n l' n -esima radice ciclotomica (con $n \not\equiv 2 \pmod{4}$)
- $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$
- $O_K = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$
- $E_K = O_K^*$, cioè l'insieme degli elementi invertibili

► Salta dimostrazione

Dimostrazione.

- $\zeta_n + \zeta_n^{-1}$ è **reale**:

$$\overline{\zeta_n + \zeta_n^{-1}} = \overline{\zeta_n} + \overline{\zeta_n^{-1}} = \zeta_n^{-1} + \zeta_n$$

- L'indice $[\mathbb{Q}(\zeta_n) : K]$ vale 2, ed è quindi minimale. Il suo polinomio minimo è:

$$f(x) = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$$

Dimostrazione.

- $\zeta_n + \zeta_n^{-1}$ è **reale**:

$$\overline{\zeta_n + \zeta_n^{-1}} = \overline{\zeta_n} + \overline{\zeta_n^{-1}} = \zeta_n^{-1} + \zeta_n$$

- L'indice $[\mathbb{Q}(\zeta_n) : K]$ vale **2**, ed è quindi minimale. Il suo polinomio minimo è:

$$f(x) = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$$

Dimostrazione.

- $\zeta_n + \zeta_n^{-1}$ è **reale**:

$$\overline{\zeta_n + \zeta_n^{-1}} = \overline{\zeta_n} + \overline{\zeta_n^{-1}} = \zeta_n^{-1} + \zeta_n$$

- L'indice $[\mathbb{Q}(\zeta_n) : K]$ vale **2**, ed è quindi minimale. Il suo polinomio minimo è:

$$f(x) = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$$

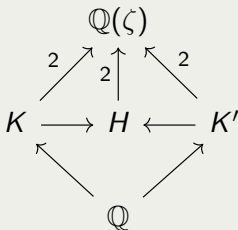
Dimostrazione.

- Un sottocampo con queste caratteristiche è **unico**:



Dimostrazione.

- Un sottocampo con queste caratteristiche è **unico**:





Proposizione

Il gruppo di Galois di K è isomorfo a $\mathbb{Z}_n^/\{\pm 1\}$*

D'ora in poi indicheremo $G_0 := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $G := \text{Gal}(K/\mathbb{Q})$

Proposizione

Il gruppo di Galois di K è isomorfo a $\mathbb{Z}_n^/\{\pm 1\}$*

D'ora in poi indicheremo $G_0 := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ e $G := \text{Gal}(K/\mathbb{Q})$

Il numero delle classi

Definizione

Se \mathbb{K} è un campo numerico possiamo definire l'**ideal class group** come il quoziente $\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ dove:

$\mathcal{F}_{\mathbb{K}}$ è il gruppo degli ideali frazionari non nulli di $O_{\mathbb{K}}$,

$\mathcal{P}_{\mathbb{K}}$ è il gruppo degli ideali principali

Si può mostrare che questo gruppo è finito e definiamo il **numero delle classi** come:

$$h_K = |\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}|$$

Il numero delle classi

Definizione

Se \mathbb{K} è un campo numerico possiamo definire l'**ideal class group** come il quoziente $\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ dove:

$\mathcal{F}_{\mathbb{K}}$ è il gruppo degli ideali frazionari non nulli di $O_{\mathbb{K}}$,

$\mathcal{P}_{\mathbb{K}}$ è il gruppo degli ideali principali

Si può mostrare che questo gruppo è finito e definiamo il **numero delle classi** come:

$$h_K = |\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}|$$

Unità circolari

Se considero il gruppo generato da $\{-1, \zeta, 1 - \zeta^a \text{ for } a = 1, \dots, n-1\}$ e lo interseco con E_K ottengo il gruppo delle **unità circolari**

Sinnot ha mostrato che esiste $a \in \mathbb{Z}$ tale che:

$$[E_K : C_K] = 2^a k_K$$

Unità circolari

Se considero il gruppo generato da $\{-1, \zeta, 1 - \zeta^a \text{ for } a = 1, \dots, n - 1\}$ e lo interseco con E_K ottengo il gruppo delle **unità circolari**

Sinnot ha mostrato che esiste $a \in \mathbb{Z}$ tale che:

$$[E_K : C_K] = 2^a k_K$$



Obbiettivo dell'articolo

Costruire **esplicitamente** un gruppo C' con indice $[E_K : C']$ finito che sia **ottimale**

Caratteri di Dirichlet

Definizione

Dato un gruppo X e un campo \mathbb{F} un carattere di Dirichlet è un omomorfismo di gruppi $\chi : X \rightarrow \mathbb{F}^*$

Possiamo anche usare l'isomorfismo $G_0 \simeq \mathbb{Z}_n^*$ e definire χ come omomorfismo di anelli da \mathbb{Z}_n in \mathbb{C} (con χ nulla sugli elementi invertibili)

Il 'periodo' di un caratte è detto conduttore (in inglese **conductor**) e si indica con f_χ

Caratteri di Dirichlet

Definizione

Dato un gruppo X e un campo \mathbb{F} un carattere di Dirichlet è un omomorfismo di gruppi $\chi : X \rightarrow \mathbb{F}^*$

Possiamo anche usare l'isomorfismo $G_0 \simeq \mathbb{Z}_n^*$ e definire χ come omomorfismo di anelli da \mathbb{Z}_n in \mathbb{C} (con χ nulla sugli elementi invertibili)

Il 'periodo' di un caratte è detto conduttore (in inglese **conductor**) e si indica con f_χ

Caratteri di Dirichlet

Definizione

Dato un gruppo X e un campo \mathbb{F} un carattere di Dirichlet è un omomorfismo di gruppi $\chi : X \rightarrow \mathbb{F}^*$

Possiamo anche usare l'isomorfismo $G_0 \simeq \mathbb{Z}_n^*$ e definire χ come omomorfismo di anelli da \mathbb{Z}_n in \mathbb{C} (con χ nulla sugli elementi invertibili)

Il 'periodo' di un caratte è detto conduttore (in inglese **conductor**) e si indica con f_χ



Anelli gruppali

Definizione

Dati un gruppo moltiplicativo X e un anello R possiamo definire l'**anello grupale** $R[X]$ come l' R -modulo libero con base X , sul quale definiamo un'operazione di moltiplicazione inducendola da quella di X

Nel nostro caso useremo $\mathbb{Z}[G_0]$ e $\mathbb{Z}[G]$, sui quali possiamo sempre estendere il carattere χ (perchè definito sulla base)

Anelli gruppali

Definizione

Dati un gruppo moltiplicativo X e un anello R possiamo definire l'**anello grupale** $R[X]$ come l' R -modulo libero con base X , sul quale definiamo un'operazione di moltiplicazione inducendola da quella di X

Nel nostro caso useremo $\mathbb{Z}[G_0]$ e $\mathbb{Z}[G]$, sui quali possiamo sempre estendere il carattere χ (perchè definito sulla base)

Anelli gruppali

Notazione

Dati $z \in \mathbb{Q}(\zeta)$ e $f \in \mathbb{Z}[G_0]$ è ben definita la nutazione esponenziale x^f , infatti dati $g \in G_0$ abbiamo una buona definizione per $z^g = g(z)$ e $z^{g_1+g_2} = z^{g_1} z^{g_2}$

Anelli gruppali

Notazione

Dati $z \in \mathbb{Q}(\zeta)$ e $f \in \mathbb{Z}[G_0]$ è ben definita la nutazione esponenziale x^f , infatti dati $g \in G_0$ abbiamo una buona definizione per $z^g = g(z)$ e $z^{g_1+g_2} = z^{g_1} z^{g_2}$



La costruzione di Greither

La funzione β

Dato $n = p_1^{e_1} \cdots p_s^{e_s}$ definiamo:

- $S = \{1, \dots, n\}$
- $\mathcal{P}_S = \{I \mid I \subsetneq S\}$
- $n_I = \prod_{i \in I} p_i^{e_i}$

Consideriamo una funzione

$$\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G_0]$$

che utilizzeremo per costruire il sottogruppo cercato.

Definizione

β si dice moltiplicativa se $\beta(\emptyset) = 1$ e dati I, J con intersezione vuota abbiamo $\beta(I \cup J) = \beta(I)\beta(J)$.

La funzione β

Dato $n = p_1^{e_1} \cdots p_s^{e_s}$ definiamo:

- $S = \{1, \dots, n\}$
- $\mathcal{P}_S = \{I \mid I \subsetneq S\}$
- $n_I = \prod_{i \in I} p_i^{e_i}$

Consideriamo una funzione

$$\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G_0]$$

che utilizzeremo per costruire il sottogruppo cercato.

Definizione

β si dice moltiplicativa se $\beta(\emptyset) = 1$ e dati I, J con intersezione vuota abbiamo $\beta(I \cup J) = \beta(I)\beta(J)$.

La funzione β

Dato $n = p_1^{e_1} \cdots p_s^{e_s}$ definiamo:

- $S = \{1, \dots, n\}$
- $\mathcal{P}_S = \{I \mid I \subsetneq S\}$
- $n_I = \prod_{i \in I} p_i^{e_i}$

Consideriamo una funzione

$$\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G_0]$$

che utilizzeremo per costruire il sottogruppo cercato.

Definizione

β si dice moltiplicativa se $\beta(\emptyset) = 1$ e dati I, J con intersezione vuota abbiamo $\beta(I \cup J) = \beta(I)\beta(J)$.

Le unità di Greither

Definiamo ora, per ogni $a \in (1, n/2)$ coprimo con n l'unità reale:

$$\xi_a(\beta) := \zeta^{d_a(\beta)} \frac{\sigma_a(z(\beta))}{z(\beta)} \text{ con } d_a(\beta) = (1 - a)\frac{t}{2}$$

dove abbiamo che

- $z_I := 1 - \zeta^{n_I}$
- $z(\beta) := \prod_{i \in I} z_I^{\beta(i)}$
- $\sigma_a(\zeta) = \zeta^a$

Il gruppo di Greither

C_β è il gruppo generato da:

$$-1 \text{ e } \xi_a(\beta) \text{ per } 1 < a < n/2 \text{ e } (a, n) = 1$$

Per l'indice useremo la notazione

$$[E_K : C_\beta] = h_K i_\beta$$

Il gruppo di Greither

C_β è il gruppo generato da:

$$-1 \text{ e } \xi_a(\beta) \text{ per } 1 < a < n/2 \text{ e } (a, n) = 1$$

Per l'indice useremo la notazione

$$[E_K : C_\beta] = h_K i_\beta$$



Buona definizione di C_β

Possiamo limitarci a definire β su $\mathbb{Z}[G]$ e poi considerare un sollevamento (in inglese lift)

Lemma

Se due funzioni β_1 e β_2 coincidono su $\mathbb{Q}(\zeta_{n/n_l})^a$ per ogni $l \in \mathcal{P}_S$ allora le unità $\xi_a(\beta)$ sono uniche a meno del segno

$$^a\zeta_{n/n_l} = \zeta_n^{n_l}$$

Buona definizione di C_β

Possiamo limitarci a definire β su $\mathbb{Z}[G]$ e poi considerare un sollevamento (in inglese lift)

Lemma

Se due funzioni β_1 e β_2 coincidono su $\mathbb{Q}(\zeta_{n/n_l})^a$ per ogni $l \in \mathcal{P}_S$ allora le unità $\xi_a(\beta)$ sono uniche a meno del segno

$$^a\zeta_{n/n_l} = \zeta_n^{n_l}$$

Precisazione sul sollevamento

Dati due insiemi Z , Y e una funzione $\phi : Y \rightarrow Z$ diciamo che $f' : X \rightarrow Y$ è un **sollevamento** di $f : X \rightarrow Z$ se commuta:

$$\begin{array}{ccc} & & Y \\ & \nearrow f' & \downarrow \phi \\ X & \xrightarrow{f} & Z \end{array}$$

Nel nostro caso ϕ è il morfismo indotto dalla proiezione

$$G_0 \simeq \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* / \pm 1 \simeq G$$

Precisazione sul sollevamento

Dati due insiemi Z , Y e una funzione $\phi : Y \rightarrow Z$ diciamo che $f' : X \rightarrow Y$ è un **sollevamento** di $f : X \rightarrow Z$ se commuta:

$$\begin{array}{ccc} & & Y \\ & \nearrow f' & \downarrow \phi \\ X & \xrightarrow{f} & Z \end{array}$$

Nel nostro caso ϕ è il morfismo indotto dalla proiezione

$$G_0 \simeq \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* / \pm 1 \simeq G$$



Calcolo degli indici

Caso generale

Teorema

Data una funzione $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ segue che

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{pari}}} \left(\sum_{\substack{I \in \mathcal{P}_S \\ (f_\chi, n_I) = 1}} \phi(n_I) \cdot \chi(\beta(I)) \cdot \prod_{i \notin I} (1 - \chi^{-1}(p_i)) \right) \quad (1)$$

Dove abbiamo che:

- ϕ è la funzione di Eulero
- χ si dice *pari* se $\chi(-1) = 1$
- Con χ^{-1} si intende il carattere che vale $1/\chi$ sugli elementi invertibili

Caso generale

Teorema

Data una funzione $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ segue che

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{pari}}} \left(\sum_{\substack{I \in \mathcal{P}_S \\ (f_\chi, n_I) = 1}} \phi(n_I) \cdot \chi(\beta(I)) \cdot \prod_{i \notin I} (1 - \chi^{-1}(p_i)) \right) \quad (1)$$

Dove abbiamo che:

- ϕ è la funzione di Eulero
- χ si dice *pari* se $\chi(-1) = 1$
- Con χ^{-1} si intende il carattere che vale $1/\chi$ sugli elementi invertibili

Caso generale

Dato un campo numerico L consideriamo un insieme di unità indipendenti $\{\epsilon_1, \dots, \epsilon_r\} \subset L$ e siano $\{\sigma_1, \dots, \sigma_{r+1}\}$ le sue immersioni (embedding) in \mathbb{R} o \mathbb{C} . Poniamo δ_j uguale a 1 se σ_j è reale e a 2 altrimenti. Allora il suo **regolatore** è definito come

$$R_L(\epsilon_1, \dots, \epsilon_r) = |\det(\delta_i \log |\epsilon_j^{\sigma_i}|)_{1 \leq i, j \leq r}|$$

Lemma

Dati i gruppi $A \subset B$ di indice finito e generati da unità indipendenti di L vale che:

$$[B : A] = \frac{R_L(\epsilon_1, \dots, \epsilon_r)}{R_L(\mu_1, \dots, \mu_r)} \quad (2)$$

Caso generale

Dato un campo numerico L consideriamo un insieme di unità indipendenti $\{\epsilon_1, \dots, \epsilon_r\} \subset L$ e siano $\{\sigma_1, \dots, \sigma_{r+1}\}$ le sue immersioni (embedding) in \mathbb{R} o \mathbb{C} . Poniamo δ_j uguale a 1 se σ_j è reale e a 2 altrimenti. Allora il suo **regolatore** è definito come

$$R_L(\epsilon_1, \dots, \epsilon_r) = |\det(\delta_j \log |\epsilon_j^{\sigma_i}|)_{1 \leq i, j \leq r}|$$

Lemma

Dati i gruppi $A \subset B$ di indice finito e generati da unità indipendenti di L vale che:

$$[B : A] = \frac{R_L(\epsilon_1, \dots, \epsilon_r)}{R_L(\mu_1, \dots, \mu_r)} \quad (2)$$

Usando l'ultimo lemma possiamo vedere che per dimostrare il teorema basta mostrare che

$$R(\xi_a(\beta)) = \pm R_K h_K A$$

con $(a, n) = 1$, $1 < a < n/2$ e A è la parte destra dell'equazione 1. Inoltre poi si procede (in modo molto tecnico) come nel capitolo 8 di [5] e usando:

Formula

$$\sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a \gamma}| = \chi(\gamma) \sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a}| \quad (3)$$

Usando l'ultimo lemma possiamo vedere che per dimostrare il teorema basta mostrare che

$$R(\xi_a(\beta)) = \pm R_K h_K A$$

con $(a, n) = 1$, $1 < a < n/2$ e A è la parte destra dell'equazione 1. Inoltre poi si procede (in modo molto tecnico) come nel capitolo 8 di [5] e usando:

Formula

$$\sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a \gamma}| = \chi(\gamma) \sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a}| \quad (3)$$

Indice per β moltiplicativa

Teorema

Se assumiamo che $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ sia moltiplicativa abbiamo che:

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{pari}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) \cdot \chi(\beta(i)) + 1 - \chi^{-1}(p_i)) \right) \quad (4)$$

Dove $\beta(i)$ indica $\beta(\{i\})$

L'indice di Ramachandra

Se poniamo β costante ad 1 otteniamo l'indice delle unità per Ramachandra da [2]:

$$[E_K : C_R] = h_K \cdot \prod_{\substack{\chi \neq 1 \\ \text{even}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \right) \quad (5)$$

Dove C_R è il gruppo generato da -1 e le unità della forma

$$\xi_a := \zeta^{d_a} \prod_{I \in \mathcal{P}_S} \frac{1 - \zeta^{an_I}}{1 - \zeta^{n_I}} \quad \text{con} \quad d_a = \frac{1}{2}(1 - a) \sum_{I \in \mathcal{P}_S} n_I$$

Definizione di β

Costruiamo β moltiplicativa, quindi definendo $\beta(i)$ per ogni $i \in \{1, \dots, s\}$:

Definiamo G_i come il gruppo di Galois: $\text{Gal}(\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+/\mathbb{Q})$ e consideriamo l'isomorfismo di Frobenius:

$$F_i : G_i \rightarrow G_i \text{ con } \alpha \mapsto \alpha^{p_i}$$

Definiamo il suo elemento traccia N_{F_i} come:

$$N_{F_i} := 1 + F_i + \dots + F_i^{\text{ord}(F_i)-1} \in \mathbb{Z}[G_i]$$

Definizione di β

Costruiamo β moltiplicativa, quindi definendo $\beta(i)$ per ogni $i \in \{1, \dots, s\}$:

Definiamo G_i come il gruppo di Galois: $\text{Gal}(\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+/\mathbb{Q})$ e consideriamo l'isomorfismo di Frobenius:

$$F_i : G_i \rightarrow G_i \text{ con } \alpha \mapsto \alpha^{p_i}$$

Definiamo il suo elemento traccia N_{F_i} come:

$$N_{F_i} := 1 + F_i + \dots + F_i^{\text{ord}(F_i)-1} \in \mathbb{Z}[G_i]$$

Definizione di β

Costruiamo β moltiplicativa, quindi definendo $\beta(i)$ per ogni $i \in \{1, \dots, s\}$:

Definiamo G_i come il gruppo di Galois: $\text{Gal}(\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+/\mathbb{Q})$ e consideriamo l'isomorfismo di Frobenius:

$$F_i : G_i \rightarrow G_i \text{ con } \alpha \mapsto \alpha^{p_i}$$

Definiamo il suo elemento traccia N_{F_i} come:

$$N_{F_i} := 1 + F_i + \dots + F_i^{\text{ord}(F_i)-1} \in \mathbb{Z}[G_i]$$

Definizione di β

Consideriamo ora un sollevamento (lift) \overline{N}_i di N_{F_i} in $\mathbb{Z}[G_0]$ e definiamo

$$\beta(i) = \overline{N}_i$$

Ovviamente β non è unica, ma per il lemma visto prima lo sono le unità a meno di un segno, quindi lo è C_β

Definizione di β

Consideriamo ora un sollevamento (lift) $\overline{N_i}$ di N_{F_i} in $\mathbb{Z}[G_0]$ e definiamo

$$\beta(i) = \overline{N_i}$$

Ovviamente β non è unica, ma per il lemma visto prima lo sono le unità a meno di un segno, quindi lo è C_β

Decomposizione in O_K

Dato un primo p in \mathbb{Z} e la sua estensione come ideale pO_K in O_K , dato che questo è un dominio di Dedekind possiamo fattorizzare:

$$pO_K = \prod_{j=1}^g \mathfrak{p}_j^{\epsilon_j} \quad (6)$$

Definizione

Il numero g si dice essere **grado di decomposizione** di p nell'estensione K/\mathbb{Q} .

Per ogni $j = 1, \dots, g$, ϵ_j si dice essere **indice di ramificazione** di \mathfrak{p}_j in K/\mathbb{Q} .

Per ogni $j = 1, \dots, g$, $f_j := [O_K/\mathfrak{p}_j : \mathbb{Z}_p]$ si dice **grado di inerzia**.

Decomposizione in O_K

Dato un primo p in \mathbb{Z} e la sua estensione come ideale pO_K in O_K , dato che questo è un dominio di Dedekind possiamo fattorizzare:

$$pO_K = \prod_{j=1}^g \mathfrak{p}_j^{\epsilon_j} \quad (6)$$

Definizione

Il numero g si dice essere **grado di decomposizione** di p nell'estensione K/\mathbb{Q} .

Per ogni $j = 1, \dots, g$, ϵ_j si dice essere **indice di ramificazione** di \mathfrak{p}_j in K/\mathbb{Q} .

Per ogni $j = 1, \dots, g$, $f_j := [O_K/\mathfrak{p}_j : \mathbb{Z}_p]$ si dice **grado di inerzia**.

Decomposizione in $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$

Si può provare che se \mathbb{K}/\mathbb{Q} è un'estensione di Galois (come K/\mathbb{Q}) e_j, f_j non dipendono da j e quindi

$$n = efg$$

Per $i \in 1, \dots, s$ definiamo g_i, f_i, e_i essere i gradi definiti prima per il primo p_i in K/\mathbb{Q} .

Queste costanti sono fortemente in relazione con altri oggetti visti finora, ad esempio si può provare:

- Se X è l'insieme dei caratteri di K/\mathbb{Q} vale $g_i = |\{\chi \in X \mid \chi(p_i) = 1\}|$
- Il grado di inerzia f_i è uguale all'ordine del morphismo di Frobenius F_i

Decomposizione in $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$

Si può provare che se \mathbb{K}/\mathbb{Q} è un'estensione di Galois (come K/\mathbb{Q}) ϵ_j, f_j non dipendono da j e quindi

$$n = efg$$

Per $i \in 1, \dots, s$ definiamo g_i, f_i, ϵ_i essere i gradi definiti prima per il primo p_i in K/\mathbb{Q} .

Queste costanti sono fortemente in relazione con altri oggetti visti finora, ad esempio si può provare:

- Se X è l'insieme dei caratteri di K/\mathbb{Q} vale $g_i = |\{\chi \in X \mid \chi(p_i) = 1\}|$
- Il grado di inerzia f_i è uguale all'ordine del morphismo di Frobenius F_i

Decomposizione in $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$

Si può provare che se \mathbb{K}/\mathbb{Q} è un'estensione di Galois (come K/\mathbb{Q}) ϵ_j, f_j non dipendono da j e quindi

$$n = efg$$

Per $i \in 1, \dots, s$ definiamo g_i, f_i, ϵ_i essere i gradi definiti prima per il primo p_i in K/\mathbb{Q} .

Queste costanti sono fortemente in relazione con altri oggetti visti finora, ad esempio si può provare:

- Se X è l'insieme dei caratteri di K/\mathbb{Q} vale $g_i = |\{\chi \in X \mid \chi(p_i) = 1\}|$
- Il grado di inerzia f_i è uguale all'ordine del morphismo di Frobenius F_i

Risultato finale

Teorema

Dato C_β definito come prima abbiamo che

$$i_\beta = \prod_{i=1}^s \epsilon_i^{g_i-1} f_i^{2g_i-1}$$

Questo indice si può dire ottimale perchè non solo rende più semplice la sua fattorizzazione (basta sapere quella di ϵ_i e f_i), ma inoltre sappiamo che questi dividono n , quindi i fattori di i_β sono solo i fattori di n .

Risultato finale

Teorema

Dato C_β definito come prima abbiamo che

$$i_\beta = \prod_{i=1}^s \epsilon_i^{g_i-1} f_i^{2g_i-1}$$

Questo indice si può dire ottimale perchè non solo rende più semplice la sua fattorizzazione (basta sapere quella di ϵ_i e f_i), ma inoltre sappiamo che questi dividono n , quindi i fattori di i_β sono solo i fattori di n .