Greither unit undex

Giacomo Borin

Università di Trento

15 aprile 2021

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 sage

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 sage

Section 1

Prereqisiti

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

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**:

$$
\begin{tikzcd}
 & \mathbb{Q}(\zeta) & \\
K \arrow[r] \arrow[ur, "2"] & H \arrow[u, "2"] & K' \arrow[l] \arrow[ul, "2"'] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}
$$

□

Dimostrazione.

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

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta) & \\
K \arrow[ur, "2"] \arrow[r] & H \arrow[u, "2"] & K' \arrow[ul, "2"'] \arrow[l] \\
 & \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

$\square$

Proposizione

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

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

Proposizione

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

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

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 $\{-1, \zeta, 1-\zeta^a \text{ for } a = 1, ..., n-1\}$ 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 $\{-1, \zeta, 1 - \zeta^a \text{ for } a = 1, ..., n-1\}$ 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 Dirchlet è un omomorfismo di gruppi $\chi : X \to \mathbb{F}^*$

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 Dirchlet è un omomorfismo di gruppi $\chi : X \to \mathbb{F}^*$

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 Dirchlet è un omomorfismo di gruppi $\chi : X \to \mathbb{F}^*$

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 gruppale** $R[X]$ 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 esterndere il carattere χ (perchè definito sulla base)

Anelli gruppali

Definizione

Dati un gruppo moltiplicativo X e un anello R possiamo definire l'**anello gruppale** $R[X]$ 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 esterndere 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 $z^{g_1+g_2} = z^{g_1} z^{g_2}$

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 $z^{g_1+g_2} = z^{g_1} z^{g_2}$

Section 2

La costruzione di Greither

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

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

Consideriamo una funzione

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

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:

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

Consideriamo una funzione

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

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:

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

Consideriamo una funzione

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

che utilizzeremo per costruire il sottogruppo cercato.

Definizione

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

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

Caso generale

Teorema

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

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

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 $\beta : \mathcal{P}_S \to \mathbb{Z}[G]$ segue che

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

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