



UNIVERSITÀ
DI TRENTO

L'indice delle unità di Greither

Giacomo Borin

giacomoborin.github.io

Dipartimento di Matematica

10 giugno 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 



-  K. Ramachandra. “On the units of cyclotomic fields”. English. In: *Acta Arith.* 12 (1966), pp. 165–173. ISSN: 0065-1036; 1730-6264/e.
-  W. Sinnott. *On the Stickelberger ideal and the circular units of an abelian field*. English. *Theorie des nombres, Semin. Delange-Pisot-Poitou, Paris 1979-80, Prog. Math.* 12, 277-286 (1981). 1981.
-  Lawrence C. Washington. *Introduction to cyclotomic fields*. English. Vol. 83. Springer, New York, NY, 1982.



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**:

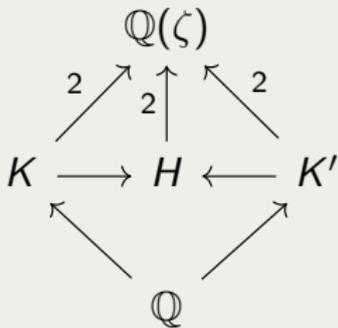
$$\overline{\zeta_n + \zeta_n^{-1}} = \overline{\zeta_n} + \overline{\zeta_n^{-1}} = \zeta_n^{-1} + \zeta_n$$

- 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.

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





Proposizione

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

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



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 $\mathcal{O}_{\mathbb{K}}$,

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

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

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



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:

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



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



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



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)



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



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 $\beta(I \cup J) = \beta(I)\beta(J)$.



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

- $z_l := 1 - \zeta^{nl}$
- $z(\beta) := \prod_{l \in I} z_l^{\beta(l)}$
- $\sigma_a(\zeta) = \zeta^a$



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

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



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

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



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

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

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



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:

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

Lemma (Lemma 5.26 in [4])

Sia X un gruppo abeliano finito e f una funzione su X a valori in \mathbb{C}

$$\det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau \neq 1} = \prod_{\substack{\chi \in \hat{X} \\ \chi \neq 1}} \sum_{\sigma \in X} \chi(\sigma) f(\sigma) \quad (3)$$

Dove \hat{X} è l'insieme dei caratteri da X in \mathbb{C}^*

Nel X sarà $G \simeq \mathbb{Z}_n / \pm 1$.

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 [4] e usando:

Formula

$$\sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a \gamma}| = \chi(\gamma) \sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a}| \quad (4)$$



Teorema

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

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{pari}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) \cdot \chi(\beta(i)) + 1 - \chi^{-1}(p_i)) \right) \quad (5)$$

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



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

$$[E_K : C_R] = h_K \cdot \prod_{\substack{\chi \neq 1 \\ \text{even}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \right) \quad (6)$$

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

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



Un nuovo sistema di unità



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:

$$F_i : \mathbb{Q}(\zeta_{n/p_i^{e_i}})^+ \rightarrow \mathbb{Q}(\zeta_{n/p_i^{e_i}})^+ \text{ con } \alpha \mapsto \alpha^{p_i}$$

Definiamo il suo elemento traccia N_{F_i} come:

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



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



Dato un primo p in \mathbb{Z} e la sua estensione come ideale $p\mathcal{O}_{\mathbb{K}}$ in $\mathcal{O}_{\mathbb{K}}$, dato che questo è un dominio di Dedekind possiamo fattorizzare:

$$p\mathcal{O}_{\mathbb{K}} = \prod_{j=1}^g \mathfrak{p}_j^{\epsilon_j} \quad (7)$$

Definizione

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

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

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



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 morfismo di Frobenius F_i

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 $\phi(n)/2$, quindi i fattori di i_β sono solo i fattori di $\phi(n)/2$.



Vediamo ora l'implementazione di alcuni calcoli in 

I principali calcoli usati sono stati:

- Creazione del campo ciclotomico e della radice ζ

```
1 sage: Qn.<z> = CyclotomicField(n)
```

- Creazione del massimo sottocampo reale K :

```
1 sage: zz = z + z.conjugate()
```

```
2 sage: K = NumberField(zz.minpoly(), 'a')
```



- Creazione dell'ideale pO_K e sua fattorizzazione:

```
1 sage: I = K.ideal(p(i))
```

```
2 sage: I.factor()
```

- Creazione dell'omomorfismo $\zeta \mapsto \zeta^f$:

```
1 sage: Qn.hom([z**f])
```

Comunque ora vedremo direttamente l'implementazione in

 dei calcoli, presentata tramite 



1 Prerequisiti

- Gruppo delle unità
- Numero delle classi
- Caratteri di Dirichlet e anelli grupपाल

2 La costruzione di Greither

- Oggetti indotti da β

3 Calcolo degli indici

- Primo teorema
- Teorema nel caso β moltiplicativa

4 Un nuovo sistema di unità



- Gradi di decomposizione

- 5** Implementazione dei calcoli