

The Greither unit index,
an undergraduate overview and
a *sagemath* implementation

Giacomo Borin

May 27, 2021

Abstract

Stuff Stuff Stuff

Contents

1	Introduction to the working set	2
1.1	The circular units and the class number	3
1.2	Dirichlet Characters	4
2	The Greither Setup	5
2.1	A little remark	6
3	Index calculation	7
3.1	Particular case of formula 5	9
3.2	A new system of units	10
3.3	A factorization for i_β	10

1 Introduction to the working set

Consider the n -th cyclotomic field $\mathbb{Q}(\zeta_n)$ with ζ_n a n -th primitive root of unity, with $n \not\equiv 2 \pmod{4}$, and define K as the maximal real subfield of $\mathbb{Q}(\zeta)$, also another notation that we will use for the maximal real subfield is $\mathbb{Q}(\zeta_n)^+$. From now we will refer to ζ_n without the index if not necessary.

Proposition 1.1. *The maximal real subfield is $K = \mathbb{Q}(\zeta + \zeta^{-1})$*

Proof. First of all we can easily see that K is real, infact since for the root of unity $\bar{\zeta} = \zeta^{-1}$ (complex conjugation) and so:

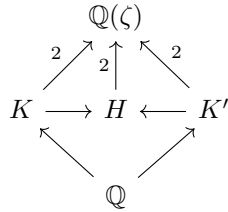
$$\overline{\zeta + \zeta^{-1}} = \bar{\zeta} + \bar{\zeta}^{-1} = \zeta^{-1} + \zeta$$

So $\zeta + \zeta^{-1}$ is real and K too.

Since $\mathbb{Q}(\zeta)$ is not real we have that the index $e := [\mathbb{Q}(\zeta) : K] \geq 2$ (strictly greater than 1).

Consider now the polynomial of degree 2 in $K[x] : f = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$, since ζ is a root obviously $e \leq 2$, so the subfield K has maximal degree since this is the minimal degree for a proper subfield.

If there was another $K' = \mathbb{Q}(\chi)$ with such property we can consider $H = \mathbb{Q}(\zeta, \chi)$ that is also real with $\mathbb{Q}(\zeta) \supsetneq H \supset K$, so $H = K$ and akin $H = K'$ so $K = K'$ and K is unique. \square



Now we will consider the **group of units** E_K that is the group formed by the invertible elements of its ring of integers O_K^* . Is it possible to characterize the ring of integers for K [6, Proposition 2.16] similiarly to what happens for $O_{\mathbb{Q}(\zeta)}$ (infact the proof follows without difficulty from this)

Proposition 1.2. $O_K = \mathbb{Z}[\zeta + \zeta^{-1}]$

Since $x^n - 1$ is separable $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension and it's easy to see that its Galois group G_0 is isomorphic to $(\mathbb{Z}_n)^*$. Also we can see that:

Proposition 1.3. K/\mathbb{Q} is a Galois extension and its Galois group G is isomorphic to $\mathbb{Z}_n^*/\{\pm 1\}$

Proof. Consider the map $\sigma : G_0 \rightarrow G$ that maps α_i to $\alpha_{i|_K}$ where α_i is the automorphism that maps ζ to ζ^i . Obviously σ is a morphism of groups. Also

it is easy to describe its kernel:

$$\begin{aligned}\ker(\sigma) &= \{\alpha_i \in G_0 \mid x = \alpha_i(x) \text{ for all } x \in K\} \\ &\stackrel{(1)}{=} \{\alpha_i \in G_0 \mid \zeta + \zeta^{-1} = \alpha_i(\zeta + \zeta^{-1}) = \zeta^i + \zeta^{-i}\} \\ &\stackrel{(2)}{=} \{\alpha_1, \alpha_{-1}\}\end{aligned}$$

Where (1) follows from the fact that $K = \mathbb{Q}(\zeta + \zeta^{-1})$ and (2) from linear algebra. So from the first theorem of isomorphism $\sigma(G_0) \simeq \mathbb{Z}_n^*/\{\pm 1\}$ and then

$$\phi(n)/2 = |\mathbb{Z}_n^*/\{\pm 1\}| \leq |G| \leq [K : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}]/2 = \phi(n)/2$$

So $\sigma(G_0) = G$ and $|G| = [K : \mathbb{Q}]$ and the thesis follows. \square

Remark 1. We excluded the case of $n \equiv 2 \pmod{4}$ because it is a repetition, infact in this situation $G_0 \simeq \mathbb{Z}_{2+4k}^*$ and since $2+4k = 2(1+2k)$ with the second term odd for the Chinese reminder theorem $\mathbb{Z}_{2+4k}^* \simeq \mathbb{Z}_2^* \times \mathbb{Z}_{1+2k}^* \simeq \{1\} \times \mathbb{Z}_{1+2k}^* \simeq \mathbb{Z}_{1+2k}^*$ that is isomorphic to the Galois group for the $n/2$ -th root of unity.

1.1 The circular units and the class number

Definiton 1.4. If \mathbb{K} is a number field (as $\mathbb{Q}(\zeta)$ and K) we can define the **ideal class group** as the quotient $\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ where:

$\mathcal{F}_{\mathbb{K}}$ is the group of the nonzero fractional ideals of the ring of integers $O_{\mathbb{K}}$, that are the $O_{\mathbb{K}}$ -submodules J of \mathbb{K} such that exists $r \in O_{\mathbb{K}}$ such that $rI \subset O_{\mathbb{K}}$

$\mathcal{P}_{\mathbb{K}}$ is the set of nonzero principal fractionary ideals, so the ideals generated by only one element

We will indicate the number of classes in $\mathcal{F}_{\mathbb{K}}/\mathcal{P}_{\mathbb{K}}$ as h_K . This number will measure the "distance" of $O_{\mathbb{K}}$ to became a unique factorization domain. In [4, Page 141] it is proven that actually the ideal class group is finite so h_K is well defined.

Definiton 1.5. For a field $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$ (with n minimal) we define the group of cyclotomic (or circular) units as the intesection $C_{\mathbb{K}}$ of the group generated by:

$$\{-1, \zeta, 1 - \zeta^a \text{ for } a = 1, \dots, n-1\}$$

and the unit group of $O_{\mathbb{K}}$ ($E_{\mathbb{K}}$). An elements of $C_{\mathbb{K}}$ is said to be a **circular unit** of \mathbb{K} .

In general the circular units aren't easy to describe, infact in general $1 - \zeta^a$ is not a unit, but for the particular case in which \mathbb{K} is the maximal real subfield (K) it has some intresting properties and it's related to the class number.

If $n = p^m$ where p is a prime it is possible to describe ([6, Lemma 8.1, Theorem 8.2]) explicitly the group of circular units as the group generated by -1 and:

$$\xi_a = \zeta^{\frac{1-a}{2}} \frac{1 - \zeta^a}{1 - \zeta} \text{ for } 1 < a < \frac{p^m}{2}, (a, p) = 1$$

Also we have the equality for the index:

$$[E_K : C_K] = h_K$$

Moreover Sinnott in [5] has generalized this to arbitrary n by showing that E_K/C_K is finite and the index is:

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

where if g is the number of distinct primes dividing n we have that $a = 0$ if $g = 1$ (as expected) and $a = 2^{g-2} + 1 - g$ otherwise. Even if the index is simple does not exist a simple construction of C_K , so we have the problem:

Explicitly construct a group C' with finite index $[E_K : C']$ that is *optimal*

Where we will understand later what we mean by *optimal*, but essentially we want the index to be small and with a simple factorization for $[E_K : C']/h_K$. In particular the construction of Greither will generalize the work of Ramachandra and Levesque, so we will omit them from now and see them later.

1.2 Dirichlet Characters

Definiton 1.6. Given a group X and a field \mathbb{F} a Dirichlet character is a group homomorphism $\chi : X \rightarrow \mathbb{F}^*$

In our case the field is \mathbb{C} and X is the Galois group $G_0 \simeq \mathbb{Z}_n^*$, so we can see the Dirichlet characters as homomorphisms: $\xi : \mathbb{Z}_n^* \rightarrow \mathbb{C}^*$. Since if $n|m$ there is a natural homomorphism $\mathbb{Z}_m^* \rightarrow \mathbb{Z}_n^*$, composing it with χ we can induct a new character $\hat{\chi} : \mathbb{Z}_m^* \rightarrow \mathbb{C}^*$. This characters are completely equivalent. So we can define k to be minimal positive integer such that exists a character $\chi' : \mathbb{Z}_k^* \rightarrow \mathbb{C}^*$ equivalent to χ , and call it the **conductor** of χ , denoted by $f_\chi := k$.

In some cases the character are also extended as ring homomorphisms from $\mathbb{Z}_n \rightarrow \mathbb{C}$, assuming χ to be zero on the non invertible elements. In this way the conductor can be seen as a sort of period, infact for all n we have $\chi(n) = \chi(n + f_\chi)$.

Also we need another object: the group ring $\mathbb{Z}[G]$, that is a free \mathbb{Z} -module with G as basis on which we define the addition (using the module addition) and the multiplication inducting it from the operation of G . This construction is also possible for a general ring and a multiplicative group:

Definiton 1.7. The group ring of X over R , denoted by $R[X]$ or RX , is the set of all mapping $f : X \rightarrow R$ with finite support (i.e. with finite $x \in X$ such that $f(x) \neq 0$). The addition and the scalar multiplication are defined as usual.

We can also have a group structure over $R[X]$ using the vector addition and the multiplication: were fg is defined as: $fg(x) = \sum_{y \in X} f(y)g(y^{-1}x) = \sum_{uv=x} f(u)g(v)$.

This is only a formal representation of the linear combinations, useful for the definition, but we will obviously use a simpler notation $f = \sum_{x \in X} f(x)x$.

Now we would like to generalize again the characters as ring homomorphism from $\mathbb{Z}[G]$ (or another Galois group) to \mathbb{C} . This is very simple since G is a basis for the free \mathbb{Z} -module its definition over the group is enough.

Notation. Given the elements $z \in \mathbb{Q}(\zeta)$ and $f \in \mathbb{Z}[G_0]$ it's well defined the power notation z^f , infact for $g \in G_0$ we have the well definiton for $z^g = g(z)$, $z^{g_1+g_2} = z^{g_1} z^{g_2}$ and $z^{-g} = (z^g)^{-1}$.

2 The Greither Setup

Let's consider an integer n (with $n \not\equiv 2 \pmod{4}$), with factorization $n = p_1^{e_1} \cdots p_s^{e_s}$ and let $S = \{1, \dots, s\}$. We will use the power set $\mathcal{P}_S = \{I \mid I \subseteq S\}$ and the notation $n_I = \prod_{i \in I} p_i^{e_i}$.

The Greither's idea is to define a subgroup starting from a function $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G_0]$, then varing β we have different subgroups but with similiar properties.

Definiton 2.1. A function β is called multiplicative if $\beta(\emptyset) = 1$ and for all sets I, J with empty intersection we have $\beta(I \cup J) = \beta(I)\beta(J)$.

A multiplicative function is uniquely determinated by its values on the singletons: $\{\{i\} \mid i \in S\}$ (we will use this later for a particular construction)

Consider a general function β and $I \in \mathcal{P}_S$, we define $z_I := 1 - \zeta^{n_I}$ and

$$z(\beta) := \prod_{I \in \mathcal{P}_S} z_I^{\beta(I)}$$

Using that $1 - \zeta^{-m} = -\zeta^{-m}(1 - \zeta^m)$, $\bar{\zeta} = \zeta^{-1}$ and the properties of complex conjugation we have that

$$\begin{aligned} \overline{z(\beta)} &= \prod_{I \in \mathcal{P}_S} (1 - \zeta^{-n_I})^{\beta(I)} = \prod_{I \in \mathcal{P}_S} -\zeta^{-n_I \beta(I)} (1 - \zeta^{n_I})^{\beta(I)} = \\ &= (-1)^{|\mathcal{P}_S|} \prod_{I \in \mathcal{P}_S} \zeta^{-n_I \beta(I)} z_I^{\beta(I)} = -\zeta^{-t} z(\beta) \text{ with } t = \sum n_I \beta(I) \end{aligned} \quad (1)$$

In $*$ we use that $|\mathcal{P}_S| = 2^s - 1$ is odd.

We define now for $a \in (1, n/2)$ coprime with n the real unit:

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

Where σ_a is the automorphism $\zeta \mapsto \zeta^a$. This is real because using the equation 1 and $\overline{\sigma_a(z)} = \sigma_a(\bar{z})$ we have:

$$\overline{\xi_a(\beta)} = \zeta^{-d_a(\beta)} \frac{\zeta^{-at} \sigma_a(z(\beta))}{\zeta^{-t} z(\beta)} = \xi_a(\beta) \quad (3)$$

And its a unit because its the product of circular units. We now use this units to define the goal group of the article:

C_β is the group generated by -1 and $\xi_a(\beta)$ for $1 < a < n/2$ and $(a, n) = 1$

For its index we will use the notation: $[E_K : C_\beta] = h_K i_\beta$.

2.1 A little remark

Sometimes it is easier to work with functions β to $\mathbb{Z}[G]$ instead of $\mathbb{Z}[G_0]$ and than consider a lift $\tilde{\beta} : \mathcal{P}_S \rightarrow \mathbb{Z}[G_0]$. Obviously this is not unique, but this is not a problem because we can show that C_β remain the same.

Remark 2. Given two set Z, Y and a function $\phi : Y \rightarrow Z$ we say that $f' : X \rightarrow Y$ is a **lift** of $f : X \rightarrow Z$ if $f = \phi \circ f'$, i.e. if the following diagram commute:

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

In our case ϕ is the morphism induced on the group ring by the projection $G_0 \simeq \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^* / \pm 1 \simeq G$

Initally we can observe that we can factor the real unit $\xi_a(\beta)$ with simpler real units

$$x_a(\beta, I) = \zeta^{\frac{(1-a)}{2} n_I \beta(I)} \frac{\sigma_a(z_I^{\beta(I)})}{z_I^{\beta(I)}}$$

such that we have the equality:

$$\xi_a(\beta) = \prod_{I \in \mathcal{P}_S} x_a(\beta, I) \quad (4)$$

Lemma 2.2. *Consider two functions β_1 and β_2 from \mathcal{P}_S to $\mathbb{Z}[G_0]$ such that for all $I \in \mathcal{P}_S$ their images of $\beta_i(I)$ coincides in $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{n/n_I})^+/\mathbb{Q})]$ ¹ for $i = 1, 2$. Then for all $I \in \mathcal{P}_S$ $x_a(\beta_i, I)$ coincides for $i = 1, 2$*

Proof. Obviously for all $I \in \mathcal{P}_S$ $x_a(\beta_i, I)$ depends only on the image of β_i over $z_I = 1 - \zeta_n^{n_I} \in \mathbb{Q}(\zeta_{n/n_I})^2$, so it's enough to show the equivalence over $\mathbb{Q}(\zeta_{n/n_I})$. Since the two functions are equal on $\mathbb{Q}(\zeta_{n/n_I})^+$ their difference $\beta_1(I) - \beta_2(I)$ is the identity on the reals, so it is a multiple of $1 - j$, where j is the complex conjugation. We can observe now, using morphism properties, that exist a unit r such that:

$$\mathbb{Q}(\zeta_{n/n_I})^+ \ni q = \frac{x_a(\beta_1, I)}{x_a(\beta_2, I)} = \left(\zeta^{\frac{(1-a)}{2} n_I} \frac{\sigma_a(z_I)}{z_I} \right)^{\beta_1(I) - \beta_2(I)} = r^{1-j}$$

¹Observe that $\mathbb{Q}(\zeta_{n/n_I})^+$ is a subfield of K since $\zeta_{n/n_I} = \zeta_n^{n_I}$, and since we see the elements of the group rings as homomorphism of fields make sense to compare two elements for their image on $\mathbb{Q}(\zeta_{n/n_I})^+$

² $\zeta_{n/n_I} = \zeta_n^{n_I}$

So we have that $\bar{q} = q^j = r^{(1-j)j} = r^{j-1} = q^{-1}$ (since $j^2 = 1$), that for real numebers happen only for ± 1 \square

Remark 3. For what we have seen in the equation 4 it follows immediatly that also $\xi_a(\beta)$ is unique up to a sign if β is a lifting of a function from \mathcal{P}_S to $\mathbb{Z}[G]$. Since the group C_β contains -1 it is enough to have a function $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ for its definition.

3 Index calculation

Theorem 3.1. *For any function $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ we have*

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{even}}} \left(\sum_{\substack{I \in \mathcal{P}_S \\ (f_\chi, n_I)=1}} \phi(n_I) \cdot \chi(\beta(I)) \cdot \prod_{i \notin I} (1 - \chi^{-1}(p_i)) \right) \quad (5)$$

Remarks 4 (On theorem 3.1). • ϕ is the Euler totient function

- A character χ is said to be **even** if $\chi(-1) = 1$
- With χ^{-1} we mean the character defined as $1/\chi$ on the invertible elements and zero otherwise, that is also a morphism because $1/(xy) = (1/x)(1/y)$.

For the proof we need the following Lemmas:

Lemma 3.2. *For $z \in \mathbb{Q}(\zeta)^*$ and $\gamma \in \mathbb{Z}[G_0]$, then for any character χ we have:*

$$\sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a \gamma}| = \chi(\gamma) \sum_{(a,n)=1} \chi^{-1}(a) \log |z^{\sigma_a}| \quad (6)$$

Proof. It is easy to prove this for $\gamma = \sigma_g \in G_0$, infact since g is invertible in \mathbb{Z}_n is possible to change the index from $(a, n) = 1$ to $(ag, n) = 1$ and rearrange. Then we can pass to $\mathbb{Z}[G_0]$ using the additivity of χ and the logarithm of exponential (also the modulo is multiplicative). \square

For the calculation of the index we need a new object that allows to evaluate a :

Definiton 3.3. The **regulator** R_L of a number fields L is defined as follows: given its rank r , a set of independent units $\{\epsilon_1, \dots, \epsilon_r\} \subset L$ and $\{\sigma_1, \dots, \sigma_{r+1}\}$ its embedding into \mathbb{R} or \mathbb{C} . Set δ_j to be 1 if σ_j is real, and 2 otherwise.

Then:

$$R_L(\epsilon_1, \dots, \epsilon_r) = |\det(\delta_i \log |\epsilon_j^{\sigma_i}|)_{1 \leq i, j \leq r}| \quad (7)$$

Remark 5. The embedding that we decide to omit is not relevant, infact since they are units their norm is 1, so $\sum_i \delta_i \log |\epsilon_j^{\sigma_i}| = \log |\prod_i \epsilon_j^{\delta_i \sigma_i}| = \log |N(\epsilon_j)| = 0$, so writing this equality as a linear system from Cramer formula follows the uniqueness of the determinant up to a sign.

Now we need to recall some Lemmas from [6] without the proofs:

Lemma 3.4 (Lemma 4.15 in [6]). *Given the groups $A \subset B$ of finite index, generated by independent units of a number field L , respectively $\{\epsilon_i\}_{i=1}^r$ and $\{\mu_i\}_{i=1}^r$:*

$$[B : A] = \frac{R_L(\epsilon_1, \dots, \epsilon_r)}{R_L(\mu_1, \dots, \mu_r)} \quad (8)$$

Lemma 3.5 (Lemma 5.26 in [6]). *Let X be a finite abelian group and let f be a function on X with values in \mathbb{C}*

$$\det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma, \tau \neq 1} = \prod_{\substack{\chi \in \hat{X} \\ \chi \neq 1}} \sum_{\sigma \in X} \chi(\sigma) f(\sigma) \quad (9)$$

Where \hat{X} is the set of homomorphisms (characters) from X to \mathbb{C}^*

In our case X will be $G \equiv \mathbb{Z}_n / \pm 1$, and so the elements of \hat{X} are the even characters of \mathbb{Z}_n .

Proof of Theorem 3.1 . Using Lemma 3.4 we can evaluate $[E_K : C_\beta]$ with the quotient of the regulators. In the equation 8 we can omit the unit -1 since it is contained in both the two groups (for what we have said in 5 can only change a sign).

So we need to prove that $R(\xi_a(\beta)) = \pm R_K h_K A$ with $(a, n) = 1$, $1 < a < n/2$ and A be the right part of the equation 5. The \pm is a more simple way to indicate that we don't matter the sign without inserting everything in a modulo.

From definition, using that δ_i is always 1 since the units are all real and the embeddings can be seen as elements of the Galois Group G :

$$\begin{aligned} R(\xi_a(\beta)) &= \pm \det[\log |\xi_a(\beta)^\tau|] \quad ((a, n) = 1, 1 < a < n/2; \tau \in G) \\ &\stackrel{(1)}{=} \pm \det[f(\tau\sigma) - f(\tau)]_{\sigma, \tau \in G-1} \quad \text{with } f(\sigma) = \log |\sigma z(\beta)| \\ &= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{(a, n)=1} \chi^{-1}(a) \log |\sigma_a z(\beta)| \quad \text{using Lemma 3.5} \\ &= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{(a, n)=1} \chi^{-1}(a) \sum_{I \in \mathcal{P}_S} \log |(1 - \zeta^{n_i a})^{\beta(I)}| \\ &= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{I \in \mathcal{P}_S} \left(\sum_{(a, n)=1} \chi^{-1}(a) \log |(1 - \zeta^{n_i a})^{\beta(I)}| \right) \\ &\stackrel{6}{=} \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{I \in \mathcal{P}_S} \left(\chi(\beta(I)) \sum_{(a, n)=1} \chi^{-1}(a) \log |(1 - \zeta^{n_i a})| \right) \end{aligned}$$

Where in (1) we have used that $\log |\zeta^d| = 0$ because ζ is a unit and the logarithm's properties.

The last part is a bit technical and uses [6, Lemma 8.4] to reduce the first sum to the $I \in \mathcal{P}_S$ such that $(f_\chi, n_I) = 1$, and then continues as for the proof of Theorem 8.3 in [6, Pages 148-150] and involves the analytic class number formula and Dirichlet L-series (also Chapter 4 in [6]). \square

3.1 Particular case of formula 5

Now we can try to see what happen if we request some conditions over β , with some particular cases.

Theorem 3.6. *If we assume $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$ to be multiplicative then:*

$$i_\beta = \prod_{\substack{\chi \neq 1 \\ \text{even}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) \cdot \chi(\beta(i)) + 1 - \chi^{-1}(p_i)) \right) \quad (10)$$

Where $\beta(i)$ mean $\beta(\{i\})$

Proof. It is easy that we can lift β to $\mathbb{Z}[G_0]$ conserving multiplicativity. Consider now, for $\chi \neq 1$ even, the two factors :

$$T_\chi = \sum_{\substack{I \in \mathcal{P}_S \\ (f_\chi, n_I)=1}} \phi(n_I) \cdot \chi(\beta(I)) \cdot \prod_{i \notin I} (1 - \chi^{-1}(p_i)) \quad (11)$$

and

$$U_\chi = \prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) \cdot \chi(\beta(i)) + 1 - \chi^{-1}(p_i)) \quad (12)$$

that are the arguments of the products in equations 5 and 10. So it's enough to prove $U_\chi = T_\chi$. Initially we can observe that the argument of the sum in 11 are the subset of $S_\chi = \{i \mid p_i \nmid f_\chi\}$. Also we can observe

$$\begin{aligned} \phi(n_I) &= \prod_{i \in I} \phi(p_i^{e_i}) \\ \chi(\beta(I)) &= \chi \left(\prod_{i \in I} \beta(i) \right) = \prod_{i \in I} \chi(\beta(i)) \end{aligned}$$

From which expanding the product of U_χ we get the equality. \square

Using this formula and the definition of C_β we can see that for $\beta \equiv 1$ (that is the simplest example of multiplicative β) we get the Ramachandra's unit index from [3] (or in a more modern notation [6, Theorem 8.3]):

$$[E_K : C_R] = h_K \cdot \prod_{\substack{\chi \neq 1 \\ \text{even}}} \left(\prod_{p_i \nmid f_\chi} (\phi(p_i^{e_i}) + 1 - \chi(p_i)) \right) \quad (13)$$

Where C_R is the group generated by -1 and the units of the form of 2 with $\beta(I) = 1$:

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

We can also construct β multiplicative such that:

$$\beta(i) = \begin{cases} 1 & \text{if exists } \chi \neq 1 \text{ even, with } \chi(p_i) = 1 \\ 0 & \text{otherwise} \end{cases}$$

And we obtain the Levesque group $C_{\mathcal{D}}$ defined in [2, Page 331]

3.2 A new system of units

Following the previous steps we know construct a new multiplicative map β with a more optimal index.

Notation. If x is an element of finite group Γ we define:

$$N_x := 1 + x + \dots + x^{\text{ord}(x)-1} \in \mathbb{Z}[\Gamma]$$

This will be called *trace* element of x .

Let now define G_i for $i = 1, \dots, s$ to be the Galois group $\text{Gal}(\mathbb{Q}(\zeta_{n/p_i^{e_i}})^+/\mathbb{Q})$. Consider now the Frobenius automorphism $F_i \in G_i$:

$$\begin{aligned} F_i : \mathbb{Q}(\zeta_{n/p_i^{e_i}})^+ &\longrightarrow \mathbb{Q}(\zeta_{n/p_i^{e_i}})^+ \\ \zeta_{n/p_i^{e_i}} &\longmapsto \zeta_{n/p_i^{e_i}}^{p_i} \end{aligned}$$

and its trace element $N_{F_i} \in \mathbb{Z}[G_i]$. Now we choose for every $i = 1, \dots, s$ a lift of N_{F_i} into $\mathbb{Z}[G_0]^3$ and associate it to $\beta(i)$; then β is defined multiplicatively.

Of course β is not unique, but for all $I \in \mathcal{P}_S$ they coincide in $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{n/n_I})^+/\mathbb{Q})]$, so we can use Lemma 2.2 and C_β is well defined.

3.3 A factorization for i_β

Here we will recall some facts and definitions from [4, Chapter 11]. These are generalities for a finite separable extension of a number field, but we will restrict in the case of \mathbb{K}/\mathbb{Q} number field.

Consider a prime p in \mathbb{Z} and its ideal extension in the ring of integers $pO_{\mathbb{K}}$. Since O_K is a Dedekind domain we can factorize it with prime ideals:

$$pO_{\mathbb{K}} = \prod_{j=1}^g \mathfrak{p}_j^{e_j} \tag{14}$$

³Remind that $\zeta_{n/p_i^{e_i}} = \zeta_n^{p_i^{e_i}}$

Definiton 3.7. The number g is said to be the *decomposition degree* (or number) of p in the extension \mathbb{K}/\mathbb{Q} .

For every $j = 1, \dots, g$, ϵ_j is said to be the *ramification degree* (or index) of \mathfrak{p}_j in \mathbb{K}/\mathbb{Q} .

For every $j = 1, \dots, g$, $f_j := [O_{\mathbb{K}}/\mathfrak{p}_j : \mathbb{Z}_p]$ is called the *inertial degree* (or residual).

In particular is possible to prove that if $n = [\mathbb{K} : \mathbb{Q}]$ so

$$n = \sum_{j=1}^g f_j \epsilon_j$$

Also if \mathbb{K}/\mathbb{Q} is a Galois extension then also ϵ_j, f_j does not depend on j and so

$$n = \epsilon f g$$

We also recall from [6, Theorem 3.7] the relation between the characters X over the galois group of \mathbb{K}/\mathbb{Q} and decomposition degree of p in the extension \mathbb{K}/\mathbb{Q} :

$$g = |\{\chi \in X \mid \chi(p) = 1\}| \quad (15)$$

We have now the ingredients for evaluating in a optimal way i_β .

For $i \in 1, \dots, s$ define g_i, f_i, ϵ_i to be as in the definition 3.7 for the prime p_i in K/\mathbb{Q} .

Is possible to show (fact A in [4, Page 544]) that the inertia degree f_i is closely realted with the Frobenius morphism, in fact

$$f_i = \text{ord}(F_i)$$

Theorem 3.8. *With C_β defined as before we have*

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

Remark 6. This index is *optimal* because we have a lot of info about its factorization for definiton, also since ϵ_i and f_i are factors of n , the factorization of the last one is enough to know the i_β 's. We will see later that is also smaller than other index already studied.

Proof. For $s = 1$ this is trivial, since $i_\beta = 1$.

For $s \geq 2$ is possible to prove that $\epsilon_i = \phi(p_i^{e_i})$. For $i \in S$ and χ such that $p_i \nmid f_\chi$ we define

$$y(\chi, i) = \phi(p_i^{e_i}) \cdot \chi(\beta(i)) + 1 - \chi^{-1}(p_i)$$

Considering $\bar{\chi}$ to be the character induced by χ in G_i we have $\chi(\beta(i)) = \bar{\chi}(N_{F^i})$ and $\chi(p_i) = \bar{\chi}(F_i)$ using the isomorphism between G_i and the relative modulo ring. There are two cases:

$$\chi(p_i) = 1 : \overline{\chi}(N_{F_i}) = \sum \overline{\chi}(F_i)^j = \sum 1 = \text{ord}(F_i) = f_i \text{ and so } y(\chi, i) = \phi(p_i^{e_i})f_i + 0 = \epsilon_i f_i$$

$$\chi(p_i) \neq 1 : \text{Since } \overline{\chi}(F_i) \neq 1 \text{ follows } \overline{\chi}(N_{F_i}) = 0. \text{ Hence } y(\chi, i) = \phi(p_i^{e_i}) \cdot \chi 0 + 1 - \chi^{-1}(p_i) = 1 - \chi^{-1}(p_i)$$

Then, indexing the product by i :

$$\begin{aligned} i_\beta &= \prod_{i=1}^s \prod_{\substack{\chi \neq 1 \text{ even} \\ p_i \nmid f_\chi}} y(\chi, i) \\ &= \prod_{i=1}^s \left(\prod_{\chi(p_i)=1} \epsilon_i f_i \prod_{\chi(p_i) \neq 1} (1 - \chi^{-1}(p_i)) \right) \quad (\chi \neq 1 \text{ even}, p_i \nmid f_\chi) \\ &= \prod_{i=1}^s ((\epsilon_i f_i)^{g_i-1} \cdot f_i^{g_i}) \\ &= \prod_{i=1}^s \epsilon_i^{g_i-1} f_i^{2g_i-1} \end{aligned}$$

In * the exponent $g_i - 1$ come from 15 (there isn't the trivial character). Instead for the second part we are using that, since $\chi^{-1}(p_i) = \overline{\chi^{-1}}(F_i)$ is a non trivial $\text{ord}(F_i) = f_i$ -th root of unity for all characters (and varing χ we get every unit g_i times) we use that from the factorization of $x^f - 1$ as $(x-1)(1+x+\dots+x^{f-1})$ evaluated in 1 we have $\prod_{\zeta^f=1, \zeta \neq 1} (1 - \zeta) = f$. □

References

- [1] 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.
- [2] Claude Levesque. *On improving Ramachandra’s unit index*. English. Number theory, Proc. 1st Conf. Can. Number Theory Assoc., Banff/Alberta (Can.) 1988, 325-338 (1990). 1990.
- [3] K. Ramachandra. “On the units of cyclotomic fields”. English. In: *Acta Arith.* 12 (1966), pp. 165–173. ISSN: 0065-1036; 1730-6264/e.
- [4] Paulo Ribenboim. *Classical theory of algebraic numbers*. English. New York, NY: Springer, 2001, pp. xxiv + 681. ISBN: 0-387-95070-2/hbk.
- [5] 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.
- [6] Lawrence C. Washington. *Introduction to cyclotomic fields*. English. Vol. 83. Springer, New York, NY, 1982.