

Giacomo Borin

April 12, 2021

### Abstract

Stuff Stuff Stuff

## 1 Introduction to the working set

Consider the  $n$ -th cyclotomic field  $\mathbb{Q}(\zeta_n)$  with  $\zeta_n$  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  $\zeta_n$  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:

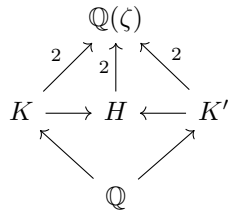
$$\overline{\zeta + \zeta^{-1}} = \bar{\zeta} + \bar{\zeta}^{-1} = \zeta^{-1} + \zeta$$

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

Since  $\mathbb{Q}(\zeta)$  is complex (so strictly greater) the index  $e := [\mathbb{Q}(\zeta) : K] \geq 2$ .

Consider now the polynomial of degree 2 in  $K[x] : f = (x - \zeta)(x - \zeta^{-1}) = x^2 - (\zeta + \zeta^{-1})x + 1$ , since  $\zeta$  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  $K$  [5, 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  $\mathbb{Q}(\xi)/\mathbb{Q}$  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  $\alpha_i$  to  $\alpha_{i|_G}$  where  $\alpha_i$  is the automorphism that maps  $\zeta$  to  $\zeta^i$ . Obviously  $\sigma$  is a morphism of groups. Also it is easy to describe its kernel:

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

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 remainder 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  $K$  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 become a unique factorization domain. In [3, 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 intersection  $C_{\mathbb{K}}$  of the group generated by:

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

and the unit of  $\mathbb{K}$  ( $E_{\mathbb{K}}$ ). An element 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 interesting properties and it's related to the class number.

If  $n = p^m$  where  $p$  is a prime it is possible to describe ([5, 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 [4] has improved this 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  $\mathbb{Z}_m^* \rightarrow \mathbb{Z}_n^*$  we can induct a new character using the composition from  $\mathbb{Z}_m^*$ . This characters are completely equivalent, so we can choose  $n$  to be minimal and call it the **conductor** of  $\chi$ , denoted by  $f_\chi$ .

In some cases the character are also extended as ring homomorphisms from  $\mathbb{Z}_n \rightarrow \mathbb{C}$ , assuming  $\chi$  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 inducing 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  $z^g = g(z)$ ,  $z^{g_1+g_2} = z^{g_1}z^{g_2}$  and  $z^{-g} = (z^g)^{-1}$ .

### 1.3 Bho

**Definiton 1.8.** Let  $G$  be a group and  $R$  a commutative ring, let's consider the *augmentation map*  $\epsilon : R[G] \rightarrow R$  that sends every  $g \in G$  to  $1_R$  and every  $r \in R$  to itself and its an homomorphism of  $R$ -modules. We also say that the kernel of  $\epsilon$  is the *augmentation ideal*

## 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  $S = \{1, \dots, n\}$ . 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  $\beta$  we have different subgroups but with similiar properties.

**Definiton 2.1.** A function  $\beta$  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 univocally determinated from its value over the singletons:  $\{\{i\} \mid i \in S\}$  (we will use this later for a particular construction)

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

$$z(\beta) := \prod_{i \in I} z_I^{\beta(I)}$$

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

conjugation we have that

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

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

$C_\beta$  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  $\beta$  to  $\mathbb{Z}[G]$  instead of  $\mathbb{Z}[G_0]$  (as we will do later), but this is not a problem because we can show that with some hypothesis  $C_\beta$  remain the same.

Initially 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  $\beta_1$  and  $\beta_2$  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  $\mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{n/n_I})^+/\mathbb{Q})]$ <sup>1</sup> for  $i = 1, 2$ . Then for all  $I \in \mathcal{P}_S$   $x_a(\beta_i, I)$  coincides for  $i = 1, 2$*

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

*Proof.* Obviously for all  $I \in \mathcal{P}_S$   $x_a(\beta_i, I)$  depends only on the image of  $\beta_i$  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:

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

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  $\pm 1$   $\square$

*Remark 2.* For what we have seen in the equation 4 it follows immediatly that also  $\xi_a(\beta)$  is unique up to a sign if  $\beta$  is a lifting of a function from  $\mathcal{P}_S$  to  $\mathbb{Z}[G]$ . Since the group  $C_\beta$  contains  $-1$  it is enough to have a function  $\beta : \mathcal{P}_S \rightarrow \mathbb{Z}[G]$  for its definition.

## 2.2 Index calculation

**Theorem 2.3.** *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 3* (On theorem 2.3). •  $\phi$  is the Euler totient function

- A character  $\chi$  is said to be **even** if  $\chi(-1) = 1$
- With  $\chi^{-1}$  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 2.4.** *For  $z \in \mathbb{Q}(\zeta)^*$  and  $\gamma \in \mathbb{Z}[G_0]$ , then for any character  $\chi$  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  $\chi$  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 :

---


$${}^2\zeta_{n/n_I} = \zeta_n^{n_I}$$

**Definiton 2.5.** 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  $\delta_j$  to be 1 if  $\sigma_j$  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 4.* 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 [5] without the proofs:

**Lemma 2.6** (Lemma 4.15 in [5]). *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 2.7** (Lemma 5.26 in [5]). *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 2.3 .* Using Lemma 2.6 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 4 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  $\delta_i$  is always 1 since the units are all real and the

embeddings can be seen as elements of the Galois Group  $G$ :

$$\begin{aligned}
R(\xi_a(\beta)) &= \pm \det[\log |\xi_a(\beta)^\tau|] \quad ((a, n) = 1, 1 < a < n/2; \tau \in G) \\
&\stackrel{(1)}{=} \pm \det[f(\tau\sigma) - f(\tau)]_{\sigma, \tau \in G-1} \quad \text{with } f(\sigma) = \log |\sigma z(\beta)| \\
&= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{(a, n)=1} \chi^{-1}(a) \log |\sigma_a z(\beta)| \quad \text{using Lemma 2.7} \\
&= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{(a, n)=1} \chi^{-1}(a) \sum_{I \in \mathcal{P}_S} \log |(1 - \zeta^{n_i a})^{\beta(I)}| \\
&= \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{I \in \mathcal{P}_S} \left( \sum_{(a, n)=1} \chi^{-1}(a) \log |(1 - \zeta^{n_i a})^{\beta(I)}| \right) \\
&\stackrel{6}{=} \prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} \sum_{I \in \mathcal{P}_S} \left( \chi(\beta(I)) \sum_{(a, n)=1} \chi^{-1}(a) \log |(1 - \zeta^{n_i a})| \right)
\end{aligned}$$

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

The last part is a bit technical and uses [5, Lemma 8.4] to reduce the first sum to the  $I \in \mathcal{P}_S$  such that  $(f_\chi, 1) = 1$ , and then continues as for the proof of Theorem 8.3 in [5, Pages 148-150] and involves the analytic class number formula and Dirichlet L-series (also Chapter 4 in [5]).  $\square$

### 3 Particular case of formula 5

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

**Theorem 3.1.** *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  $\beta$  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  $U_\chi$  we get the equality.  $\square$

Using this formula and the definition of  $C_\beta$  we can see that for  $\beta$  costant to 1 (that is the simplest example of multiplicative  $\beta$ ) we get the Ramachandra's unit index from [2] (or in a more modern notation [5, 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  $\beta(I) = 1$ :

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

We can also coNstruct  $\beta$  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 [1, Page 331]

### 3.1 A new system of units

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

**Notation.** If  $x$  is an element of finite group  $\Gamma$  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:

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

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  $\mathbb{Z}[G_0]$ <sup>3</sup> and associate it to  $\beta(i)$ ; then  $\beta$  is defined multiplicatively.

Of course  $\beta$  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  $C_\beta$  is well defined.

### 3.2 A factorization for $i_\beta$

Here we will recall some facts and definitions from [3, Chapter 11]. These are general 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:

$$pO_{\mathbb{K}} = \prod_{i=1}^g \mathfrak{p}_i^{e_i} \quad (14)$$

**Definiton 3.2.** The number  $g$  is said to be the *decomposition degree* (or number) of  $p$  in the extension  $\mathbb{K}/\mathbb{Q}$ .

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

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

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

$$n = \sum_{i=1}^g f_i e_i$$

Also if  $\mathbb{K}/\mathbb{Q}$  is a Galois extension then also  $e_i, f_i$  does not depend on  $i$  and so

$$n = efg$$

We also recall from [5, 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  $i_\beta$ .

For  $i \in 1, \dots, s$  define  $g_i, f_i, e_i$  to be as in the definition 3.2 for the prime  $p_i$  in  $K/\mathbb{Q}$ .

---

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

**Theorem 3.3.** *With  $C_\beta$  as defined before we have*

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

*Remark 5.* This index is *optimal* because we have a lot of info about its factorization for definiton, also since  $e_i$  and  $f_i$  are factors of  $n$ , the factorization of the last one is enough to know the  $i_\beta$ '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  $e_i = \phi(p_i^{e_i})$ . For  $i \in S$  and  $\chi$  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  $\chi$  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:

$\chi(p_i) = 1$  :  $\bar{\chi}(N_{F_i}) = \sum \bar{\chi}(F_i)^j = \sum 1 = \text{ord}(F_i) = f_i$  (from fact A in [3, Page 544])  
and so  $y(\chi, i) = \phi(p_i^{e_i})f_i + 0 = e_i f_i$

$\chi(p_i) \neq 1$  : Since  $\bar{\chi}(F_i) \neq 1$  follows  $\bar{\chi}(N_{F_i}) = 0$ . 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  $i$ :

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

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  $\chi$  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] 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.
- [2] K. Ramachandra. "On the units of cyclotomic fields". English. In: *Acta Arith.* 12 (1966), pp. 165–173. ISSN: 0065-1036; 1730-6264/e.
- [3] Paulo Ribenboim. *Classical theory of algebraic numbers*. English. New York, NY: Springer, 2001, pp. xxiv + 681. ISBN: 0-387-95070-2/hbk.
- [4] 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.
- [5] Lawrence C. Washington. *Introduction to cyclotomic fields*. English. Vol. 83. Springer, New York, NY, 1982.