Giacomo Borin

April 7, 2021

Abstract

Stuff Stuff Stuff

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 $n \not\equiv 2 \mod 4$, 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 easly see that K is real, infact since for the root of unity $\overline{\zeta} = \zeta^{-1}$ (complex conjugation) and so:

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

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 ζ is a root obviosly $e \leq 2$, so the subfield K has maximal degre 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. $\square$

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

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 [3, Proposition 2.16] similiarly to what happens for $O_{\mathbb{Q}(\zeta)}$ (infact the proof follows without difficulty from this)

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

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 se 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 $\sigma : G_0 \to G$ that maps α_i to $\alpha_{i|_G}$ 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 kernerl:

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

Where (1) follows from the fact that $K = \mathbb{Q}(\zeta + \zeta^{-1})$ and (2) from linear algebra. So from the first theoremo 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. □

Remark. We excluded the case of $n \equiv 2 \mod 4$ 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 circluar 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 became a unique factorization domain. In [1, 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:

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

and the unit of $\mathbb{K}$ ($E_{\mathbb{K}}$). 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 ([3, Lemma 8.1, Theorem 8.2]) explicitly the group of circluar 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 Sinnot in [2] has imporved 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 $a = 2^{g-2}+1-g$ otherwhise. Even if the index is simple does not exist a simple costruction 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 costruction 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 $\chi : X \to \mathbb{F}^*$

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: $\xi : \mathbb{Z}_n^* \to \mathbb{C}^*$. Since if $n|m$ there is a natural homomorphism $\mathbb{Z}_m^* \to \mathbb{Z}_n^*$ 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 χ, denoted by f_χ.

In some cases the character are also extended as ring homomorphisms from $\mathbb{Z}_n \to \mathbb{C}$, 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 moltiplication inducting it from the operation of G. This costruction 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 $f : X \to R$ 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 obviosly use a simpler notation $f = \sum_{x \in X} f(x)x$.

Now we would like to generalize again the characters as ring homorphism 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 enougth.

Notation. Given the elements $z \in \mathbb{Q}(\zeta)$ and $f \in \mathbb{Z}[G_0]$ it's well defined the power notation x^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* $\epsilon : R[G] \to R$ 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 ϵ is the *augmentation ideal*

2 The Greither Construction

Let's consider an integer n (with $n \not\equiv 2 \mod 4$), with factorization $n = p_1^{e_1} \cdots p_s^{e_s}$ and let $S = \{1, ..., n\}$. We will use the power set $\mathcal{P}_S = \{I \mid I \subsetneq S\}$ 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 $\beta : \mathcal{P}_S \to \mathbb{Z}[G_0]$, 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 univocally determinated from its value over the singletons: $\{\{i\} \,|, \, i \in S\}$ (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

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

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

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

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 $\overline{\sigma_a(z)} = \sigma_a(\overline{z})$ 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 $\mathbb{Z}[G_0]$ (as we will do later), but this is not a problem because we can show that with somo hypotesis C_β remain the same.

Initally we can osserve 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 $\xi_a(\beta) = \prod_{I\in\mathcal{P}_S} x_a(\beta, I)$.

References

[1] Paulo Ribenboim. *Classical theory of algebraic numbers*. English. New York, NY: Springer, 2001, pp. xxiv + 681. ISBN: 0-387-95070-2/hbk.

[2] 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.

[3] Lawrence C. Washington. *Introduction to cyclotomic fields*. English. Vol. 83. Springer, New York, NY, 1982.