Algebraic number theory **LTCC 2008**

Lecture notes, Part 4

10. Cyclotomic fields

Let $n \in \mathbb{N}$ and $\zeta_n = \exp(2\pi i/n) \in \mathbb{C}$. Then ζ_n is a primitive n-th root of unity, i.e. ζ_n is a root of unity which has order n. The algebraic number fields $\mathbb{Q}(\zeta_n)$ for $n \in \mathbb{N}$ are called *cyclotomic fields.* If $m \mid n$ then $\zeta_m = (\zeta_n)^{n/m} \in \mathbb{Q}(\zeta_n)$ and therefore $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$. Note that if n is odd, then $\zeta_{2n} = -(\zeta_n)^{(n+1)/2} \in \mathbb{Q}(\zeta_n)$ and hence $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$. We can therefore assume that n is either odd or divisible by 4, i.e. that $n \not\equiv 2 \pmod 4$. To avoid the trivial case $\mathbb{Q}(\zeta_1) = \mathbb{Q}$ we will also assume that $n \neq 1$.

Theorem 10.1. *Let $n > 1$ be an integer and assume that $n \not\equiv 2 \pmod 4$.*

1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ *where ϕ is Euler's ϕ-function.*
2. *The field $\mathbb{Q}(\zeta_n)$ is totally complex, i.e. the image of every embedding $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{C}$ is not contained in $\mathbb{R}$.*
3. *The group of roots of unity in $\mathbb{Q}(\zeta_n)$ is*
$$\mu_{\mathbb{Q}(\zeta_n)} = \begin{cases} \{\pm\zeta_n^i : 0 \le i \le n-1\} & \text{if } n \text{ is odd,} \\ \{\zeta_n^i : 0 \le i \le n-1\} & \text{if } n \text{ is divisible by } 4. \end{cases}$$
4. $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\phi(n)-1}$ *is an integral basis of the ring of integers of $\mathbb{Q}(\zeta_n)$.*

Proof. (1) See [1, Theorem 2.5].
(2) If $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{C}$ is any embedding then $\sigma(\zeta_n) \notin \mathbb{R}$ because $\sigma(\zeta_n)$ is an element of order n in $\mathbb{C}^\times$ but the only elements of finite order in $\mathbb{R}^\times$ are ± 1.
(3) Exercise.
(4) See [1, Theorem 2.6]. □

If $\alpha \in \mathbb{Q}(\zeta_n) \subset \mathbb{C}$ then the complex conjugate $\overline{\alpha}$ also lies in $\mathbb{Q}(\zeta_n)$ because $\overline{\zeta_n} = \zeta_n^{-1} \in \mathbb{Q}(\zeta_n)$. Therefore complex conjugation induces an automorphism of the field $\mathbb{Q}(\zeta_n)$. We define $\mathbb{Q}(\zeta_n)^+$ to be the fixed field of $\mathbb{Q}(\zeta_n)$ under complex conjugation, i.e.
$$\mathbb{Q}(\zeta_n)^+ = \{\alpha \in \mathbb{Q}(\zeta_n) : \overline{\alpha} = \alpha\}.$$
The field $\mathbb{Q}(\zeta_n)^+$ is called the *maximal real subfield* of $\mathbb{Q}(\zeta_n)$.

Theorem 10.2. *Let $n > 1$ be an integer and assume that $n \not\equiv 2 \pmod 4$.*

1. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$ *and* $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \phi(n)/2$.
2. *The field $\mathbb{Q}(\zeta_n)^+$ is totally real, i.e. the image of every embedding $\sigma : \mathbb{Q}(\zeta_n)^+ \to \mathbb{C}$ is contained in $\mathbb{R}$.*
3. *The group of roots of unity of $\mathbb{Q}(\zeta_n)^+$ is $\mu_{\mathbb{Q}(\zeta_n)^+} = \{\pm 1\}$.*
4. $1, \zeta_n + \zeta_n^{-1}, (\zeta_n + \zeta_n^{-1})^2, \ldots, (\zeta_n + \zeta_n^{-1})^{\phi(n)/2-1}$ *is an integral basis of the rings of integers of $\mathbb{Q}(\zeta_n)^+$.*

Proof. (1) Complex conjugation generates a subgroup of order 2 of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2$ by Galois theory. From this $[\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = \phi(n)/2$ follows because
$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] \cdot [\mathbb{Q}(\zeta_n)^+ : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n).$$

(2) Let $\sigma : \mathbb{Q}(\zeta_n)^+ \to \mathbb{C}$ be an embedding. Then σ can be extended to an embedding $\sigma' : \mathbb{Q}(\zeta_n) \to \mathbb{C}$. Since $\sigma'(\zeta_n)$ is a primitive n-th root of unity in $\mathbb{C}$, it follows that $\sigma'(\zeta_n) = \zeta_n^a$ for some integer a with $(a, n) = 1$. Hence $\overline{\sigma'(\zeta_n)} = \overline{\zeta_n^a} = \zeta_n^{-a} = \sigma'\big(\zeta_n^{-1}\big) = \sigma'\big(\overline{\zeta_n}\big)$. This implies that $\overline{\sigma'(\alpha)} = \sigma'(\overline{\alpha})$ for all $\alpha \in \mathbb{Q}(\zeta_n)$ because ζ_n generates $\mathbb{Q}(\zeta_n)$. Therefore $\overline{\sigma(\alpha)} = \sigma(\alpha)$ for all $\alpha \in \mathbb{Q}(\zeta_n)^+$. This shows that $\sigma(\mathbb{Q}(\zeta_n)^+) \subseteq \mathbb{R}$, so σ is a real embedding.

(3) This is obvious since $\mathbb{Q}(\zeta_n)^+$ is a subfield of $\mathbb{R}$ and $\{\pm 1\}$ are the only roots of unity in $\mathbb{R}$.

(4) See [1, Proposition 2.16]. □

As before let $n > 1$ be an integer with $n \not\equiv 2 \pmod 4$. To simplify the notation we now write $K = \mathbb{Q}(\zeta_n)$ and $K^+ = \mathbb{Q}(\zeta_n)^+$. We want to study the relation between the unit groups of R_{K^+} and of R_K. It is clear that $R_{K^+}^\times$ is a subgroup of $R_K^\times$ because $R_{K^+} \subset R_K$ The field K has no real embeddings and $\phi(n)$ complex embeddings, so by Dirichlet's unit theorem we have

$$R_K^\times \cong \mu_K \times \mathbb{Z}^{\phi(n)/2-1}.$$

The field K^+ has $\phi(n)/2$ real embeddings and no complex embeddings, so by Dirichlet's unit theorem we have

$$R_{K^+}^\times \cong \{\pm 1\} \times \mathbb{Z}^{\phi(n)/2-1}.$$

Hence the groups $R_{K^+}^\times$ and $R_K^\times$ have the same rank. This implies that $R_{K^+}^\times$ has finite index in $R_K^\times$. More precisely we have the following result.

Theorem 10.3. *Let $K = \mathbb{Q}(\zeta_n)$ and $K^+ = \mathbb{Q}(\zeta_n)^+$ where $n > 1$ and $n \not\equiv 2 \pmod 4$. Then*

$$[R_K^\times : \mu_K R_{K^+}^\times] = \begin{cases} 1 & \text{if } n \text{ is a prime power,} \\ 2 & \text{otherwise.} \end{cases}$$

Proof. See [1, Theorem 4.12 and Corollary 4.13]. □

Next we consider the relation between the ideal class groups and class numbers of K^+ and K. There exists a canonical map $I(K^+) \to I(K)$ which sends a fractional ideal $A \in I(K^+)$ to the fractional ideal $A \cdot R_K \in I(K)$, i.e. to the fractional ideal of K generated by A. A principal fractional ideal of K^+ is mapped to a principal fractional ideal of K, hence we obtain an induced map of ideal class groups $\mathrm{Cl}(K^+) \to \mathrm{Cl}(K)$.

Theorem 10.4. *Let $K = \mathbb{Q}(\zeta_n)$ and $K^+ = \mathbb{Q}(\zeta_n)^+$ where $n > 1$ and $n \not\equiv 2 \pmod 4$. Then the canonical map $\mathrm{Cl}(K^+) \to \mathrm{Cl}(K)$ is injective. In particular the class number of K^+ divides the class number of K.*

Proof. See [1, Theorem 4.14]. □

11. Cyclotomic units

Let $n > 1$ be an integer which satisfies $n \not\equiv 2 \pmod 4$. Let $\zeta = \zeta_n = \exp(2\pi i/n)$. For an integer a which is prime to n we define

$$g_a = \frac{\zeta^a - 1}{\zeta - 1} \in \mathbb{Q}(\zeta).$$

Lemma 11.1. *For every $a \in \mathbb{Z}$ with $(a, n) = 1$, the element g_a is a unit in the ring of integers $R_{\mathbb{Q}(\zeta)}$.*

Proof. Let a' is any positive integer such that $a \equiv a' \pmod n$. Then

$$g_a = g_{a'} = \frac{\zeta^{a'} - 1}{\zeta - 1} = \zeta^{a'-1} + \zeta^{a'-2} + \cdots + \zeta + 1.$$

This shows that $g_a \in R_{\mathbb{Q}(\zeta)}$. Since $(a,n)=1$ there exists $b \in \mathbb{N}$ such that $ab \equiv 1 \pmod{n}$. Hence $\zeta = (\zeta^a)^b$ and so

$$g_a^{-1} = \frac{\zeta - 1}{\zeta^a - 1} = \frac{(\zeta^a)^b - 1}{\zeta^a - 1} = (\zeta^a)^{b-1} + (\zeta^a)^{b-2} + \cdots + \zeta^a + 1.$$

This shows that $g_a^{-1} \in R_{\mathbb{Q}(\zeta)}$. □

Next we construct units of the ring of integers of the maximal real subfield $\mathbb{Q}(\zeta)^+$. For $a \in \mathbb{Z}$ with $(a,n)=1$ we define

$$\xi_a = \zeta^{(1-a)/2} \frac{\zeta^a - 1}{\zeta - 1}.$$

Note that $\zeta^{(1-a)/2}$ lies in the field $\mathbb{Q}(\zeta)$ because if n is odd then $\zeta^{1/2} \in \mathbb{Q}(\zeta)$ and if n is divisible by 4 then the assumption $(a,n)=1$ implies that the exponent $(1-a)/2$ is even. Now $\zeta^{(1-a)/2} \in \mu_{\mathbb{Q}(\zeta)} \subseteq R_{\mathbb{Q}(\zeta)}^\times$ and $\frac{\zeta^a-1}{\zeta-1} \in R_{\mathbb{Q}(\zeta)}^\times$ by Lemma 11.1, thus ξ_a is a unit of $R_{\mathbb{Q}(\zeta)}$. Since

$$\begin{aligned}\overline{\xi_a} &= \zeta^{-(1-a)/2} \frac{\zeta^{-a} - 1}{\zeta^{-1} - 1} \\ &= \zeta^{-(1-a)/2} \frac{\zeta^{-a} \cdot (1 - \zeta^a)}{\zeta^{-1} \cdot (1 - \zeta)} \\ &= \xi_a\end{aligned}$$

it follows that ξ_a lies in the maximal real subfield $\mathbb{Q}(\zeta)^+$, hence $\xi_a \in R_{\mathbb{Q}(\zeta)^+}^\times$.

To simplify the presentation we now restrict to the case where $n = p$ is an odd prime number. We define the *group of cyclotomic units* of $\mathbb{Q}(\zeta_p)$ to be the subgroup of $R_{\mathbb{Q}(\zeta_p)}^\times$ generated by the roots of unity $\mu_{\mathbb{Q}(\zeta_p)}$ and by the units g_a for all $a \in \mathbb{Z}$ with $(a,p)=1$. We denote this group by C. We define the *group of cyclotomic units* of $\mathbb{Q}(\zeta_p)^+$ to be the subgroup of $R_{\mathbb{Q}(\zeta_p)^+}^\times$ generated by -1 and by the units ξ_a for all $a \in \mathbb{Z}$ with $(a,p)=1$. We denote this group by C^+.

Lemma 11.2. *Let p be an odd prime number. Then*

$$\frac{R_{\mathbb{Q}(\zeta_p)^+}^\times}{C^+} \cong \frac{R_{\mathbb{Q}(\zeta_p)}^\times}{C}.$$

For the proof of Lemma 11.2 we will need the following result.

Lemma 11.3. *The ideal $(1-\zeta_p)$ is a prime ideal of $R_{\mathbb{Q}(\zeta_p)}$ and $(1-\zeta_p)^{p-1} = (p)$.*

Proof of Lemma 11.3. The polynomial $X^p - 1$ has the roots ζ_p^a for $a = 0, 1, \ldots, p-1$, hence $X^p - 1 = \prod_{a=0}^{p-1}(X - \zeta_p^a)$. Dividing this equation by $X - \zeta_p^0$ gives

$$X^{p-1} + X^{p-2} + \cdots + X + 1 = \prod_{a=1}^{p-1}(X - \zeta_p^a).$$

Letting $X = 1$ shows that $p = \prod_{a=1}^{p-1}(1-\zeta_p^a)$. Now for every $a = 1, 2, \ldots, p-1$ we know from Lemma 11.1 that $1 - \zeta_p^a = \mathrm{unit} \cdot (1 - \zeta_p)$, therefore $p = \mathrm{unit} \cdot (1-\zeta_p)^{p-1}$. From this we obtain the equation of principal ideals $(p) = (1-\zeta_p)^{p-1}$ which proves the second statement of the lemma. Taking the norm of these ideals gives $p^{p-1} = \mathbf{N}\big((p)\big) = \mathbf{N}\big((1-\zeta_p)^{p-1}\big) = \mathbf{N}\big((1-\zeta_p)\big)^{p-1}$. Hence $\mathbf{N}\big((1-\zeta_p)\big) = p$ which implies that $(1-\zeta_p)$ is a prime ideal. □

Proof of Lemma 11.2. Let $f : R_{\mathbb{Q}(\zeta_p)^+}^\times \to R_{\mathbb{Q}(\zeta_p)}^\times / C$ be the canonical homomorphism. We will show that f is surjective and has kernel C^+.

First we show that $\ker(f) = C^+$. It is clear that $C^+ \subseteq \ker(f)$. Conversely let $\alpha \in R_{\mathbb{Q}(\zeta_p)^+}^\times$ be in the kernel of f. Then $\alpha \in C$, i.e. $\alpha = \varepsilon \cdot g_{a_1}^{\pm 1} g_{a_2}^{\pm 1} \cdots g_{a_r}^{\pm 1}$ for some $\varepsilon \in \mu_{\mathbb{Q}(\zeta_p)}$ and integers $a_1, a_2, \ldots, a_r$ which are prime to p. It follows that $\alpha = \varepsilon' \cdot \xi_{a_1}^{\pm 1}\xi_{a_2}^{\pm 1}\cdots\xi_{a_r}^{\pm 1}$ for some $\varepsilon' \in \mu_{\mathbb{Q}(\zeta_p)}$. Now $\alpha \in R_{\mathbb{Q}(\zeta_p)^+}^{\times}$ and $\xi_{a_1}^{\pm 1}\xi_{a_2}^{\pm 1}\cdots\xi_{a_r}^{\pm 1} \in R_{\mathbb{Q}(\zeta_p)^+}^{\times}$ implies that $\varepsilon' \in R_{\mathbb{Q}(\zeta_p)^+}^{\times}$, hence $\varepsilon' \in \{\pm 1\}$. This shows that $\alpha \in C^+$ as claimed.

Next we prove the surjectivity of f. Let $\alpha \in R_{\mathbb{Q}(\zeta_p)}^{\times}$. Define $\varepsilon \in R_{\mathbb{Q}(\zeta_p)}^{\times}$ by $\varepsilon = \alpha/\overline{\alpha}$. Then for every embedding $\sigma : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ we have $|\sigma(\varepsilon)| = |\sigma(\alpha)|/|\sigma(\overline{\alpha})| = 1$ because $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)}$ (compare the proof of Theorem 10.2.(2)). Now the same argument as in the proof of Lemma 6.8 shows that ε must have finite order, i.e. $\varepsilon \in \mu_{\mathbb{Q}(\zeta_p)}$. Hence $\varepsilon = \pm\zeta_p^a$ for some $a \in \mathbb{Z}$.

Suppose that $\alpha/\overline{\alpha} = \varepsilon = -\zeta_p^a$. Since $1, \zeta_p, \ldots, \zeta_p^{p-2}$ is an integral basis of $R_{\mathbb{Q}(\zeta_p)}$, we can write $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$. Modulo the ideal $(1-\zeta_p)$ we have $\zeta_p^i \equiv \zeta_p$ for all $i \in \mathbb{Z}$, hence

$$\begin{aligned}
\alpha &= a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{(p-2)} \\
&\equiv a_0 + a_1 + \cdots + a_{p-2} \\
&\equiv a_0 + a_1\zeta_p^{-1} + \cdots + a_{p-2}\zeta_p^{-(p-2)} \\
&= \overline{\alpha} \\
&= -\zeta_p^{-a}\alpha \\
&\equiv -\alpha.
\end{aligned}$$

So $2\alpha \equiv 0$ modulo $(1-\zeta_p)$, i.e. $2\alpha \in (1-\zeta_p)$. Since $(1-\zeta_p)$ is a prime ideal and $2 \notin (1-\zeta_p)$ (because otherwise $2^{p-1} \in (1-\zeta_p)^{p-1} = (p)$ and thus $p \mid 2^{p-1}$ which is impossible since p is odd) this implies $\alpha \in (1-\zeta_p)$. This is a contradiction because α is a unit and therefore cannot be contained in the prime ideal $(1-\zeta_p)$.

Hence $\alpha/\overline{\alpha} = \varepsilon = +\zeta_p^a$. Let $b \in \mathbb{Z}$ be such that $2b \equiv a \pmod{p}$. Let $\beta = \zeta_p^{-b}\alpha$. Then $\overline{\beta} = \zeta_p^b\overline{\alpha} = \beta$, i.e. $\beta \in R_{\mathbb{Q}(\zeta_p)^+}^{\times}$, and since $\zeta_p^{-b} \in C$ we have $f(\beta) = \alpha \cdot C \in R_{\mathbb{Q}(\zeta_p)}^{\times}/C$. This completes the proof of the surjectivity of f. □

Theorem 11.4. *Let p be an odd prime number. The cyclotomic units C^+ of $\mathbb{Q}(\zeta_p)^+$ have finite index in the full group of units $R_{\mathbb{Q}(\zeta_p)^+}^{\times}$, and*

$$[R_{\mathbb{Q}(\zeta_p)^+}^{\times} : C^+] = h_{\mathbb{Q}(\zeta_p)^+}$$

where $h_{\mathbb{Q}(\zeta_p)^+}$ is the class number of $\mathbb{Q}(\zeta_p)^+$.

Remark 11.5. One can define a group of cyclotomic units for any cyclotomic field $\mathbb{Q}(\zeta_n)$ and its maximal real subfield $\mathbb{Q}(\zeta_n)^+$, and suitable versions of Theorem 11.4 hold for all cyclotomic fields. See [1, §8.1].

Sketch of proof of Theorem 11.4. To simplify the notation we write $\zeta = \zeta_p$. Recall that $[\mathbb{Q}(\zeta)^+ : \mathbb{Q}] = (p-1)/2$ and $R_{\mathbb{Q}(\zeta)^+}^{\times} \cong \{\pm 1\} \times \mathbb{Z}^{(p-3)/2}$.

In §6 we defined a homomorphism $\lambda : R_{\mathbb{Q}(\zeta)^+}^{\times} \to \mathbb{R}^{(p-1)/2}$ by

$$\lambda(x) = \big(\log|\sigma_1(x)|, \ldots, \log|\sigma_{(p-1)/2}(x)|\big),$$

where $\sigma_1, \ldots, \sigma_{(p-1)/2} : \mathbb{Q}(\zeta)^+ \to \mathbb{R}$ are the embeddings of $\mathbb{Q}(\zeta)^+$. The kernel of λ is $\mu_{\mathbb{Q}(\zeta)^+} = \{\pm 1\}$ and the image is a free abelian group of rank $(p-3)/2$.

It is not difficult to see that λ induces an isomorphism

$$(1) \qquad \frac{R_{\mathbb{Q}(\zeta)^+}^{\times}}{C^+} \cong \frac{\lambda(R_{\mathbb{Q}(\zeta)^+}^{\times})}{\lambda(C^+)}.$$

Since C^+ is generated by ± 1 and $\xi_2, \xi_3, \ldots, \xi_{(p-1)/2}$, it follows that $\lambda(C^+)$ is generated by $\lambda(\xi_2), \lambda(\xi_3), \ldots, \lambda(\xi_{(p-1)/2})$.

We define the regulator $\mathrm{Reg}(\{\xi_a\})$ of the units $\xi_2, \xi_3, \ldots, \xi_{(p-1)/2}$ to be the absolute value of the determinant of any $(p-3)/2 \times (p-3)/2$-minor of the matrix with columns $\lambda(\xi_2), \ldots, \lambda(\xi_{(p-1)/2})$. We will show that

$$\mathrm{Reg}(\{\xi_a\}) = h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}. \tag{2}$$

Equation (2) implies that $\mathrm{Reg}(\{\xi_a\}) \neq 0$ and therefore that $\lambda(C^+)$ has rank $(p-3)/2$. This implies that $\lambda(C^+)$ has finite index in $\lambda(R^\times_{\mathbb{Q}(\zeta)^+})$. From the definitions of $\mathrm{Reg}_{\mathbb{Q}(\zeta)^+}$ and $\mathrm{Reg}(\{\xi_a\})$ it is not difficult to see that the index $[\lambda(R^\times_{\mathbb{Q}(\zeta)^+}) : \lambda(C^+)]$ can then be computed as a quotient of regulators

$$[\lambda(R^\times_{\mathbb{Q}(\zeta)^+}) : \lambda(C^+)] = \mathrm{Reg}(\{\xi_a\})/\mathrm{Reg}_{\mathbb{Q}(\zeta)^+}.$$

The isomorphism (1) and equation (2) imply that

$$[R^\times_{\mathbb{Q}(\zeta_p)^+} : C^+] = [\lambda(R^\times_{\mathbb{Q}(\zeta)^+}) : \lambda(C^+)] = h_{\mathbb{Q}(\zeta)^+}$$

which completes the proof of Theorem 11.4.

Let G be the group $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. We write $\hat{G}$ for the group of characters of G, i.e. the group of homomorphisms $G \to \mathbb{C}^\times$. If $\chi \in \hat{G}$ and $n \in \mathbb{N}$ is prime to p then (the coset of) n is an element of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\} = G$, thus $\chi(n)$ is defined. If $n \in \mathbb{N}$ is divisible by p then we define $\chi(n) = 0$. In this way we can consider χ as a function $\chi : \mathbb{N} \to \mathbb{C}$.

Lemma 11.6. *We have*

$$\mathrm{Reg}(\{\xi_a\}) = \pm \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} \frac{1}{2} \sum_{a=1}^{p-1} \chi(a) \log|1 - \zeta^a|.$$

Proof. This follows from a tricky computation of the determinant defining $\mathrm{Reg}(\{\xi_a\})$. See [1, Proof of Theorem 8.2]. □

Let $\chi \in \hat{G}$. We define the *Dirichlet L-function* $L(s, \chi)$ by

$$L(z, \chi) = \begin{cases} \sum_{n=1}^\infty \frac{\chi(n)}{n^z} & \text{if } \chi \neq 1, \\ \zeta(z) & \text{if } \chi = 1, \end{cases}$$

where $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$. Here $\zeta(z)$ is the Riemann zeta function. We define the *Gauss sum* $\tau(\chi)$ by

$$\tau(\chi) = \begin{cases} \sum_{a=1}^p \chi(a) \exp(2\pi i a/p) & \text{if } \chi \neq 1, \\ 1 & \text{if } \chi = 1. \end{cases}$$

The following theorem summarises the relevant properties of the Dirichlet L-functions and Gauss sums.

Theorem 11.7. (1) *Let $\zeta_{\mathbb{Q}(\zeta)^+}(z)$ be the Dedekind zeta function of $\mathbb{Q}(\zeta)^+$. Then*

$$\zeta_{\mathbb{Q}(\zeta)^+}(z) = \prod_{\chi \in \hat{G}} L(z, \chi).$$

(2) *If $\chi \in \hat{G} \setminus \{1\}$ then the series $L(z, \chi)$ converges at $z = 1$ and*

$$L(1, \chi) = -\frac{\tau(\chi)}{p} \sum_{a=1}^{p-1} \overline{\chi}(a) \log|1 - \zeta^a|.$$

(3) *We have*

$$\prod_{\chi \in \hat{G}} \tau(\chi) = \sqrt{|d_{\mathbb{Q}(\zeta)^+}|}$$

where $d_{\mathbb{Q}(\zeta)^+}$ is the discriminant of $\mathbb{Q}(\zeta)^+$.

(4) *If* $\chi \in \hat{G} \setminus \{1\}$ *then* $\tau(\chi)\tau(\overline{\chi}) = p$.

Proof. (1) See [1, Theorem 4.3].
(2) See [1, Theorem 4.9].
(3) See [1, Corollary 4.6].
(4) This follows from [1, Lemmas 4.7 and 4.8]. □

From Theorem 11.7.(1), the analytic class number formula (Theorem 9.4.(3)) and the fact that at $z = 1$ the Riemann zeta function has a simple pole with residue 1, we deduce that

$$\frac{2^{(p-1)/2} h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}}{2\sqrt{|d_{\mathbb{Q}(\zeta)^+}|}} = \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(1, \chi). \tag{3}$$

If $\chi \in \hat{G} \setminus \{1\}$ then by parts (2) and (4) of Theorem 11.7 we have

$$\sum_{a=1}^{p-1} \chi(a) \log|1 - \zeta^a| = -\frac{p}{\tau(\overline{\chi})} L(1, \overline{\chi}) = -\tau(\chi) L(1, \overline{\chi}). \tag{4}$$

Hence

$$\begin{aligned}
\mathrm{Reg}(\{\xi_a\}) &= \pm \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} \frac{1}{2} \sum_{a=1}^{p-1} \chi(a) \log|1 - \zeta^a| && \text{by Lemma 11.6} \\
&= \pm \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} \frac{-1}{2} \tau(\chi) L(1, \overline{\chi}) && \text{by (4)} \\
&= \pm 2^{-(p-3)/2} \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} \tau(\chi) \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} L(1, \overline{\chi}) \\
&= \pm 2^{-(p-3)/2} \sqrt{|d_{\mathbb{Q}(\zeta)^+}|} \frac{2^{(p-1)/2} h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}}{2\sqrt{|d_{\mathbb{Q}(\zeta)^+}|}} && \text{by (3) \& Th. 11.7.(3)} \\
&= \pm h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}.
\end{aligned}$$

Since $\mathrm{Reg}(\{\xi_a\})$ and $h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}$ are positive, it follows that

$$\mathrm{Reg}(\{\xi_a\}) = h_{\mathbb{Q}(\zeta)^+} \mathrm{Reg}_{\mathbb{Q}(\zeta)^+}$$

as required. □

References

[1] L.C. Washington, *Introduction to cyclotomic fields*, 2nd edition, Springer, 1997.