CHAPTER II
CARMICHAEL QUOTIENTS AND WILSON QUOTIENTS OVER THE RINGS OF INTEGERS OF NUMBER FIELDS

In the first section, we recall the notations and properties of the rings of integers of number fields and construct the Carmichael quotients and the Wilson quotients over this ring. Then we give the congruence relations of these quotients in Section 2.2.

2.1 Some definitions

A **number field** K is a finite extension of $\mathbb{Q}$ in $\mathbb{C}$ and an element $m \in K$ is called an **algebraic integer** if m is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of all algebraic integers in K is called the **ring of integers** of K, denoted by $\mathcal{O}_K$. It is well known that for any nonzero ideal I of $\mathcal{O}_K$, the cardinality of $\mathcal{O}_K/I$ is finite, see [8]. Then for a nonzero element $m \in \mathcal{O}_K$, the quotient ring $\mathcal{O}_K/m\mathcal{O}_K$ is finite.

Let $m, a \in \mathcal{O}_K \setminus \{0\}$ and m be a nonunit element. We say that a and m are relatively prime if $a\mathcal{O}_K + m\mathcal{O}_K = \mathcal{O}_K$, i.e., there exist $x, y \in \mathcal{O}_K$ such that $ax + my = 1$. In other words, $a + m\mathcal{O}_K \in (\mathcal{O}_K/m\mathcal{O}_K)^\times$. In [3], Bamunoba defined $\phi(m) = |(\mathcal{O}_K/m\mathcal{O}_K)^\times|$, so $a^{\phi(m)} + m\mathcal{O}_K = 1 + m\mathcal{O}_K$; that is, $a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$. Then he defined the **Euler quotient of** m **base** a as an element

$$E(a, m) = \frac{a^{\phi(m)} - 1}{m} \in \mathcal{O}_K.$$

He studied the congruence relations of these quotients based on the results of [1].

In his work, Bamunoba considered only $\mathcal{O}_K$ which are PIDs because he used the unique factorization property to confirm that his Euler quotients are well defined. However, we can use only the cancellative property of $\mathcal{O}_K$ to confirm that the quotients are well defined. So we can define the Euler quotients over arbitrary $\mathcal{O}_K$ but we may lose some results in [3].

Let $o(a + m\mathcal{O}_K)$ be the order of $a + m\mathcal{O}_K$ in $(\mathcal{O}_K/m\mathcal{O}_K)^\times$. We can define $\lambda(m) = \text{lcm}\ \{o(a + m\mathcal{O}_K) : a + m\mathcal{O}_K \in (\mathcal{O}_K/m\mathcal{O}_K)^\times\} = \exp((\mathcal{O}_K/m\mathcal{O}_K)^\times)$. Therefore, $a^{\lambda(m)} + m\mathcal{O}_K = 1 + m\mathcal{O}_K$; that is, $a^{\lambda(m)} \equiv 1 (\text{mod } m)$. Then we can define the **Carmichael quotient for** m **base** a as the element

$$C(a, m) = \frac{a^{\lambda(m)} - 1}{m} \in \mathcal{O}_K.$$

Next, we define the Wilson quotient for m. Let $\mathbb{A}_m$ be a set of all coset representatives of $\mathcal{O}_K/m\mathcal{O}_K$ and $\mathbb{A}_m^\times!$ be the product of all elements $r \in \mathbb{A}_m$ such that $r + m\mathcal{O}_K \in (\mathcal{O}_K/m\mathcal{O}_K)^\times$. From Proposition 1 in [5], we have that if $(\mathcal{O}_K/m\mathcal{O}_K)^\times$ has exactly one element of order two namely $b + m\mathcal{O}_K$, then $\mathbb{A}_m^\times! \equiv b (\text{mod } m)$, otherwise $\mathbb{A}_m^\times! \equiv 1 (\text{mod } m)$. Then we define $\epsilon_m = b$ when $b + m\mathcal{O}_K$ is the unique element of order two in $(\mathcal{O}_K/m\mathcal{O}_K)^\times$ and $b \in \mathbb{A}_m$, otherwise $\epsilon_m = 1$. Now, we have $\mathbb{A}_m^\times! \equiv \epsilon_m (\text{mod } m)$. So we get an element

$$W(m) := \frac{\mathbb{A}_m^\times! - \epsilon_m}{m} \in \mathcal{O}_K$$

which is called the **Wilson quotient for** m.

2.2 Some congruence relations

Let $m \in \mathcal{O}_K$ be a nonzero nonunit element and $\mathbb{A}_m$ be a set of all coset representatives of $\mathcal{O}_K/m\mathcal{O}_K$. Then for any $c \in \mathcal{O}_K$, $c + m\mathcal{O}_K = r + m\mathcal{O}_K$ for some unique $r \in \mathbb{A}_m$. Since $\mathcal{O}_K$ has no zero divisor, $c - r = hm$ for some unique $h \in \mathcal{O}_K$. Denote h by $\left[\frac{c}{m}\right]$ and it is called the quotient when m divides c.

Theorem 2.1. *Let $m \in \mathcal{O}_K$ be a nonzero nonunit element and $a \in \mathcal{O}_K$ relatively prime to m. Denote by $\langle a \rangle_m$ the subgroup of $(\mathcal{O}_K/m\mathcal{O}_K)^\times$ generated by $a + m\mathcal{O}_K$ and $o(a) = |\langle a \rangle_m|$. Then, we have*

$$C(a.m) \equiv \frac{\lambda(m)}{o(a)} \sum_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar} \left[\frac{ar}{m}\right] \pmod{m}$$

where $\left[\frac{ar}{m}\right]$ is the quotient when m divides ar.

Proof. For any element $r \in \mathbb{A}_m$ and $r + m\mathcal{O}_K \in \langle a \rangle_m$, there exists $c_r \in \mathbb{A}_m$ such that $ar \equiv c_r \pmod{m}$; that is, $ar - c_r = m\left[\frac{ar}{m}\right]$. Since $a + m\mathcal{O}_K$ and $r + m\mathcal{O}_K$ are in $\langle a \rangle_m$, $c_r + m\mathcal{O}_K$ are also in $\langle a \rangle_m$. Then when r runs through all elements r in $\mathbb{A}_m$ and $r + m\mathcal{O}_K \in \langle a \rangle_m$, so does c_r. Let $\mathcal{C}_r$ be the product of all elements c_r for all r. Then

$$\mathcal{C}_r^{\frac{\lambda(m)}{o(a)}} = \prod_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} c_r^{\frac{\lambda(m)}{o(a)}} = \prod_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \left(ar - m\left[\frac{ar}{m}\right]\right)^{\frac{\lambda(m)}{o(a)}}$$
$$= a^{\lambda(m)} \mathcal{C}_r^{\frac{\lambda(m)}{o(a)}} \prod_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \left(1 - \frac{m}{ar}\left[\frac{ar}{m}\right]\right)^{\frac{\lambda(m)}{o(a)}}.$$

Dividing it by $\mathcal{C}_r^{\frac{\lambda(m)}{o(a)}}$ yields

$$1 = a^{\lambda(m)} \prod_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \left(1 - \frac{m}{ar}\left[\frac{ar}{m}\right]\right)^{\frac{\lambda(m)}{o(a)}}$$
$$\equiv a^{\lambda(m)} \left(1 - \sum_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \frac{m}{ar}\left[\frac{ar}{m}\right]\right)^{\frac{\lambda(m)}{o(a)}} \pmod{m^2}$$
$$\equiv a^{\lambda(m)} \left(1 - m \sum_{\substack{r \in \mathbb{A}_m \\ r+m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar}\left[\frac{ar}{m}\right]\right)^{\frac{\lambda(m)}{o(a)}} \pmod{m^2}$$

$$1 \equiv a^{\lambda(m)} \left(1 - \frac{\lambda(m)}{o(a)} m \sum_{\substack{r \in \mathbb{A}_m \\ r + m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar} \left\lceil \frac{ar}{m} \right\rceil \right) \pmod{m^2}.$$

Now, we have

$$a^{\lambda(m)} - 1 \equiv a^{\lambda(m)} \frac{\lambda(m)}{o(a)} m \sum_{\substack{r \in \mathbb{A}_m \\ r + m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar} \left\lceil \frac{ar}{m} \right\rceil \pmod{m^2}.$$

Finally, by dividing this congruence by m, we get that

$$\begin{aligned} C(a, m) = \frac{a^{\lambda(m)} - 1}{m} &\equiv a^{\lambda(m)} \frac{\lambda(m)}{o(a)} \sum_{\substack{r \in \mathbb{A}_m \\ r + m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar} \left\lceil \frac{ar}{m} \right\rceil \pmod{m} \\ &\equiv \frac{\lambda(m)}{o(a)} \sum_{\substack{r \in \mathbb{A}_m \\ r + m\mathcal{O}_K \in \langle a \rangle_m}} \frac{1}{ar} \left\lceil \frac{ar}{m} \right\rceil \pmod{m} \end{aligned}$$

as desired. □

Theorem 2.2. *Let $m \in \mathcal{O}_K$ be a nonzero nonunit element. Then*

$$\sum_{\substack{a \in \mathbb{A}_m \\ a, m \text{ relatively prime}}} C(a, m) \equiv \epsilon_m \lambda(m) W(m) + C(\epsilon_m, m) \pmod{m}.$$

Proof. For each $a \in \mathbb{A}_m$ where a and m are relatively prime, we rewrite the Carmichael quotient for m base a as $a^{\lambda(m)} = 1 + m \cdot C(a, m)$. Then we have

$$\begin{aligned} (\mathbb{A}_m^\times !)^{\lambda(m)} = \prod_{\substack{a \in \mathbb{A}_m \\ a, m \text{ relatively prime}}} a^{\lambda(m)} &= \prod_{\substack{a \in \mathbb{A}_m \\ a, m \text{ relatively prime}}} (1 + mC(a, m)) \\ &\equiv 1 + m \sum_{\substack{a \in \mathbb{A}_m \\ a, m \text{ relatively prime}}} C(a, m) \pmod{m^2}. \end{aligned}$$

Next, we rewrite the Wilson quotient for m as $\mathbb{A}_m^\times ! = \epsilon_m + m \cdot W(m)$. We obtain

$$(\mathbb{A}_m^\times !)^{\lambda(m)} = (\epsilon_m + m \cdot W(m))^{\lambda(m)} \equiv \epsilon_m^{\lambda(m)} + \lambda(m) \epsilon_m^{\lambda(m)-1} m \cdot W(m) \pmod{m^2}.$$

Finally, we know that $\epsilon_m = \epsilon_m^{-1}$ in modulo m. Then

$$1 + m \sum_{\substack{a \in \mathbb{A}_m \\ a,m \text{ relatively prime}}} C(a,m) \equiv \epsilon_m^{\lambda(m)} + \epsilon_m^{\lambda(m)-1}\lambda(m)mW(m) \pmod{m^2}$$

$$m \sum_{\substack{a \in \mathbb{A}_m \\ a,m \text{ relatively prime}}} C(a,m) \equiv (\epsilon_m^{\lambda(m)} - 1) + \epsilon_m^{\lambda(m)-1}\lambda(m)mW(m) \pmod{m^2}$$

$$\sum_{\substack{a \in \mathbb{A}_m \\ a,m \text{ relatively prime}}} C(a,m) \equiv (\frac{\epsilon_m^{\lambda(m)} - 1}{m}) + \epsilon_m\lambda(m)W(m) \pmod{m}$$

$$\sum_{\substack{a \in \mathbb{A}_m \\ a,m \text{ relatively prime}}} C(a,m) \equiv C(\epsilon_m, m) + \epsilon_m\lambda(m)W(m) \pmod{m}.$$

This completes the proof. □