CHAPTER III
CARMICHAEL QUOTIENTS OVER POLYNOMIAL RINGS OVER FINITE LOCAL RINGS

For this chapter, we discuss the polynomial ring over a finite local ring and construct the Carmichael quotients over this ring in Section 3.1. Then we give the congruence relation of these quotients as in Section 2.2. Next, in Section 3.2, we consider $(R[x]/fR[x])^\times$ the unit group of the quotient ring of $R[x]$ modulo f in the case that f is a monic primary polynomial. Some special properties of this polynomial give more detail about a structure of $(R[x]/fR[x])^\times$. Importantly, this detail yields an idea to define the λ, dth power residue symbol. Finally, we use this symbol to define the Carmichael quotients of degree d and give relations of these quotients and the Euler quotients of degree d and the Wilson quotients defined in [6].

3.1 Carmichael quotients over polynomial rings over finite local rings

A **local ring** is a commutative ring with identity which has a unique maximal ideal. Let R be a finite local ring and M the unique maximal ideal. Let $\Bbbk := R/M$ and define the reduction map $\bar{\cdot} : R \to \Bbbk$ by letting $\alpha \in R$, $\overline{\alpha} = \alpha + M$. In addition, for a polynomial $h = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in R[x]$, we define $\overline{h} = \overline{\alpha_0} + \overline{\alpha_1} x + \ldots + \overline{\alpha_n} x^n \in \Bbbk[x]$ and we say that h is **regular** if its reduction $\overline{h} \in \Bbbk[x]$ is not the zero in $\Bbbk[x]$. Note that every monic polynomial in $R[x]$ is regular. Moreover, if h is regular then there exists a monic polynomial $h^* \in R[x]$ and a unit $u \in R[x]$ such that $uh = h^*$. This condition was shown in [9]. Then we may study only the monic polynomial in our work.

Let f be a monic non-constant polynomial in $R[x]$. Then we have the division algorithm for f stated that for any $h \in R[x]$, there exist unique $v, r \in R[x]$ where $\deg(r) < \deg(f)$ such that $h = v \cdot f + r$. Denote g by $\left[\frac{h}{f}\right]$ and it is called the quotient when f divide h.

Let $(R[x]/fR[x])^\times$ be the unit group of the quotient ring of $R[x]$ modulo f and $a \in R[x]$. We say that a and f are relatively prime if $aR[x] + fR[x] = R[x]$, i.e., there exist $g, h \in R[x]$ such that $ag + fh = 1$. That is, $a + fR[x] \in (R[x]/fR[x])^\times$. Let $o(a + fR[x])$ be the order of $a + fR[x]$ in $(R[x]/fR[x])^\times$. We define $\lambda(f) = \text{lcm}\ \{o(c + fR[x]) \mid c + fR[x] \in (R[x]/fR[x])^\times\} = \exp((R[x]/fR[x])^\times)$. Hence, $a^{\lambda(f)} + fR[x] = 1 + fR[x]$, i.e., $a^{\lambda(f)} \equiv 1 (\text{mod } f)$. Then we get the polynomial

$$C(a, f) = \frac{a^{\lambda(f)} - 1}{f}$$

which is called the **Carmichael quotient for f base a**. Note that this quotient is well-defined by the division algorithm of f.

Theorem 3.1. *Let $f \in R[x]$ be a monic non-constant polynomial and $a \in R[x]$ relatively prime to f. Denote $\langle a \rangle_f$ is the subgroup of $(R[x]/fR[x])^\times$ generated by $a + fR[x]$ and $o(a) = |\langle a \rangle_f|$. We have*

$$C(a, f) \equiv \frac{\lambda(f)}{o(a)} \sum_{\substack{\deg(r) < \deg(f) \\ r + fR[x] \in \langle a \rangle_f}} \frac{1}{ar} \left[\frac{ar}{f}\right] (\text{mod } f)$$

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

Proof. For any polynomial r with $\deg(r) < \deg(f)$ and $r + fR[x] \in \langle a \rangle_f$, there exists $c_r \in R[x]$ such that $ar \equiv c_r (\text{mod } f)$ and $\deg(c_r) < \deg(f)$; that is, $ar - c_r = \left[\frac{ar}{f}\right] f$. Since $a + fR[x], r + fR[x] \in \langle a \rangle_f$, we have $c_r + fR[x] \in \langle a \rangle_f$. Then when r runs through all the polynomials with $\deg(r) < \deg(f)$ and $r + fR[x] \in \langle a \rangle_f$, so does c_r. Let $\mathcal{C}_r$ be the product of all such polynomials c_r.

Then

$$C_r^{\frac{\lambda(f)}{o(a)}} = \prod_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} c_r^{\frac{\lambda(f)}{o(a)}} = \prod_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \left(ar - f\left[\frac{ar}{f}\right]\right)^{\frac{\lambda(f)}{o(a)}}$$

$$= a^{\lambda(f)} C_r^{\frac{\lambda(f)}{o(a)}} \prod_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \left(1 - \frac{f}{ar}\left[\frac{ar}{f}\right]\right)^{\frac{\lambda(f)}{o(a)}}.$$

Dividing it by $C_r^{\frac{\lambda(f)}{o(a)}}$ yields

$$1 = a^{\lambda(f)} \prod_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \left(1 - \frac{f}{ar}\left[\frac{ar}{f}\right]\right)^{\frac{\lambda(f)}{o(a)}}.$$

Next, we consider the previous equation in modulo f^2

$$1 \equiv a^{\lambda(f)} \left(1 - \sum_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \frac{f}{ar}\left[\frac{ar}{f}\right]\right)^{\frac{\lambda(f)}{o(a)}} \pmod{f^2}$$

$$\equiv a^{\lambda(f)} \left(1 - f\sum_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \frac{1}{ar}\left[\frac{ar}{f}\right]\right)^{\frac{\lambda(f)}{o(a)}} \pmod{f^2}$$

$$\equiv a^{\lambda(f)} \left(1 - \frac{\lambda(f)}{o(a)} f \sum_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \frac{1}{ar}\left[\frac{ar}{f}\right]\right) \pmod{f^2}.$$

Now, we have

$$a^{\lambda(f)} - 1 \equiv a^{\lambda(f)} \frac{\lambda(f)}{o(a)} f \sum_{\substack{\deg(r)<\deg(f)\\ r+fR[x]\in\langle a\rangle_f}} \frac{1}{ar}\left[\frac{ar}{f}\right] \pmod{f^2}.$$

Finally, divide this congruence by f, we get that

$$C(a,f) = \frac{a^{\lambda(f)}-1}{f} \equiv a^{\lambda(f)}\frac{\lambda(f)}{o(a)} \sum_{\substack{\deg(r)<\deg(f) \\ r+fR[x]\in\langle a\rangle_f}} \frac{1}{ar}\left[\frac{ar}{f}\right] \pmod{f}$$

$$\equiv \frac{\lambda(f)}{o(a)} \sum_{\substack{\deg(r)<\deg(f) \\ r+fR[x]\in\langle a\rangle_f}} \frac{1}{ar}\left[\frac{ar}{f}\right] \pmod{f}$$

as desired. □

Iamthong and Meemark [6] defined the Wilson quotients over polynomial rings over finite local rings as follows. For a monic non-constant polynomial f in $R[x]$, we let $\mathbb{A}_f^{\times}!$ be the product of the coset representatives of the group of unit $(R[x]/fR[x])^{\times}$, in other words, it is the product of all element in the set $\{a \in R[x] | a$ and f are relatively prime and $\deg(a) < \deg(f)\}$. We shall let $\epsilon_f = b$ if $b+fR[x]$ is the unique element of order two in $(R[x]/fR[x])^{\times}$ and $\deg(b) < \deg(f)$, and $\epsilon_f = 1$ otherwise, so that we have $\mathbb{A}_f^{\times}! \equiv \epsilon_f \pmod{f}$. Note that $b = -1$ if the characteristic of R is not equal to 2. This congruence gives the **Wilson quotient for** f as the polynomial

$$W(f) = \frac{\mathbb{A}_f^{\times}! - \epsilon_f}{f}.$$

Theorem 3.2. *Let $f \in R[x]$ be a monic non-constant polynomial. Assume that the characteristic of R is not equal to 2. Then*

$$\sum_{\substack{\deg(a)<\deg(f) \\ a,f \text{ relatively prime}}} C(a,f) \equiv \epsilon_f \lambda(f) W(f) \pmod{f}.$$

Proof. For each $a \in R[x]$ where a and f are relatively prime and $\deg(a) < \deg(f)$, we rewrite the Carmichael quotient for f base a as $a^{\lambda(f)} = 1 + f \cdot C(a,f)$. Then

we have

$$(\mathbb{A}_f^\times!)^{\lambda(f)} = \prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} a^{\lambda(f)} = \prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} (1 + fC(a,f))$$
$$\equiv 1 + f \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} C(a,f) \pmod{f^2}.$$

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

$$(\mathbb{A}_f^\times!)^{\lambda(f)} = (\epsilon_f + f \cdot W(f))^{\lambda(f)} \equiv \epsilon_f^{\lambda(f)} + \lambda(f)\epsilon_f^{\lambda(f)-1} f \cdot W(f) \pmod{f^2}$$
$$\equiv 1 + \epsilon_f^{\lambda(f)-1}\lambda(f) f W(f) \pmod{f^2}.$$

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

$$1 + f \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} C(a,f) \equiv 1 + \epsilon_f^{\lambda(f)-1}\lambda(f) f W(f) \pmod{f^2}$$
$$\sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} C(a,f) \equiv \epsilon_f \lambda(f) W(f) \pmod{f}.$$

This completes the proof. □

3.2 λ, dth power residue symbol

Let R be a finite local ring and M its unique maximal ideal. Let $\Bbbk := R/M$ and define the reduction map $\bar{\cdot} : R \to \Bbbk$ as in the last section. For this chapter, assume that $\Bbbk$ is a field of order $q = p^s$ where p is a prime number and $s \in \mathbb{N}$. By Theorem XVIII.2 in [9], we have that the unit group of R is isomorphic to the group $\Bbbk^\times \times (1 + M)$. Recall that $\Bbbk^\times$ is a cyclic group of order $q - 1 = p^s - 1$, so $\exp(\Bbbk^\times) = q - 1$. Moreover, $1 + M$ is a p-group which has p power elements then $\exp(1 + M) = p^e$ for some $e \in \mathbb{N}$. Since $p^s - 1$ and p^e are relatively prime, $\exp(R^\times) = \operatorname{lcm}\{\exp(\Bbbk^\times), \exp(1 + M)\} = \exp(\Bbbk^\times) \cdot \exp(1 + M)$.

A monic polynomial $f \in R[x]$ is **primary** if $\bar{f} = \pi^t$ for some monic irreducible polynomial π of degree n in $\mathbb{k}[x]$ and $t \in \mathbb{N}$. Let f be a monic primary polynomial. The special property of f is that its quotient ring $R[x]/fR[x]$ is a finite local ring with a unique maximal ideal $M_f = \langle M, \pi \rangle / fR[x]$ (for more detail, see [4]). Note that

$$(R[x]/fR[x])/(\langle M, \pi \rangle / fR[x]) \cong R[x]/\langle M, \pi \rangle \cong \mathbb{k}[x]/\langle \pi \rangle \cong \mathbb{k}_n$$

where $\mathbb{k}_n$ is a finite field of order q^n. After we have that $R[x]/fR[x]$ is a finte local ring, as in the last paragraph, we have $(R[x]/fR[x])^\times \cong \mathbb{k}_n^\times \times (1 + M_f)$ where $\mathbb{k}_n^\times$ is a cyclic group of order $q^n - 1$ and $1 + M_f$ is a $p-$group, so $\lambda(f) = \exp((R[x]/fR[x])^\times) = \exp(\mathbb{k}_n^\times) \cdot \exp(1 + M_f) = (q^n - 1) \cdot p^l$ for some $l \in \mathbb{N}$.

By the map $r \to r + fR[x]$ for an $r \in R^\times$, we can embed $R^\times$ into $(R/fR[x])^\times$. Now, we can consider $\mathbb{k}^\times$ which is a cyclic group of order $q - 1$ as a subgroup of $R^\times$ and so of $(R/fR[x])^\times$. For a divisor d of $q - 1$, $R^\times$ and $(R/fR[x])^\times$ have a unique cyclic subgroup of order d.

Lemma 3.3. *Let $f \in R[x]$ be a monic primary polynomial and $a \in R[x]$ relatively prime to f. For a divisor d of $q - 1$, there exists unique $\beta \in \mathbb{k}^\times$ (embedded in $R^\times$) such that $a^{\frac{\lambda(f)}{d}} \equiv \beta (\mathrm{mod}\ f)$.*

Proof. Since $(a^{\frac{\lambda(f)}{d}})^d + fR[x] = 1 + fR[x]$, the order of $a^{\frac{\lambda(f)}{d}} + fR[x]$ divides d. Since d is a divisor of $|\mathbb{k}^\times| = q - 1$ and $\mathbb{k}_n^\times$ is a cyclic group containing $\mathbb{k}^\times$, there exists a subgroup of $\mathbb{k}^\times$ of order d containing $a^{\frac{\lambda(f)}{d}} + fR[x]$. Therefore, there exists β in $\mathbb{k}^\times$ such that $a^{\frac{\lambda(f)}{d}} \equiv \beta (\mathrm{mod}\ f)$. Moreover, the division algorithm of f implies that β is unique. □

Let $f \in R[x]$ be a monic primary polynomial and $a \in R[x]$ relatively prime to f. For a divisor d of $q - 1$, define $\left(\frac{a}{f}\right)_{\lambda,d} = \beta$ where β is the unique element in $R^\times$ such that $a^{\frac{\lambda(f)}{d}} \equiv \beta (\mathrm{mod}\ f)$. We call this symbol that the **λ, dth power residue symbol of a modulo f**. In [6], Iamthong and Meemark defined **dth power residue symbol of a modulo f**, denoted by $\left(\frac{a}{f}\right)_d$, which is the unique α in $R^\times$ such that $a^{\frac{\phi(f)}{d}} \equiv \alpha (\mathrm{mod}\ f)$ where $\phi(f) = |(R[x]/fR[x])^\times|$. They also

had the **Euler quotient of degree** d **for** f **base** a as a polynomial

$$E_d(a,f) = \frac{a^{\frac{\phi(f)}{d}} - \left(\frac{a}{f}\right)_d}{f}.$$

Next, we find some relations between dth power residue symbol and $\lambda.d$th power residue symbol. Since $\lambda(f) \mid \phi(f)$, we obtain

$$\left(\frac{a}{f}\right)_d \equiv a^{\frac{\phi(f)}{d}} \equiv (a^{\frac{\lambda(f)}{d}})^{\frac{\phi(f)}{\lambda(f)}} \equiv \left(\frac{a}{f}\right)_{\lambda,d}^{\frac{\phi(f)}{\lambda(f)}} \pmod f \text{ and}$$
$$\left(\frac{a}{f}\right)_d \equiv a^{\frac{\phi(f)}{d}} \equiv (a^{\frac{\phi(f)}{\lambda(f)}})^{\frac{\lambda(f)}{d}} \equiv \left(\frac{a^{\frac{\phi(f)}{\lambda(f)}}}{f}\right)_{\lambda,d} \pmod f.$$

However, these two symbols lie in $R^\times$, so $\left(\frac{a}{f}\right)_d = \left(\frac{a}{f}\right)_{\lambda,d}^{\frac{\phi(f)}{\lambda(f)}} = \left(\frac{a^{\frac{\phi(f)}{\lambda(f)}}}{f}\right)_{\lambda,d}$.

Proposition 3.4. *Let $f \in R[x]$ be a monic primary polynomial and $r \in R[x]$ where r and f are relatively prime. We have that*

$$\left(\frac{r}{f}\right)_d = 1 \text{ if and only if } \left(\frac{r}{f}\right)_{\lambda,d} = 1.$$

Proof. We know that $\left(\frac{r}{f}\right)_d = \left(\frac{r}{f}\right)_{\lambda,d}^{\frac{\phi(f)}{\lambda(f)}}$, so the converse is obvious. Assume that $\left(\frac{r}{f}\right)_d = 1$. Note that $\frac{\phi(f)}{\lambda(f)} = \frac{(q^n-1)|1+M_f|}{(q^n-1)\lambda(1+M_f)} = \frac{|1+M_f|}{\lambda(1+M_f)}$. Since $|1+M_f|$ and $\lambda(1+M_f)$ are both power of p, there exists $g \in \mathbb{N} \cup \{0\}$ such that $\frac{\phi(f)}{\lambda(f)} = \frac{|1+M_f|}{\lambda(1+M_f)} = p^g$, so $\left(\frac{r}{f}\right)_d = \left(\frac{r}{f}\right)_{\lambda,d}^{p^g}$. Then $1 = \left(\frac{r}{f}\right)_{\lambda,d}^{p^g}$, so the order of $\left(\frac{r}{f}\right)_{\lambda,d}$ in the group $\Bbbk^\times$ divides p^g. However, $\Bbbk^\times$ is a cyclic group of order $q-1 = p^s - 1$ and $p^s - 1$ is relatively prime to p. Hence, $\left(\frac{r}{f}\right)_{\lambda,d} = 1$. □

3.3 Carmichael quotients of degree d

Let f be a monic primary polynomial in $R[x]$. We define the **Carmichael quotient of degree d for f base a** as a polynomial:

$$C_d(a,f) = \frac{a^{\frac{\lambda(f)}{d}} - \left(\frac{a}{f}\right)_{\lambda,d}}{f}.$$

Note that, in case $d = 1$, this quotient reduces to the Camichael quotient $C(a,f)$ as in section 3.1. Next, we consider the Euler quotient of degree d for f base a and we have

$$E_d(a,f) = \frac{a^{\frac{\phi(f)}{d}} - \left(\frac{a}{f}\right)_d}{f} = \frac{(a^{\frac{\phi(f)}{\lambda(f)}})^{\frac{\lambda(f)}{d}} - \left(\frac{a^{\frac{\phi(f)}{\lambda(f)}}}{f}\right)_d}{f} = C_d(a^{\frac{\phi(f)}{\lambda(f)}}, f).$$

We will complete this chapter with a congruence relation between the Carmichael quotients of degree d and the Wilson quotients.

Theorem 3.5. *Let $f \in R[x]$ be a monic primary polynomial. For any divisor d of $q-1$, we have*

$$\sum_{\substack{\deg(a)<\deg(f) \\ a,f \text{ relatively prime}}} \left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f) \equiv \frac{\lambda(f)}{d}\epsilon_f W(f) \pmod{f}.$$

Proof. For any $a \in R[x]$ with $\deg(a) < \deg(f)$ and a and f are relatively prime, we rewrite the Carmichael quotient of degree d for f base a as follows:

$$fC_d(a,f) + \left(\frac{a}{f}\right)_{\lambda,d} = a^{\frac{\lambda(f)}{d}}.$$

Then

$$(\mathbb{A}_f^\times!)^{\frac{\lambda(f)}{d}} = \prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} a^{\frac{\lambda(f)}{d}}$$

$$= \prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d} + fC_d(a,f)\right)$$

$$= \left(\prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\frac{a}{f}\right)_{\lambda,d}\right)\left(\prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(1+\left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} fC_d(a,f)\right)\right)\right).$$

Consider

$$\prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\frac{a}{f}\right)_{\lambda,d} \equiv \prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} a^{\frac{\lambda(f)}{d}} \pmod f$$

$$\equiv \left(\prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} a\right)^{\frac{\lambda(f)}{d}} \pmod f$$

$$\equiv (\mathbb{A}_f^\times!)^{\frac{\lambda(f)}{d}} \pmod f$$

$$\equiv \epsilon_f^{\frac{\lambda(f)}{d}} \pmod f.$$

By Lemma 3.3, both sides of this congruence lie in $R^\times$. This implies that they are equal. Then we have

$$(\mathbb{A}_f^\times!)^{\frac{\lambda(f)}{d}} = \epsilon_f^{\frac{\lambda(f)}{d}} \left(\prod_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(1+\left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} fC_d(a,f)\right)\right)\right)$$

Consider this equation in modulo f^2, we obtain

$$\begin{aligned}(\mathbb{A}_f^{\times}!)^{\frac{\lambda(f)}{d}} &\equiv \epsilon_f^{\frac{\lambda(f)}{d}} \left(1 + \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} f C_d(a,f)\right)\right) \pmod{f^2} \\ &\equiv \epsilon_f^{\frac{\lambda(f)}{d}} + \epsilon_f^{\frac{\lambda(f)}{d}} f \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \pmod{f^2}.\end{aligned}$$

Rewriting the Wilson quotient for f as $\langle f\rangle^{\times}! = \epsilon_f + f \cdot W(f)$ implies that

$$\begin{aligned}(\mathbb{A}_f^{\times}!)^{\frac{\lambda(f)}{d}} &= (\epsilon_f + fW(f))^{\frac{\lambda(f)}{d}} \\ &\equiv \epsilon_f^{\frac{\lambda(f)}{d}} + \frac{\lambda(f)}{d}\epsilon_f^{\frac{\lambda(f)}{d}-1} fW(f) \pmod{f^2}.\end{aligned}$$

Therefore,

$$\epsilon_f^{\frac{\lambda(f)}{d}} + \epsilon_f^{\frac{\lambda(f)}{d}} f \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \equiv \epsilon_f^{\frac{\lambda(f)}{d}} + \frac{\lambda(f)}{d}\epsilon_f^{\frac{\lambda(f)}{d}-1} fW(f) \pmod{f^2}$$

$$\epsilon_f^{\frac{\lambda(f)}{d}} f \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \equiv \frac{\lambda(f)}{d}\epsilon_f^{\frac{\lambda(f)}{d}-1} fW(f) \pmod{f^2}$$

$$\epsilon_f^{\frac{\lambda(f)}{d}} \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \equiv \frac{\lambda(f)}{d}\epsilon_f^{\frac{\lambda(f)}{d}-1} W(f) \pmod{f}.$$

Since $\epsilon_f = \epsilon^{-1}$ in modulo f, we have

$$\epsilon_f^{\frac{\lambda(f)}{d}} \sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \equiv \frac{\lambda(f)}{d}\epsilon_f^{\frac{\lambda(f)}{d}-1} W(f) \pmod{f}$$

$$\sum_{\substack{\deg(a)<\deg(f)\\ a,f \text{ relatively prime}}} \left(\left(\frac{a}{f}\right)_{\lambda,d}^{-1} C_d(a,f)\right) \equiv \frac{\lambda(f)}{d}\epsilon_f W(f) \pmod{f}$$

as desired. □