A PROOF OF WEIL'S BOUND ON GENERAL CHARACTER SUMS

MORITZ WINGER

Abstract. This bachelor thesis presents a proof of Weil's theorem on general character sums over a finite field. As an application, a bound on Kloosterman sums is deduced.

Key words and phrases. Character sums, Weil's Theorem.

The author acknowledges and expresses deep gratitude to Professor Richard Pink for the supervision of this thesis.

Contents

1. Weil's Theorem

The current work presents a proof of the Weil theorem on the bound on general character sums over a finite field $\mathbb{F}_q$. Suppose for the moment that q is prime. One example of such a character sum is the Kloosterman sum

$$\sum_{x\in\mathbb{F}_q^*} e(ax+bx^{-1}) \tag{1}$$

with $a, b \in \mathbb{F}_q$, where we denote $e(x) \coloneqq \exp(\frac{2\pi i}{q}x)$ and x^{-1} is the inverse of x in $\mathbb{F}_q$. An application that Kloosterman has derived from studying these sums is a theorem on the representations of large positive integers in the form $a_1x_1^2 + a_2y^2 + a_3z^2 + a_4t^2$ in [4]. In the proof of this theorem, a crucial building block was an estimate on Kloosterman sums.
This example elucidates the importance of general character sums over finite fields and their upper bounds, and shall be the motivation of this thesis: As well as proving Weil's theorem, we will show a direct application of Weil's theorem to deduce the Kloosterman bound

$$\left|\sum_{x\in\mathbb{F}_q^*} e(ax+bx^{-1})\right| \quad \leq \quad 2q^{1/2}. \tag{2}$$

The prerequisites to the understanding of this thesis are some basic knowledge on finite fields, classical algebraic geometry [2], algebraic number theory [5], L-series [5, 3], and characters [3].

Theorem 1.1 (Weil)**.** *Let q be a prime power and χ be a non-trivial multiplicative character of order d of $\mathbb{F}_q$. Let ψ a non-trivial additive character of $\mathbb{F}_q$. Let $m, n \geq 1$ and let f and g be polynomials in one variable over $\mathbb{F}_q$ with the following properties:*

- *(a) The polynomial f has m distinct roots in a fixed algebraic closure $\overline{\mathbb{F}_q}$.*
- *(b) The polynomial g is of degree n.*
- *(c) The polynomials $Y^d - f(X) \in \mathbb{F}_q[X][Y]$ and $Z^q - Z - g(X) \in \mathbb{F}_q[X][Z]$ are absolutely irreducible, i.e., irreducible over any algebraic closure of $\mathbb{F}_q$.*

Then,

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\psi(g(x))\right| \quad \leq \quad (m+n-1)\sqrt{q}. \tag{3}$$

The present work shows a proof for Theorem 1.1 following [6] and [3]. In the remainder of the current section we shall give an outline of the proof.

Fix $f, g \in \mathbb{F}_q[X]$ satisfying the conditions of Theorem 1.1. We first assume that f is a monic polynomial and g has zero constant term; restrictions which we will remove at the end of the proof.

Let $\mathbb{F}_{q^\nu}/\mathbb{F}_q$ be a field extension of degree ν. The norm $\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ and the trace $\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ from $\mathbb{F}_q^\nu$ to $\mathbb{F}_q$ are multiplicative, respectively additive characters [3] and therefore we find that the compositions $\chi_\nu \coloneqq \chi \circ \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ and $\psi_\nu \coloneqq \psi \circ \mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ are also multiplicative, respectively additive characters.

Definition 1.2.

$$S_{\chi\psi\nu} \coloneqq \sum_{x \in \mathbb{F}_{q^\nu}} \chi_\nu(f(x))\psi_\nu(g(x)) \tag{4}$$

In Chapter 3 we show that for all χ, ψ there exist complex numbers $\omega_{\chi\psi,1}, ..., \omega_{\chi\psi,m+n-1}$ such that for all ν

$$S_{\chi\psi\nu} = -(\omega_{\chi\psi,1}^\nu + ... + \omega_{\chi\psi,m+n-1}^\nu). \tag{5}$$

Further, we find that for the trivial characters χ_0 and ψ_0 the sum $S_{\chi_0\psi_0\nu}$ evaluates to q^ν.

Definition 1.3. $N_\nu \coloneqq \left|\{(x, y, z) \in \mathbb{F}_{q^\nu}^3 : y^d = f(x), \quad z^q - z = g(x)\}\right|$

It turns out that N_ν is related to $S_{\chi\psi\nu}$ via the formula

$$N_\nu = \sum_{\substack{\chi \\ \text{of exponent } d}} \sum_{\psi} S_{\chi\psi\nu} \tag{6}$$

a result which will be derived in Chapter 2.

Theorem 1.4. *Suppose $f \in \mathbb{F}_q[X, Y]$ is absolutely irreducible and of total degree $d > 0$. Let N be the number of zeros of f in $\mathbb{F}_q^2$. If $q > 250d^5$, then*

$$|N - q| < \sqrt{2}d^{5/2}q^{1/2}. \tag{7}$$

Proof. This follows from the Riemann hypothesis for curves over finite fields, which is proved in [7] and [1]. □

In Chapter 4, using the bound

$$|N_\nu - q^\nu| < O(q^{\nu/2}) \tag{8}$$

derived from Theorem 1.4, we will deduce

$$|S_\nu| \leq (m+n-1)q^{\nu/2} \tag{9}$$

and in particular

$$|S| \leq (m+n-1)\sqrt{q} \tag{10}$$

which proves Theorem 1.1.

As an application, we will apply Weil's theorem to deduce an upper bound on Kloosterman sums in Chapter 5.

2. Relating character sums to the numbers of solutions of polynomials

Let χ, ψ, χ_ν and ψ_ν as above. Let χ_0 be the trivial multiplicative character and ψ_0 the trivial additive character.

We shall first study multiplicative character sums: Suppose that the polynomial $f(x)$ satisfies the conditions of Theorem 1.1 and is monic. Let

$$S_{\chi,\nu} \coloneqq \sum_{x \in \mathbb{F}_{q^\nu}} \chi_\nu(f(x)). \tag{11}$$

We note that

$$S_{\chi_0,\nu} = q^\nu. \tag{12}$$

Lemma 2.1 (Orthogonality Relation)**.** *Let G be a finite abelian group and θ_0 be the trivial character $G \to \mathbb{C}^*$.*

(a) For any character $\theta : G \to \mathbb{C}^*$

$$\sum_{x \in G} \theta(x) = \begin{cases} |G| & \text{if } \theta = \theta_0, \\ 0 & \text{if } \theta \neq \theta_0. \end{cases} \tag{13}$$

(b) For any $x \in G$

$$\sum_{\theta \in \hat{G}} \theta(x) = \begin{cases} |G| & \text{if } x = 1, \\ 0 & \text{if } x \neq 1, \end{cases} \tag{14}$$

where $\hat{G}$ is the dual group of characters of the group G.

Proof. (a) If $\theta = \theta_0$, then

$$\sum_{x\in G} \theta_0(x) = \sum_{x\in G} 1 = |G| \tag{15}$$

If $\theta \neq \theta_0$, then there exists $y \in G$ such that $\theta(y) \neq 1$. As x runs through G in the summation, so does yx. Hence,

$$\sum_{x\in G} \theta(x) = \sum_{x\in G} \theta(yx) = \theta(y) \sum_{x\in G} \theta(x). \tag{16}$$

Since we have assumed that $\theta(y) \neq 1$, it must be true that

$$\sum_{x\in G} \theta(x) = 0. \tag{17}$$

The proof of (b) is analogous to that of (a). □

Let d be an integer dividing $q - 1$.

Lemma 2.2. *For any given $w \in \mathbb{F}_{q^\nu}$, the number of $y \in \mathbb{F}_{q^\nu}$ with $y^d = w$ equals*

$$\sum_{\chi_\nu^d=1} \chi_\nu(w) = \sum_{\chi^d=1} \chi(\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(w)) \tag{18}$$

Proof. The characters of exponent d are precisely those which are trivial on the subgroup $(\mathbb{F}_{q^\nu}^*)^d := \{w^d \mid w \in \mathbb{F}_{q^\nu}^*\}$. Therefore, we may view them as characters on the factor group $\mathbb{F}_{q^\nu}^*/(\mathbb{F}_{q^\nu}^*)^d$. The orthogonality relation in Lemma 2.1 (b) becomes

$$\sum_{\chi_\nu^d=1} \chi_\nu(w) = \begin{cases} [\mathbb{F}_{q^\nu}^* : (\mathbb{F}_{q^\nu}^*)^d] & \text{if } w \in (\mathbb{F}_{q^\nu}^*)^d, \\ 0 & \text{otherwise.} \end{cases} \tag{19}$$

The characters of $\mathbb{F}_{q^\nu}^*/(\mathbb{F}_{q^\nu}^*)^d$ correspond to the characters of $\mathbb{F}_{q^\nu}^*$ which are of order dividing d by the composition

$$\mathbb{F}_{q^\nu}^* \to \mathbb{F}_{q^\nu}^*/(\mathbb{F}_{q^\nu}^*)^d \to \mathbb{C}^*. \tag{20}$$

and since x is trivial in $\mathbb{F}_{q^\nu}^*/(\mathbb{F}_{q^\nu}^*)^d$ if and only if $w = y^d$. Therefore, setting $\chi_\nu(0) = 0$ if χ_ν is non-trivial and $\chi_\nu(0) = 1$ if χ_ν is trivial, we get that

$$\sum_{\chi_\nu^d=1} \chi_\nu(w) = \begin{cases} d & \text{if } w = y^d \text{ for some } y \in \mathbb{F}_{q^\nu}^* \\ 0 & \text{otherwise} \end{cases} \tag{21}$$

and hence

$$\sum_{\chi_\nu^d=1} \chi_\nu(w) = |\{y \in \mathbb{F}_{q^\nu} | y^d = w\}|. \tag{22}$$

□

We shall now look at additive character sums. Suppose that $g(x)$ satisfies the conditions given by Theorem 1.1.We define

$$S_{\psi,\nu} \coloneqq \sum_{x \in \mathbb{F}_{q^\nu}} \psi_\nu(g(x)). \tag{23}$$

It follows that

$$S_{\psi_0,\nu} = q^\nu. \tag{24}$$

Lemma 2.3. *For any $y \in \mathbb{F}_{q^\nu}$ we have*

$$|\{x \in \mathbb{F}_{q^\nu} | x^q - x = y\}| = \begin{cases} q & \text{if } \mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(y) = 0 \\ 0 & \text{if } \mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(y) \neq 0 \end{cases} \tag{25}$$

Proof. Let $\alpha \in \mathbb{F}_{q^\nu}$. Considering the Frobenius map $\sigma : \alpha \to \alpha^q$ we clearly have $\sigma^\nu(\alpha) = \alpha$. The kernel of the map

$$\begin{aligned} \delta &\colon \mathbb{F}_{q^\nu} \to \mathbb{F}_{q^\nu} \\ x &\mapsto x^q - x = \sigma(x) - x \end{aligned}$$

is $\mathbb{F}_q$ because the Frobenius automorphism only fixes the field $\mathbb{F}_q$. Hence, $|\operatorname{Im}(\delta)| = q^{\nu-1}$. Further, $\operatorname{Im}(\delta) \subset \operatorname{Ker}(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q})$ since for all $x \in \mathbb{F}_{q^\nu}$ we have

$$\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(\delta(x)) = \mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(\sigma(x) - x) = \sum_{i=0}^{\nu=1} \sigma^{i+1} - \sigma^i(x) = \sigma^n(x) - x = 0. \tag{26}$$

However, since $\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ is a polynomial of degree $q^{\nu-1}$, it cannot vanish at more than $q^{\nu-1}$ points and hence $\operatorname{Im}(\delta) = \operatorname{Ker}(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q})$ and the result follows, since the equation has no solution if $y \notin \operatorname{Ker}(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q})$ and q solutions otherwise. □

Lemma 2.4. *For any given $w \in \mathbb{F}_{q^\nu}$, the number of $z \in \mathbb{F}_{q^\nu}$ with $z^q - z = w$ equals*

$$\sum_{\psi_\nu} \psi_\nu(w) = \sum_{\psi} \psi(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(w)) \tag{27}$$

Proof. By Lemma 2.3, if $\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(w) = 0$, then we have q solutions of $z^q - z = w$ and by the orthogonality relation from Lemma 2.1 our sum (27) equals q. If $\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(w) \neq 0$, then there are no solutions by Lemma 2.3 and the sum is zero by Lemma 2.1 again. □

Lemma 2.5. *The number N_ν of $(x,y,z) \in \mathbb{F}_{q^\nu}^3$ with $y^d = f(x)$ and $z^q - z = g(x)$ is*

$$N_\nu = \sum_{\chi_\nu^d = 1} \sum_{\psi} S_{\chi\psi\nu}. \tag{28}$$

Proof. Combining Lemmas 2.2 and 2.4 we write

$$\begin{aligned} N_\nu &= \left|\{(x,y,z) \in \mathbb{F}_{q^\nu}^3 : y^d = f(x), \quad z^q - z = g(x)\}\right| \\ &= \sum_{x \in \mathbb{F}_{q^\nu}} |\{y \in \mathbb{F}_{q^\nu} : y^d = f(x)\}| \cdot |\{z \in \mathbb{F}_{q^\nu} : z^q - z = g(x)| \\ &= \sum_{x \in \mathbb{F}_{q^\nu}} \left(\sum_{\chi_\nu^d = 1} \chi_\nu(f(x)) \right) \left(\sum_{\psi_\nu \neq \psi_0} \psi_\nu(g(x)) \right) \qquad (29) \\ &= \sum_{\chi_\nu^d = 1} \sum_{\psi_\nu \neq \psi_0} \sum_{x \in \mathbb{F}_{q^\nu}} \chi_\nu(f(x)) \psi_\nu(g(x)) \\ &= \sum_{\chi_\nu^d = 1} \sum_{\psi_\nu \neq \psi_0} S_{\chi\psi\nu}. \end{aligned}$$

□

Additionally, Equations (12) and (24) yield

$$S_{\chi_0\psi_0\nu} = q^\nu. \tag{30}$$

3. Writing character sums as sums of complex numbers

Fix $f \in \mathbb{F}_q[X]$ monic with m distinct roots over $\overline{\mathbb{F}_q}$, a fixed algebraic closure of $\mathbb{F}_q$. In $\overline{\mathbb{F}_q}[X]$ we have

$$f(x) = \prod_{i=1}^{m} (x + \gamma_i)^{a_i} \tag{31}$$

with distinct $\gamma_1, ..., \gamma_m$.

Let G_ν be the multiplicative group of rational functions $r(x) = \frac{h_1(x)}{h_2(x)}$ with $h_2(x) \neq 0$ and $h_i(x) \in \mathbb{F}_{q^\nu}[X]$ monic. We define $G'_\nu \leq G_\nu$ as the subgroup consisting of rational functions

with $h_1(\gamma_i)h_2(\gamma_i) \neq 0$ for all $i \in \{1, ..., m\}$. For $r(x) \in G'_\nu$, we define

$$\{r\} \coloneqq \prod_{i=1}^{m} r(\gamma_i)^{a_i}. \tag{32}$$

Proposition 3.1. $\{r\}$ is an element of $\mathbb{F}^*_{q^\nu}$.

Proof. It is easily seen that $\{r\}$ is an algebraic element. To show that $\{r\} \in \mathbb{F}_{q^\nu}$ it suffices to show that $\sigma(\{r\}) = \{r\}$ for every automorphism σ of the splitting field of $f(X)$. Such automorphisms, however, simply permute the roots γ_i of $f(X)$ and therefore permute the factors of $\{r\}$ and the result follows. □

Lemma 3.2. *The character $G'_\nu \to \mathbb{C}^*, r \mapsto \chi_\nu(\{r\})$ is multiplicative.*

Proof. Let $r_1(x)$ and $r_1(x)$ be elements of G'_ν. Then,

$$\begin{aligned} \chi_\nu(\{r_1\}\{r_2\}) &= \chi \circ \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(\{r_1\}\{r_2\}) \\ &= \chi \circ \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(\{r_1\})\chi \circ \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(\{r_2\}) \\ &= \chi_\nu(\{r_1\})X_\nu(\{r_2\}) \end{aligned} \tag{33}$$

using the fact that $\chi_\nu = \chi \circ \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}$ is a multiplicative character. □

Further, we define $H''_\nu \leq G'_\nu$ as the subgroup consisting of $r(x) = \frac{h_1(x)}{h_2(x)}$ with $h_1(\gamma_i) = h_2(\gamma_i) \neq 0$ for all $i \in \{1, ..., m\}$.

Lemma 3.3. *For all $r \in H''_\nu$ we have*

$$\chi_\nu(\{r\}) = 1. \tag{34}$$

Proof. The result follows from Lemma 3.2 and the definition of H''_ν. □

We now proceed similarly with the additive character ψ_ν: Fix a polynomial $g \in \mathbb{F}_{q^\nu}[X]$ of degree n with constant term zero. Let $r \coloneqq r(x) \in G_\nu$. Define

$$[r] \coloneqq g(\alpha_1) + \ldots + g(\alpha_u) - g(\beta_1) - \ldots - g(\beta_v) \quad \text{if } r = \frac{\prod_{i=1}^{u}(X + \alpha_i)}{\prod_{j=1}^{v}(X + \beta_j)} \tag{35}$$

with $\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v \in \overline{\mathbb{F}_q}$.

Proposition 3.4. $[r]$ is an element of $\mathbb{F}_{q^\nu}$.

Proof. The automorphisms σ of the splitting field of $g(X)$ permute the roots α_i of $\prod_{i=1}^{u}(X+\alpha_i)$ and β_i of $\prod_{j=1}^{v}(X+\beta_j)$. Therefore $\sigma([r])=[r]$ for all σ. □

Lemma 3.5. *The character $G_\nu \to \mathbb{C}^*, r \mapsto \psi_\nu([r])$ is additive.*

Proof. We observe that $[r] \in \mathbb{F}_{q^\nu}$ and $[r_1 r_2] = [r_1] + [r_2]$. Therefore, since ψ_ν is an additive character, $\psi_\nu([r_1 r_2]) = \psi_\nu([r_1]) + \psi_\nu([r_2])$. □

Let $u, v \geq n$. We define $H'_\nu \subset G_\nu$ as the subset of elements $r(x) = \frac{h_1(x)}{h_2(x)}$ with $h_1(x) = x^u + a_1 x^{u-1} + \ldots + a_u$ and $h_2(x) = x^v + b_1 x^{v-1} + \ldots + b_v$ where $a_1 = b_1, \ldots, a_n = b_n$. For example, the polynomials x^u lie in H'_ν, as well as the polynomials $x^u + a_{n+1}x^{u-n-1} + \ldots + a_u$ with $u > n$.

Proposition 3.6. The subset H'_ν is a subgroup of G_ν.

Proof. It can easily be seen that the inverse and 1 lie in H'_ν. Let $h_1 = \frac{p}{q}$ and $h_2 = \frac{p'}{q'}$ be elements of H'_ν with

$$p = x^u + a_1 x^{u-1} + \ldots + a_u, \quad q = x^v + b_1 x^{v-1} + \ldots + b_v \tag{36}$$

and

$$p' = x^w + c_1 x^{w-1} + \ldots + c_w, \quad q' = x^r + d_1 x^{r-1} + \ldots + d_r \tag{37}$$

Then the coefficient of x^ℓ in $h_1 h_2$ is $\sum_{i+j=\ell} a_i c_j$ in the numerator and $\sum_{i+j=\ell} b_i d_j$ in the denominator. Since $a_i = b_i$ and $c_j = d_j$ for all $i, j \in \{1, \ldots, n\}$, we have that $h_1 h_2 \in H'_\nu$. □

Lemma 3.7. *If $r \in H'_\nu$, then $\psi_\nu([r]) = 1$.*

Proof. The function $g(\alpha_1) + \ldots + g(\alpha_u)$ viewed as a polynomial in $\mathbb{F}_{q^\nu}[\alpha_1, \ldots, \alpha_u]$ is a symmetric polynomial of degree n. Therefore it is a polynomial in the first n elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_u$, which means it is also a polynomial in the coefficients $a_1, \ldots, a_n$ of $h_1(x)$. We can write $g(\alpha_1) + \ldots + g(\alpha_u) = l_1(a_1, \ldots, a_n)$. Similarly, we get $g(\beta_1) + \ldots + g(\beta_u) = l_2(b_1, \ldots, b_n)$. Recalling that g has constant term zero and that by definition of H'_ν, we have $a_i = b_i$ for all $1 \leq i \leq n$, we get that $l_1 = l_2$. Hence, $[r] = 0$ and therefore $\psi([r]) = 1$. □

We now define the subgroup $H_\nu \coloneqq H'_\nu \cap H''_\nu$.

Proposition 3.8. Suppose that $\ell \geq 0$. Then every coset of H_ν in G'_ν contains precisely q^ℓ polynomials of degree $n+m+\ell$.

Proof. Let $r(x) \in G'_\nu$. We need to show that there are precisely q^ℓ polynomials $k(x) = x^{n+m+\ell} + b_1 x^{n+m+\ell-1} + ... + b_{n+m+\ell}$ with $k(x)/r(x) \in H_\nu$. If $k(x)/r(x) \in H_\nu$ and if $r(x)$ has the expansion $r(x) = x^u + a_1 x^{u-1} + ...$, then

$$b_1 = a_1, \ldots, b_n = a_n \tag{38}$$

and

$$k(\gamma_i) = r(\gamma_i) \ \ \forall i \in \{1, \ldots, m\}. \tag{39}$$

Hence, the coefficients $b_1, ..., b_n$ are determined by Equation (38). Picking arbitrary values for $b_{n+1}, ..., b_{n+\ell}$, the equations (39) form a non-homogeneous linear system of equations in the m remaining coefficients $b_{n+\ell+1}, \ldots, b_{n+\ell+m}$. The corresponding matrix to this system is the Vandermonde matrix in γ_i and, since $\gamma_1, \ldots, \gamma_m$ are distinct, its determinant is non-zero. Hence, the system in Equation (39) can be solved uniquely and the freedom of choice consists of picking $b_{n+1}, ..., b_{n+\ell}$, which gives q^ℓ possibilities. □

Proposition 3.9. Suppose that the polynomial $Y^d - f(X)$ has coefficients in a field K. Then, if $Y^d - cf(X)$ is absolutely irreducible for every c with $c \in K \setminus \{0\}$ it follows that if $f(X) = a(X - x_1)^{d_1} \cdots (X - x_s)^{d_s}$ is the factorisation of f in any algebraic closure $\overline{K}$ with $x_i \neq x_j$ for $i \neq j$, then $(d, d_1, \ldots, d_s) = 1$.

Proof. Suppose $t \coloneqq (d, d_1, \ldots . d_s) > 1$. Then, by putting

$$g(X) \coloneqq (X - x_1)^{d_1/t} \ldots (X - x_s)^{d_s/t} \tag{40}$$

we get that

$$Y^d - \frac{1}{a} f(X) = Y^d - g(X)^d = (Y^{a/t} - g(X))(Y^{\frac{d}{t}(t-1)} + Y^{\frac{d}{t}(t-2)} g(X) + \ldots + g(X)^{t-1}) \tag{41}$$

which shows that $Y^d - \frac{1}{a} f(X)$ is reducible over $\overline{K}$, which is a contradiction. □

Definition 3.10. We define the character $X_\nu(r) \coloneqq \chi_\nu(\{r\})\psi_\nu([r])$ from G'_ν to $\mathbb{C}^*$.

Proposition 3.11. (a) The character X_ν is a character on the group G'_ν and on the subgroup $H_\nu \coloneqq H'_\nu \cap H''_\nu$ we have $X_\nu(r) = 1$.

(b) Suppose that $\chi \neq \chi_0$ is of exponent d and $Y^d - f(X)$ is absolutely irreducible, or $\psi \neq \psi_0$ and $Z^q - Z - g(X)$ is irreducible. Then, the character X_ν is not principal, *i.e.*, $X_\nu(k) \neq 1$ for some $k \in G'_\nu$.

(c) Suppose the conditions of (b) hold and $\ell \geq 0$. Then,

$$\sum_{\substack{h \in G'_\nu \\ h \text{ monic} \\ \deg(h)=n+m+\ell}} X_\nu(h) = 0. \tag{42}$$

Proof. (a) The equality $X_\nu(r) = 1$ follows immediately from the definition of the subgroup H_ν and the properties of χ_ν and ψ_ν on H_ν.
(b) Suppose $X_\nu(k) = 1$. Because $\chi_\nu(\{k\})$ is a d^{th} root of unity and $\psi_\nu([k])$ is a p^{th} root of unity where $(d, p) = 1$ and with $X_\nu(k) = \chi_\nu(\{k\})\psi_\nu([k])$, we have

$$\chi_\nu(\{k\}) = \psi_\nu([k]) = 1. \tag{43}$$

Therefore it suffices to find a k with $\chi_\nu(\{k\}) \neq 1$ for the first case and a k where $\psi_\nu([k]) \neq 1$ for the second case.

Assume that χ_ν is non-trivial of order e with $e|d$. Since $Y^d - f(X)$ is absolutely irreducible, not all the exponents in

$$f(X) = (X + \gamma_1)^{a_1} \cdots (X + \gamma_m)^{a_m} \tag{44}$$

are multiples of e by Proposition 3.9. Say, e does not divide a_1. Given $c_2, \ldots, c_m \in \mathbb{F}_q^*$, we can pick $c_1 \in \mathbb{F}_q^*$ with $c_1^{a_1} \cdots c_m^{a_m} \notin (\mathbb{F}_q^*)^e$ and therefore with $\chi_\nu(c_1^{a_1} \ldots c_m^{a_m}) \neq 1$. By the argument of Proposition 3.8, there exists a polynomial $k(X) \in G'_\nu$ with

$$k(\gamma_i) = c_i \qquad (i = 1, \ldots, m). \tag{45}$$

Then, $\{k\} = c_1^{a_1} \cdots c_m^{a_m}$ and $\chi_\nu(\{k\}) \neq 1$.

For the second case, considering a fixed non-trivial additive character ψ_ν, let $Z^q - Z - g(X)$ be absolutely irreducible. Denoting by $\mathrm{Tr}, \mathrm{Tr}_\nu, \mathrm{Tr}'_\nu$ the trace homomorphisms $\mathbb{F}_q \to \mathbb{F}_p$, $\mathbb{F}_{q^\nu} \to \mathbb{F}_q$, $\mathbb{F}_{q^\nu} \to \mathbb{F}_p$, respectively, the character ψ_ν is of the type

$$\psi_\nu(z) = e(\mathrm{Tr}(az)/p) \tag{46}$$

where $e(x) \coloneqq \exp(\frac{2\pi i}{p}x)$ and for some $a \in \mathbb{F}_q^*$. The polynomial $Z^q - Z - ag(X) = a\left((\frac{Z}{a})^q - (\frac{Z}{a}) - g(X)\right)$ is absolutely irreducible as well. Hence, the polynomial

$$Z^p - Z - ag(x) \tag{47}$$

is absolutely irreducible, where p is the characteristic. This is true because if $q = p^\nu$, then $Z^q - Z = u(Z)^p - u(Z)$ with $u(Z) = Z^{p^{\nu-1}} + \ldots + Z^p + Z$. Given $x \in \mathbb{F}_{q^\nu}$, if $\mathrm{Tr}'_\nu(x) = 0$, by Lemma 2.3, there are p values of $z \in \mathbb{F}_{q^\nu}$ with $z^p - z - ag(x) = 0$. If $\mathrm{Tr}'_\nu(x) \neq 0$, there are no such z. By Theorem 1.4 we have that $N_\nu < pq^\nu$ for large enough ν. Therefore, there will be some $x \in \mathbb{F}_{q^\nu}$ with $\mathrm{Tr}'_\nu(ag(x)) \neq 0$. Let $k(X) = (X + x_1)\cdots(X + x_\nu) \in \mathbb{F}_q[X]$, where $x = x_1, \ldots, x_\nu$ are the conjugates of x over $\mathbb{F}_q$. Then $[k] = g(x_1) + \ldots + g(x_\nu) = \mathrm{Tr}_\nu(x)$ and

$$\begin{aligned} \psi([k]) &= e(\mathrm{Tr}(a\,\mathrm{Tr}_\nu(g(x)))/p) \\ &= e(\mathrm{Tr}(\mathrm{Tr}_\nu)(ag(x))/p) \\ &= e(\mathrm{Tr}'_\nu(ag(x))/p) \neq 1. \end{aligned} \tag{48}$$

By the freedom of choice of x, one may ensure that $k \in G'_\nu$.
(c) By (a) and (b), the character X_ν induces a non-principal character on the finite factor group G'_ν/H_ν. By Proposition 3.8, the polynomial h will lie precisely q^ℓ times in every given coset of G'_ν/H_ν. Then the result follows from the orthogonality property of characters χ on finite abelian groups G, namely that $\sum_{x\in G}\chi(x) = 0$ if χ is nontrivial (see Theorem 2.1). □

We shall extend the definition of X_ν by setting $X_\nu(h) = 0$, if h is a polynomial not in G'_ν. Consider the formal power series

$$L_\nu(X_\nu, U) \coloneqq \sum_{\substack{h\in\mathbb{F}_{q^\nu}[X] \\ \text{monic}}} X_\nu(h)U^{\nu\deg(h)} \in \mathbb{C}[[U]]. \tag{49}$$

Proposition 3.12 (Product Formula)**.**

$$L_\nu(X_\nu, U) = \prod_{h \text{ irreducible, monic}} (1 - X_\nu(h)U^{\deg(h)})^{-1}. \tag{50}$$

Proof. Since every polynomial can be written uniquely as a product of powers of irreducible polynomials, we get in analogy to the Euler product formula for Zeta-functions

$$\begin{aligned}\sum_{\substack{h\in\mathbb{F}_{q^\nu}[X]\\ \text{monic}}} X_\nu(h)U^{\nu\deg(h)} &= \prod_{h \text{ irreducible, monic}} (1+\frac{X_\nu(h)}{U^{\deg(h)}}+\frac{X_\nu(h^2)}{U^{2\deg(h)}}+\cdots)\\ &= \prod_{h \text{ irreducible, monic}} (1-X_\nu(h)U^{\deg(h)})^{-1}.\end{aligned} \tag{51}$$

□

Now let χ_0 the trivial multiplicative character and ψ_0 the trivial additive character. In accordance to the conditions of Weil's theorem, suppose now that $\chi \neq \chi_0$ is of exponent d and $Y^d - f(X)$ is absolutely irreducible, or $\psi \neq \psi_0$ and $Z^q - Z - g(X)$ is irreducible. Equation (5) is a corollary of Proposition 3.14 on the properties of the series L_ν.

Proposition 3.13. Let ζ be a ν-th root of unity and m be a positive integer. Then we have the polynomial identity

$$\prod_{\zeta^\nu=1}(1-\zeta^m U) = \left(1-U^{\nu/(\nu,m)}\right)^{(\nu,m)}. \tag{52}$$

Proof. In the case where $(\nu,m)=1$, the identity reduces to

$$\prod_{\zeta^\nu=1}(1-\zeta^m U) = 1-U^\nu, \tag{53}$$

which in this case is a true statement, since both sides are polynomials of degree ν with constant term 1 and with roots ζ^{-m}. For the general case, let $\nu=\nu_1(\nu,m)$ and $m=m_1(\nu,m)$. As the summation runs through a residue system modulo ν, it runs (ν,m) times a residue system modulo ν_1. Therefore, the result is obtained by raising

$$\prod_{\zeta^{\nu_1}=1}(1-\zeta_1^m U) = 1-U^{\nu_1} \tag{54}$$

to the (ν,m)-th power. Equation 54 is correct by the first case, since $(\nu_1,m_1)=1$. □

Proposition 3.14. The series L_ν can be written as

$$L_\nu(X_\nu,U) = \prod_{\zeta^\nu=1} L_1(X_1,\zeta U), \tag{55}$$

where ζ is a root of unity.

Proof. By Proposition 3.12, for all ν

$$L_\nu(X_\nu, U) = \prod_{\substack{h\in\mathbb{F}_{q^\nu}[X]\\ \text{irreducible,monic}}} (1 - X_\nu(h)U^{\nu\deg(h)})^{-1}. \tag{56}$$

All irreducible, monic polynomials $h \in \mathbb{F}_q[X]$ of degree d split into $k \coloneqq (d, \nu)$ distinct monic irreducible polynomials of degree $e \coloneqq d/k$:

$$h(X) = \tilde{h_1}(X)\cdots\tilde{h_k}(X) \tag{57}$$

with $\tilde{h_i} \in \mathbb{F}_{q^k}[X]$ for all $i \in \{1, \dots, k\}$. By definition,

$$X_\nu(\tilde{h_i}) = \chi_\nu(\{\tilde{h_i}\})\psi_\nu([\tilde{h_i}]) \tag{58}$$

with

$$\begin{aligned}
\chi_\nu(\{\tilde{h_i}\}) &= \chi\left(\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}\left(\prod_{j=1}^m \tilde{h_i}(\gamma_j)^{a_j}\right)\right)\\
&= \chi\left(\prod_{i=1}^k \mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_{q^k}}\left(\prod_{j=1}^m \tilde{h_i}(\gamma_j)^{a_j}\right)\right)\\
&= \chi\left(\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_{q^k}}\left(\prod_{j=1}^m h(\gamma_j)^{a_j}\right)\right)\\
&= \chi\left(\prod_{j=1}^m h(\gamma_j)^{a_j}\right) = \chi(\{h\})^{\nu/k}
\end{aligned} \tag{59}$$

and

$$\begin{aligned}
\psi_\nu([\tilde{h_i}]) &= \psi\left(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}([\tilde{h_i}])\right)\\
&= \psi\left(\sum_\mu \sum_j g(\alpha_{ij})^{q^\mu}\right)\\
&= \psi\left(\sum_\mu \sum_j g(\alpha_{ij}^{q^\mu})\right)\\
&= \psi\left(\frac{\nu}{k}\sum_{i,j} g(\alpha_{ij})\right)\\
&= \psi\left(\sum_{i,j} g(\alpha_{ij})\right)^{\nu/k}\\
&= \psi([h])^{\nu/k}.
\end{aligned} \tag{60}$$

Therefore for all $i \in \{1, \dots, k\}$

$$X_\nu(\tilde{h_i}) = X_1(h)^{\nu/k}. \tag{61}$$

It follows that

$$X_\nu(\tilde{h_i})U^{\nu/k} = (X_1(h)U)^{\nu/k}. \tag{62}$$

Now, by Proposition 3.13, setting $m = d$ and $X = X_1(h)U^d$ we can write

$$\begin{aligned} L_\nu(X_\nu, U) &= \prod_{\substack{h \in \mathbb{F}_{q^\nu}[X] \\ \text{irreducible,monic}}} (1 - X_1(h)U^{e\nu})^{-k} \\ &= \prod_{\substack{h \in \mathbb{F}_{q^\nu}[X] \\ \text{irreducible,monic}}} \prod_{\zeta^\nu = 1} (1 - \zeta^d X_1(h)U^d)^{-1} \\ &= \prod_{\zeta^\nu = 1} \prod_{\substack{h \in \mathbb{F}_{q^\nu}[X] \\ \text{irreducible,monic}}} (1 - \zeta^d X_1(h)U^d)^{-1} \\ &= \prod_{\zeta^\nu = 1} L_1(X_1, \zeta U) \end{aligned} \tag{63}$$

which is the desired result. □

Proposition 3.15. The L-series is a polynomial in the variable U that is of the form

$$L_1(X_\nu, U) = 1 + c_1 U + \ldots + c_{n+m-1}U^{(n+m-1)} \tag{64}$$

and if $\chi \neq \chi_0$ or if $\chi = \chi_0$ and $f(X) = 1$, then

$$c_1 = \sum_{x \in \mathbb{F}_q} \chi(f(x))\psi(g(x)). \tag{65}$$

Proof. We write $L_1(X_\nu, U_h) = 1 + c_1 U_h + \ldots$ with

$$c_t = \sum_{\substack{h \in G'_\nu \\ \text{polynomial} \\ \text{of degree } t}} X_\nu(h). \tag{66}$$

for all t. By Proposition 3.11 (c), we have $c_t = 0$ if $t \geq n+m$. Thus $L_1(X_\nu, U_h)$ is a polynomial in U_h of degree less than $n+m$. Using the definition of X_ν we get

$$\begin{aligned} c_1 &= \sum_{\substack{h \in G'_\nu \\ \text{polynomial} \\ \text{of degree 1}}} X_\nu(h) = \sum_{\substack{x \\ \forall i:\ x+\gamma_i \neq 0}} X_\nu(X+x) \\ &= \sum_{\substack{\forall i:\ x+\gamma_i \neq 0}} \chi_\nu(\{X+x\})\psi_\nu([X+x]) \\ &= \sum_{\substack{\forall i:\ x+\gamma_i \neq 0}} \chi_\nu((x+\gamma_1)^{a_1}\cdots(x+\gamma_m)^{a_m})\psi_\nu(g(x)) \\ &= \sum_{f(x)\neq 0} \chi_\nu(f(x))\psi_\nu(g(x)) \\ &= \sum_x \chi_\nu(f(x))\psi_\nu(g(x)). \end{aligned} \tag{67}$$

□

Proposition 3.16. There exist $k \in \mathbb{N}$ and $\omega_1, ..., \omega_k \in \mathbb{C}$ such that for all ν

$$L_\nu(X_\nu, U) = (1-\omega_1^\nu U^\nu)\cdots(1-\omega_k^\nu U^\nu). \tag{68}$$

Proof. By Proposition 3.15 we can write $L_1(X,U) = 1 + c_1 U + ... + c_{n+m-1}U^{(n+m-1)}$. *i.e* it is a polynomial in U with constant term 1. Therefore we can write

$$L_1(X, U_h) = (1-\omega_1 U)...(1-\omega_k U) \tag{69}$$

for complex $\omega_1, ..., \omega_k$. With Proposition 3.14 we can write

$$\begin{aligned} L_\nu(X_\nu, U) &= \prod_{\zeta^\nu = 1} L_1(X, \zeta U) \\ &= (1-\omega_1^\nu U^\nu)...(1-\omega_k^\nu U^\nu) \end{aligned} \tag{70}$$

which is the desired result. □

The next proposition is the main result of this chapter and yields Equation (5).

Proposition 3.17. Suppose that $\chi \neq \chi_0$ is of exponent d and $Y^d - f(X)$ is absolutely irreducible, or that $\psi \neq \psi_0$ and $Z^q - Z - g(X)$ is irreducible. Suppose that $\chi \neq \chi_0$ or $\chi = \chi_0$ with $f(X) = 1$. Then, for all ν

$$S_{\chi\psi\nu} = -(\omega_{\chi\psi,1}^\nu + ... + \omega_{\chi\psi,m+n-1}^\nu). \tag{71}$$

Proof. We apply Proposition 3.15 to $\mathbb{F}_{q^\nu}$ and with Proposition 3.16 we have

$$\begin{aligned} L_\nu(X,U) &= 1 + c_{\nu,1}U^\nu + \ldots + c_{\nu,n+m-1}U^{\nu(n+m-1)} \\ &= (1-\omega_1^\nu U^\nu)...(1-\omega_k^\nu U^\nu) \end{aligned} \tag{72}$$

Comparing coefficients and, since by Proposition 3.15 $c_{\nu,1} = S_{\chi\psi\nu}$, we deduce

$$S_{\chi\psi\nu} = c_{\nu,1} = -(\omega_{\chi\psi,1}^\nu + ... + \omega_{\chi\psi,m+n-1}^\nu). \tag{73}$$

□

4. Proof of Weil's Theorem: Putting it all together

The goal of this section is to use the results from the previous chapters to prove Theorem 1.1. Let $f, g \in \mathbb{F}_{q^\nu}[x]$ satisfy the hypotheses of Theorem 1.1. We first impose the condition that f is monic and that g has constant term zero. We recall the definition

$$S_{\chi\psi\nu} \coloneqq \sum_{x\in\mathbb{F}_q} \chi\left(\mathrm{Nm}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(f(x))\right)\cdot\psi\left(\mathrm{Tr}_{\mathbb{F}_{q^\nu}/\mathbb{F}_q}(g(x))\right). \tag{74}$$

By Proposition 3.17 we can write

$$S_{\chi\psi\nu} = -(\omega_{\chi\psi,1}^\nu + ... + \omega_{\chi\psi,m+n-1}^\nu) \tag{75}$$

with the following bound on the absolute values of $\omega_{\chi\psi,1}^\nu, ..., \omega_{\chi\psi,m+n-1}^\nu$:

Proposition 4.1. For all i,

$$|\omega_{\chi\psi,i}| \leq \sqrt{q}. \tag{76}$$

Proof. By Lemma 2.5 and Theorem 1.4 applied to $\mathbb{F}_{q^\nu}$ we can write

$$\sum_{\substack{\chi \\ \text{of exponent} \\ \text{dividing } d}} \sum_{\psi} S_{\chi\psi\nu} = N_\nu = q^\nu + O(q^{\nu/2}). \tag{77}$$

Applying Lemma 4.2 on Equation (77) together with Proposition 3.17 and using the fact that $S_{\chi_0\psi_0\nu} = q^\nu$ yields the desired result. □

Lemma 4.2. *If $\omega_1, ..., \omega_l$ are complex numbers and for a $B > 0$ such that $\omega_1^\nu + ... + \omega_l^\nu = O(B^\nu)$ for all ν, then $|\omega_j| \leq B$ for all $j \in \{1, ..., l\}$.*

Proof. We consider the expansion

$$-\log(1-\omega z) = \omega x + \frac{1}{2}\omega^2 z^2 + \frac{1}{3}\omega^3 z^3 + \dots \quad . \tag{78}$$

Then

$$-\log((1-\omega_1 z)\cdots(1-\omega_l z)) = \sum_{\nu=1}^{\infty} \frac{1}{\nu}(\omega_1^\nu + \ldots + \omega_l^\nu) z^\nu. \tag{79}$$

By assumption, the sum on the right hand side converges and therefore the function on the left hand side is analytic for $|z| < B^{-1}$. We get that $1 - \omega_j z \neq 0$ if $|z| < B^{-1}$ and hence $|\omega_j| \leq B$. □

With Equation (75) , we obtain

$$|S_{\chi\psi\nu}| \leq (m+n-1)q^{\nu/2} \tag{80}$$

and in particular the statement of Theorem 1.1.

It remains to remove the restrictions on the polynomials f and g. So far, we have used that f is monic and g has zero constant term. However, since $\chi(af(x)) = \chi(a)\chi(f(x))$ our estimate for the multiplicative character still holds in general. Further, since $\psi(g(x)+b) = \psi(g(x))\psi(b)$ we find that the absolute value of the character sum does not change.

This concludes the proof of Weil's Theorem.

5. Application of Weil's Theorem: A Bound on Kloosterman Sums

We consider a non-trivial additive character ψ and the Kloosterman sums

$$\left| \sum_{x \in \mathbb{F}_q^*} \psi(ax + bx^{-1}) \right| \tag{81}$$

where $a, b \in \mathbb{F}_q^*$ and x^{-1} is the inverse of x in $\mathbb{F}_q$.

Theorem 5.1. *Let ψ a non-trivial character of $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q^*} \psi(ax + bx^{-1}) \right| \leq 2\sqrt{q}. \tag{82}$$

In the following, we present a proof of the theorem for the case when q is odd. In order to be able to directly apply Weil's Theorem, we apply the following Lemma to the given Kloosterman sum.

Lemma 5.2. *Let $\psi \neq \psi_0$ and χ be any quadratic character of $\mathbb{F}_q^*$. Then,*

$$\sum_{x\in\mathbb{F}_q^*} \psi(ax+bx^{-1}) = \sum_{y\in\mathbb{F}_q} \psi(y)\chi(y^2-4ab). \tag{83}$$

Proof. The sum on the left hand side can be written as

$$\sum_{y\in\mathbb{F}_q} \psi(y)Z(y) \tag{84}$$

with $Z(y)$ the number of $x \in \mathbb{F}_q^*$ with $y = ax + bx^{-1}$. Solving for x yields

$$x = \frac{1}{2a} \pm \sqrt{y^2-4ab} \tag{85}$$

which may or may not be an element of $\mathbb{F}_q$. If $y^2 - 4ab \neq 0$ is a square, then $Z(y) = 2$. If $y^2 - 4ab \neq 0$ is not a square, then $Z(y) = 0$. If $y^2 - 4ab = 0$, then $Z(y) = 1$. Now, since χ is the quadratic character of $\mathbb{F}_q$, we have that $\chi(z) = 1$ or $\chi(z) = -1$ if $z \neq 0$ is a square or a non-square in $\mathbb{F}_q$. We get

$$Z(y) = \chi(y^2-4ab) + 1. \tag{86}$$

With this we can write

$$\begin{aligned}\sum_{x\in\mathbb{F}_q^*} \psi(ax+bx^{-1}) &= \sum_{y\in\mathbb{F}_q} \psi(y)Z(y) \\ &= \sum_{y\in\mathbb{F}_q} \psi(y)\chi(y^2-4ab) + \sum_{y\in\mathbb{F}_q} \psi(y) \\ &= \sum_{x\in\mathbb{F}_q} \psi(x)\chi(x^2-4ab).\end{aligned} \tag{87}$$

□

The polynomials $Y^2 - (X^2 - 4ab)$ and $Z^q - Z - X$ are absolutely irreducible and therefore the conditions of Weil's theorem are satisfied and we deduce that the sum on the right hand side of Lemma 5.2 has absolute value $\leq (m+n-1)\sqrt{q} = 2\sqrt{q}$, which proves Theorem 5.1.

Theorem 5.1 also holds when q is even and we shall now sketch a proof for this case. Let G be the group of rational functions $\frac{h_1(X)}{h_2(X)}$ where $h_1(X)$ and $h_2(X)$ are monic polynomials. Let $\hat{G}$ be the subgroup of functions whose numerators and denominators have non-zero constant

term. For $r(x) \in \hat{G}$, let

(88)
$$[r] \coloneqq \begin{cases} a(\alpha_1 + \ldots + \alpha_u - \beta_1 - \ldots - \beta_v) + b(\frac{1}{\alpha_1} + \ldots + \frac{1}{\alpha_u} - \frac{1}{\beta_1} - \ldots - \frac{1}{\beta_v}) & \text{if } r(X) = \frac{\prod_{i=1}^{u}(X+\alpha_i)}{\prod_{j=1}^{u}(X+\beta_j)} \\ 0, & \text{if } r(X) = 1 \end{cases},$$

with $\alpha_1, \ldots, \alpha_u, \beta_1, \ldots, \beta_v \in \overline{\mathbb{F}_q}$. Then $[r] \in \mathbb{F}_q$ and $[r_1 r_2] = [r_1] + [r_2]$ and the function $X(r) \coloneqq \psi([r])$ is a character on $\hat{G}$. We let $\hat{H}$ be the subset of $\hat{G}$ consisting of $r(X) = \frac{h_1(X)}{h_2(X)}$ where

$$\begin{aligned} h_1(X) &= X^u + a_1 X^{u-1} + \ldots + a_{u-1} X + a_u, \\ h_2(X) &= X^v + b_1 X^{v-1} + \ldots + b_{v-1} X + b_v \end{aligned} \tag{89}$$

with

$$a_1 = b_1, \quad \frac{a_{u-1}}{a_u} = \frac{b_{v-1}}{b_v}. \tag{90}$$

We find that $\hat{H}$ is a subgroup of $\hat{G}$ and as an analogue to Lemma 3.7 we have

Lemma 5.3. *If $r \in \hat{H}$, then $X(r) = 1$.*

Proof. If $r \in \hat{H}$, then

$$\alpha_1 + \ldots + \alpha_u - \ldots - \beta_v = a_1 - b_1 = 0 \tag{91}$$

and

$$\frac{1}{\alpha_1} + \ldots + \frac{1}{\alpha_u} - \frac{1}{\beta_1} - \ldots - \frac{1}{\beta_v} \tag{92}$$

which yields $[r] = 0$ and $X(r) = \psi([r]) = 1$. □

The analogue to Proposition 3.8 is

Proposition 5.4. Let $\ell \geq 0$. Then every coset of $\hat{H}$ in $\hat{G}$ contains precisely $q^\ell(q-1)$ polynomials of degree $\ell + 3$.

By carrying out the analogue of the argument in Chapter 3, we find that the L-function $L(X, U)$ is a polynomial of the type

$$L(X, U) = 1 + c_1 U + c_2 U^2 = (1 - \omega_1)(1 - \omega_2 U) \tag{93}$$

with

$$c_1 = \sum_{x \in \mathbb{F}_q^*} \psi(ax + bx^{-1}). \tag{94}$$

The result follows immediately from $|\omega_i| \leq q^{1/2}$ which is deduced by showing that the numer N_ν x, z in $\mathbb{F}_{q^\nu}$ of $x \neq 0, \quad z^q - z = ax + bx^{-1}$ satisfies Equation (7). This follows from Theorem 1.4 , since $aX^2 - (Z^q - Z)X + b$ is absolutely irreducible.

References

1. A.Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités sci. et ind. **1041** (1948).
2. Robin Hartshorne, *Algebraic Geometry*, Springer, 2000.
3. Henryk Iwaniec and Emmanuel Kowalski, *Analytic Number Theory*, American Mathematical Society, 2000.
4. H. Kloosterman, *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Mathematica **49** (1926), 407–464.
5. Jürgen Neukirch, *Algebraic Number Theory*, Springer, 1999.
6. Wolfgang M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Springer, 1976.
7. A. Weil, *Sur les fonctions algébriques à corps de constantes fini*, C. R. Acad. Sci. **210** (1940), 592–594.

ETH Zurich, Zurich, Switzerland