Explicit Construction of the Intermediate Fields Between $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}$

Shuaishuai Duan
Nanjing University of Information Science and Technology

1 Preliminary

This article aims to give an explicit construction of the intermediate fields between $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}$ by using Galois theory, exponential sum and valuation theory, where ζ_p is a primitive p-th root of unity. Proofs of propositions and theorems in the preliminary could be found in the sources listed in the references part.

1.1 Galois Theory

Definition 1.1. *Let K be a field extension of F. A field L with $F \subseteq L \subseteq K$ is called an **intermediate field** of the extension K/F.*

Definition 1.2. *Let K be a field extension of F. The **Galois group** $\mathrm{Gal}(K/F)$ is the set of all F-automorphisms of K.*

Proposition 1.1. *Let $\tau : K \to L$ be an F-automorphism and let $\alpha \in K$ be algebraic over F. If $f(x) = 0$, then $f(\tau(\alpha)) = 0$. Therefore, τ permutes the roots of the minimal polynomial of α over F.*

Definition 1.3. *Let S be a subset of $Aut(K)$. The set*

$$\mathcal{F}(S) = \{a \in K | \tau(a) = a \, for \, all \, \tau \in S\}$$

*is a subfield of K, called the **fixed field** of S.*

Theorem 1.1. (Fundamental Theorem of Galois Theory) *Let K be a finite Galois extension of F, and let $G = \mathrm{Gal}(K/F)$. Then there is a $1-1$ inclusion reversing correspondence between intermediate fields of K/F and subgroups of G, given by $L \mapsto \mathrm{Gal}(K/L)$ and $H \mapsto \mathcal{F}(H)$. Furthermore, if $L \leftrightarrow H$, then $[K : L] = |H|$ and $[L : F] = [G : H]$.*

Theorem 1.2. *Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements and $\mathbb{F}_p = \{1, 2, \ldots, p-1\}$ be a finite field with p elements, where p is a prime. Then the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group of order n with generator $\sigma : \alpha \mapsto \alpha^p$.*

Definition 1.4. *The map*

$$\mathrm{Tr}_n : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p, \alpha \mapsto \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)} \sigma(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$$

*is called **trace** map.*

1.2 Cyclic Group and Exponential Sum

Theorem 1.3. (Fundamental Theorem of Cyclic Group) *Let $G = \langle a \rangle$ be a cyclic group. Then every subgroup of G is cyclic. Moreover, if $|G| = n$, then the order of any subgroup of G is a divisor of n and for each positive divisor d of n, the group G has exactly one subgroup of order d, namely, $\langle a^{\frac{n}{d}} \rangle$.*

Definition 1.5. *The **exponential sums** over $\mathbb{F}_{p^k}$ is to be*

$$S_k(f) = \sum_{x_1, \ldots, x_n \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(f(x_1, \ldots, x_n))} \in \mathbb{Z}[\zeta_p]$$

where p is a prime, f is a polynomial with n variables over $\mathbb{Z}$.

Definition 1.6. *Let α be an algebraic element over $\mathbb{Q}$, the **degree** of α is* $\deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Proposition 1.2. *If F be a finite field, then F^* is cyclic, where $F^* = F \backslash \{0\}$.*

1.3 Valuations

Definition 1.7. *Let K^* be the multiplicative group of a field K, and let $\mathbb{Z}$ be the integers under addition. A map*

$$\upsilon : K \to \mathbb{Z} \cup \infty$$

*is a **discrete valuation** of K, if*
(1). υ defines a surjective homomorphism $K^* \to \mathbb{Z}$;
(2). $\upsilon(0) = \infty$;
(3). $\upsilon(x + y) \geq \min\{\upsilon(x), \upsilon(y)\}$.
*Moreover, if we replace $\mathbb{Z}$ by $\mathbb{R}$, then υ is a **valuation** of K.*

Definition 1.8. *Let p be a prime. The p-**adic valuation** $\upsilon_p : \mathbb{Q} \to \mathbb{Z}$ is given by*

$$\upsilon_p(r) = \begin{cases} a_p, if\ r \neq 0, \\ \infty, if\ r = 0, \end{cases}$$

for any $r \in \mathbb{Q}^*$, where $r = \pm \prod_p p^{a_p}$, $a_p \in \mathbb{Z}$.

Definition 1.9. *Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ is a monic polynomial. $f(x)$ is p-**Eisentein** if $p|a_i$ for all $1 \leq i \leq n$ and $p^2 \nmid a_n$ where p is a prime. More general, $f(x)$ is **generalized** p-**Eisentein** if $\upsilon_p(a_i) \geq \frac{i}{n}\upsilon_p(a_n)$ for all $1 \leq i \leq n$ and $(n, \upsilon_p(a_n)) = 1$.*

Proposition 1.3. *If $f(x)$ is generalized p-Eisenstein, then $f(x)$ is irreducible over $\mathbb{Q}_p$, and hence irreducible over $\mathbb{Q}$.*

Proposition 1.4. *Let K be complete with respect to the norm induced by the valuation υ. Then υ may be extended in a unique way to a valuation of any given algebraic extension L/K. Therefore, we may assume that the valuation υ_p is obtained after extension as $\mathbb{Q}_p$ is complete, and we still denote it as υ_p.*

1.4 Representation of $\mathbb{F}_{p^k}^*$ and p-adic Gauss Sum

Proposition 1.5. *Any multiplicative character $\chi : \mathbb{F}_{p^k}^* \to \mathbb{C}_p^*$ can be uniquely written as $\chi = \omega^{-i}$, $0 \leq i < p^k - 1$, where ω is the **Teichmüller lifting** of $\mathbb{F}_{p^k}^*$. The case $i = 0$ corresponds to the trivial character.*

Definition 1.10. *The p-**adic Gauss sum** attached to the multiplicative character $\omega^{-i} : \mathbb{F}_{p^k}^* \to \mathbb{C}_p^*$ is defined as*

$$G_k(i) = -\sum_{x \in \mathbb{F}_{p^k}^*} \omega^{-i}(x)\zeta_p^{\mathrm{Tr}_k(x)} = -\sum_{x \in \mathbb{F}_{p^k}^*} \chi(x)\zeta_p^{\mathrm{Tr}_k(x)},$$

where $0 \leq i < p^k - 1$ and χ is the corresponding character.

In this article we will not go further in the Teichmüller lifting and we only use it formally. For more details, see [1].

Proposition 1.6. *We have the relation*

$$\sum_{\chi^d = 1} \chi(x) = \begin{cases} d, \text{ if } x \in (\mathbb{F}_{p^k}^*)^d; \\ 0, \text{ otherwise.} \end{cases}$$

2 Construction of the Intermediate Fields

Recall that υ_p is defined on an algebraic extension over $\mathbb{Q}_p$, more precisely, the finite algebraic extension $\mathbb{Q}_p(\zeta_p)$ over $\mathbb{Q}_p$.

Lemma 2.1. *Let υ_p be the p-adic valuation. If $\upsilon_p(x) \neq \upsilon_p(y)$, for any $x,\ y \in \mathbb{Q}_p(\zeta_p) \setminus \{0\}$, then $\upsilon_p(x+y) = \min\{\upsilon_p(x),\ \upsilon_p(y)\}$.*

Proof. Without loss of generality, we assume $\upsilon(x) < \upsilon_p(y)$, then the definition of valuation gives

$$\upsilon_p(x+y) \geq \min\{\upsilon_p(x),\ \upsilon_p(y)\} = \upsilon_p(x).$$

On the other hand,

$$\upsilon_p(x) = \upsilon_p(x-y+y) \geq \min\{\upsilon_p(x+y),\ \upsilon_p(y)\}.$$

If $\min\{\upsilon_p(x+y),\ \upsilon_p(y)\} = \upsilon_p(y)$, then $\upsilon_p(x) \geq \upsilon_p(y)$ which is impossible by our assumption.
Therefore,

$$\upsilon_p(x) \geq \min\{\upsilon_p(x+y),\ \upsilon_p(y)\} = \upsilon_p(x+y),$$

which implies $\upsilon_p(x) = \upsilon_p(x+y)$. □

Lemma 2.2. *The exponential sum $S_k(x)$ equals to 0.*

Proof. We expand the exponential sum as

$$S_k(x) = \sum_{x \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(x)} = \sum_{a \in \mathbb{F}_p} \zeta_p^a \cdot \#\{x \in \mathbb{F}_{p^k} | \mathrm{Tr}_k(x) = a\}.$$

Since Tr_k is $\mathbb{F}_p$-linear and surjective, then the kernel of Tr_k has dimension $k-1$. It follows that

$$\#\{x \in \mathbb{F}_{p^k} | \mathrm{Tr}_k(x) = a\} = p^{k-1}.$$

Therefore, $S_k(x) = p^{k-1} \sum_{a \in \mathbb{F}_p} \zeta_p^a = 0$. □

Theorem 2.1. (Stickelbeger) *For $0 \leq i < p^k - 1$, write*

$$i = i_0 + i_1 p + i_2 p^2 + \cdots + i_{k-1} p^{k-1}$$

and

$$\sigma_p(i) = i_0 + i_1 + \cdots + i_{k-1} = \text{sum of } p\text{-digits of } i,$$

then

$$\upsilon_p(G_k(i)) = \frac{1}{p-1} \sigma_p(i).$$

Proof. See [2]. $\square$

Lemma 2.3. *If $d|p-1$ and $d>0$, then for $1 \le i \le d-1$, we have*

$$\upsilon_p\left(G_k(\frac{p^k-1}{d}i)\right) = \frac{ki}{d}.$$

Proof. Write

$$\frac{p^k-1}{d}i = \frac{i(p-1)}{d}\frac{p^k-1}{p-1} = \frac{i(p-1)}{d} + \frac{i(p-1)}{d}p + \cdots + \frac{i(p-1)}{d}p^{k-1}.$$

Then $\sigma_p(\frac{p^k-1}{d}i) = ki\frac{p-1}{d}$. Hence, by Theorem 2.1, we obtain

$$\upsilon_p\left(G_k(\frac{p^k-1}{d}i)\right) = \frac{ki}{d}.$$

$\square$

Lemma 2.4. *If $d|p-1$,$d>0$ then $\upsilon_p(S_k(ax^d)) = \frac{k}{d}$ for all $a \in \mathbb{F}_p^*$.*

Proof. Let $\chi := \omega^{-\frac{p^k-1}{d}} : \mathbb{F}_{p^k}^* \to \mathbb{C}_p$ be the primitive character of degree d. Then

$$\begin{aligned} S_k(ax^d) &= \sum_{x\in\mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(ax^d)} = \zeta_p^a\left(1 + \sum_{x\in\mathbb{F}_{p^k}^*} \zeta_p^{\mathrm{Tr}_k(x^d)}\right) \\ &= \zeta_p^a\left(1 + \sum_{y\in\mathbb{F}_{p^k}^*}\left(\sum_{i=1}^{d}\chi^i(y)\right)\zeta_p^{\mathrm{Tr}_k(y)}\right) \end{aligned}$$

because of

$$\sum_{i=1}^{d}\chi^i(y) = \begin{cases} d, \ if \ y \in (\mathbb{F}_{p^k}^*)^d, \\ 0, \ if \ y \notin (\mathbb{F}_{p^k}^*)^d, \end{cases}$$

by Proposition 1.6. It follows that

$$\begin{aligned} S_k(ax^d) &= \zeta_p^a\left(\sum_{i=1}^{d-1}\sum_{y\in\mathbb{F}_{p^k}^*}\chi^i(y)\zeta_p^{\mathrm{Tr}_k(y)} + \left(\sum_{y\in\mathbb{F}_{p^k}^*}\zeta_p^{\mathrm{Tr}_k(y)} + 1\right)\right) \\ &= \zeta_p^a\left(\sum_{i=1}^{d-1}\sum_{y\in\mathbb{F}_{p^k}^*}\chi^i(y)\zeta_p^{\mathrm{Tr}_k(y)} + \sum_{y\in\mathbb{F}_{p^k}}\zeta_p^{\mathrm{Tr}_k(y)}\right) \\ &= \zeta_p^a\left(\sum_{i=1}^{d-1}\sum_{y\in\mathbb{F}_{p^k}^*}\chi^i(y)\zeta_p^{\mathrm{Tr}_k(y)} + S_k(y)\right). \end{aligned}$$

Then Definition 1.10 and Lemma 2.2 display

$$S_k(ax^d) = -\zeta_p^a \left(\sum_{i=1}^{d-1} G_k(\frac{p^k-1}{d}i) \right),$$

which leads to

$$\upsilon_p(S_k(ax^d)) = a\upsilon_p(\zeta_p) + \upsilon_p \left(\sum_{i=1}^{d-1} G_k(\frac{p^k-1}{d}i) \right).$$

Thus, Lemma 2.1 and Lemma 2.3 imply

$$\upsilon_p(S_k(ax^d)) = \frac{k}{d}.$$

$\square$

Theorem 2.2. *If* $d|p-1$*, then* $\deg(S_k(x^d)) = \frac{d}{(d,k)}$*, where* (d,k) *is the greatest common divisor of* d *and* k*.*

Proof. Let $H = \{a \in \mathbb{F}_p^* | a^{\left(p-1,\, \frac{p^k-1}{(d,\, p^k-1)}\right)} = 1\} \subseteq \mathbb{F}_p^*$. Clearly, H is s subgroup of $\mathbb{F}_p^*$ and $|H| = \left(p-1,\, \frac{p^k-1}{(d,\, p^k-1)}\right)$. By the uniqueess of subgroups of finite cyclic groups, H can be represented as

$$H = \{a^{\frac{p-1}{|H|}} | a \in \mathbb{F}_p^*\}.$$

Since $d|p-1$ and $\frac{p-1}{d} | \left(p-1,\, \frac{p^k-1}{(d,\, p^k-1)}\right) = \left(p-1,\, \frac{p-1}{d}N\right)$ for some $N \in \mathbb{N}$, then H is a subset of H_d, Namely, for any $z \in H$, there exists $a \in \mathbb{F}_p^*$ such that $z = a^d$. Therefore, for any element $z \in H$, we have

$$\sigma_z(S_k(x^d)) = \sigma_z(\sum_{x \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(x^d)}) = \sum_{x \in \mathbb{F}_{p^k}} \zeta_p^{z\mathrm{Tr}_k(x^d)} \tag{1}$$

It is not hard to see that the trace map Tr_k is $\mathbb{F}_p$-linear. Therefore, the equation (1) becomes

$$\sigma_z(S_k(x^d)) = \sum_{x \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(zx^d)} = \sum_{x \in \mathbb{F}_{p^k}} \zeta_p^{\mathrm{Tr}_k(a^d x^d)} = S_k(x^d),$$

for some $a \in \mathbb{F}_p^*$ i.e. $S_k(x^d)$ is fixed by H. That is $\mathbb{Q}(S_k(x^d)) \subseteq \mathcal{F}(H)$. Again, when $d|p-1$, we deduce the following equality,

$$\begin{aligned}
\frac{p-1}{|H|} &= \frac{p-1}{\left(p-1,\ \frac{p^k-1}{(d,\,p^k-1)}\right)} = \frac{p-1}{\left(p-1,\ \frac{p^k-1}{d}\right)} = \frac{p-1}{\left(p-1,\ \frac{p-1}{d}\frac{p^k-1}{p-1}\right)} \\
&= \frac{d}{\left(d,\ \frac{p^k-1}{p-1}\right)} = \frac{d}{\left(d,\ \frac{(p-1)(p^{k-1}+p^{k-2}+\cdots+1)}{p-1}\right)} \\
&= \frac{d}{(d,\ k+p^{k-1}-1+p^{k-2}-1+\cdots+1-1)} \\
&= \frac{d}{(d,\ k+(p-1)M)} = \frac{d}{(d,\ k)}
\end{aligned}$$

for some $M \in \mathbb{N}$.
Now we consider the polynomial

$$m(y) = \prod_{a\in\mathbb{F}_p^*/H} (y - S_k(ax^d)).$$

Obviously, the polynomial is monic of degree $D := \frac{p-1}{|H|} = \frac{d}{(d,\,k)}$ with $\deg(S_k(x^d))$ as a root. We claim that the polynomial $m(y)$ is irreducible over $\mathbb{Q}$, then it implies the result because of $\deg(S_k(x^d)) = [\mathbb{Q}(S_k(x^d)) : \mathbb{Q}] = \deg(m(y)) = \frac{d}{(d,\,k)} = [\mathcal{F}(H) : \mathbb{Q}]$.
For any $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $1 \le i \le p-1$, we have

$$\begin{aligned}
\sigma_i(m(y)) &= \prod_{a\in\mathbb{F}_p^*/H} (y - \sum_{x\in\mathbb{F}_{p^k}} \sigma_i(\zeta_p^{ax^d})) = \prod_{a\in\mathbb{F}_p^*/H} (y - \sum_{x\in\mathbb{F}_{p^k}} \zeta_p^{aix^d}) \\
&= \prod_{z\in\mathbb{F}_p^*/H} (y - \sum_{x\in\mathbb{F}_{p^k}} \zeta_p^{zx^d}) = m(y)
\end{aligned}$$

where $z = ai$. Then it follows that $m(y)$ is a polynomial over $\mathbb{Q}$. To prove the irreducibility of $m(y)$, we write $m(y)$ as the sum

$$m(y) = y^D - b_1 y^{D-1} + b_2 y^{D-2} + \cdots + (-1)^D b_D,$$

where b_i is the i-th elementary symmetric polynomial of $\{S_k(ax^d) | a \in \mathbb{F}_p^*/H\}$, for $1 \le i \le D$. Then Lemma 2.4 displays

$$\upsilon_p(b_D) = D\frac{k}{d} = \frac{d}{(d,\ k)}\frac{k}{d} = \frac{k}{(d,\ k)}$$

and

$$\upsilon_p(b_i) \ge i\frac{k}{d} = \frac{i}{\frac{d}{(d,\,k)}}\frac{d}{(d,\ k)} = \frac{i}{D}\frac{k}{(d,\ k)},\ 1 \le i \le D,$$

where $(D,\ \upsilon_p(b_D)) = \left(\frac{d}{(d,\,k)},\ \frac{k}{(d,\,k)}\right) = 1$. It shows that $m(y)$ is generalized p-Eisenstein, and therefore irreducible over $\mathbb{Q}$ from Proposition 1.3. Namely, the claim is correct. $\square$

Definition 2.1. *The function $\tau(n)$ is the number of positive divisors of n, namely,*

$$\tau(n) = \sum_{d|n,\, d>0} 1,$$

where n is a positive integer.

Theorem 2.3. *There are exactly $\tau(p-1)$ intermediate fields between $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}$. Moreover, the intermediate fields are given by $\mathbb{Q}(S_1(x^d))$ for all positive integers $d|p-1$.*

Proof. We know that the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension and the minimal polynomial of ζ_p over $\mathbb{Q}$ is the cyclotomic polynomial

$$\Phi(x) = \frac{x^p - 1}{x - 1} = \prod_{i=1}^{p-1}(x - \zeta_p^i).$$

By Proposition 1.1 the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ permute the roots of $\Phi(x)$, which implies that for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we obtain $\sigma \in \{\zeta_p, \ldots, \zeta_p^{p-1}\}$. For a fixed i, $1 \le i \le p-1$, we have isomorphisms

$$\phi_1 : \mathbb{Q}(\zeta_p) \to \mathbb{Q}[x]/(\Phi(x)),\ \zeta_p \mapsto x + (\Phi(x))$$

and

$$\phi_2 : \mathbb{Q}[x]/(\Phi(x)) \to \mathbb{Q}(\zeta_p^i) = \mathbb{Q}(\zeta_p),\ x + (\Phi(x)) \mapsto \zeta_p^i.$$

Since $|\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, then we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \{\sigma_i | \sigma_i : \zeta_p \mapsto \zeta_p^i,\ 1 \le i \le p-1\} \cong \mathbb{F}_p^*.$$

According to Proposition 1.2, $\mathbb{F}_p^*$ is cyclic and therefore all subgroups of $\mathbb{F}_p^*$ are exactly given by $H_d = \{a^d | a \in \mathbb{F}_p^*\}$ for every positive integer $d|p-1$, followed from Theorem 1.3. In addition, Theorem 1.1 gives a $1-1$ correspondence between intermediate fields and the subgroups of $\mathbb{F}_p^*$, as the diagram shows below.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[r, dash] \arrow[d, dash] & \{1\} \arrow[d, dash] \\
\mathcal{F}(H) \arrow[r, dash] \arrow[d, dash] & H = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathcal{F}(H)) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{F}_p^*
\end{tikzcd}$$

Since we have explicitly given the structure of subgroups of $\mathbb{F}_p^*$, namely H_d, then the diagram becomes

$$\begin{tikzcd}
\mathbb{Q}(\zeta_p) \arrow[r, dash] \arrow[d, dash, "\frac{p-1}{d}"] & \{1\} \arrow[d, dash, "\frac{p-1}{d}"] \\
K_d := \mathcal{F}(H) \arrow[r, dash] \arrow[d, dash, "d"] & H_d = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_d) \arrow[d, dash, "d"] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{F}_p^*
\end{tikzcd}$$

and there are precisely $\tau(p-1)$ intermediate fields.
Therefore, the question reduces to construct the corresponding fixed field $K_d := \mathcal{F}(H_d)$ for each d, which is what we do as follows.
In general, for any $d|p-1$ we have $H_d = \{a^d | a \in \mathbb{F}_p^*\}$. For a fixed $a \in \mathbb{F}_p^*$, the corresponding $\mathbb{Q}$-automorphism of H_d is

$$\sigma_{a^d} : \zeta_p \mapsto \zeta_p^{a^d}.$$

It follows that

$$\begin{aligned}
\sigma_{a^d}(S_1(x^d)) &= \sigma_{a^d}(\sum_{x\in\mathbb{F}_p} \zeta_p^{x^d}) = \sum_{x\in\mathbb{F}_p} \sigma_{a^d}(\zeta_p^{x^d}) \\
&= \sum_{x\in\mathbb{F}_p} \zeta_p^{x^d a^d} = \sum_{x\in\mathbb{F}_p} \zeta_p^{(ax)^d} \\
&= S_1(x^d)
\end{aligned}$$

Thus, $\mathbb{Q}(S_1(x^d))$ is s subfield of K_d. Let $k=1$ in the Theorem 2.2, we deduce that $\mathbb{Q}(S_1(x^d)) = K_d$ as $\deg(S_1(x^d)) = [\mathbb{Q}(S_1(x^d)) : \mathbb{Q}] = d$, which completes the proof. $\square$

References

[1] E. Kowalski. *Exponential sums over finite fields: elementary methods.* 2018.

[2] Ludwig Stickelberger. Über eine verallgemeinerung der kreistheilung. *Mathematische Annalen*, 37(3):321–367, 1890.

[3] John William Scott Cassels and Albrecht Frölich. *Algebraic number theory: proceedings of an instructional conference.* Academic Pr, 1967.

[4] Robert Ellis. Applied algebra. 2008.

[5] Patrick Morandi. *Field and Galois theory*, volume 167. Springer Science & Business Media, 2012.

[6] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[7] Sun Qi. Some results and problems on the diophantine equations. 1988.

[8] Da Qing Wan. Some arithmetic properties of the minimal polynomials of gauss sums. *Proceedings of the American Mathematical Society*, 100(2):225–228, 1987.

[9] Daqing Wan. Algebraic theory of exponential sums over finite fields. 2019.

[10] Henri Cohen. *Number theory: Volume I: Tools and diophantine equations*, volume 239. Springer Science & Business Media, 2008.