A NEW PROOF OF ABEL-RUFFINI THEOREM

YAN PAN AND YUZHEN CHEN

ABSTRACT. The Abel-Ruffini theorem shows that the general quintic polynomial is not solvable in radicals. A proof based on a theorem of Kronecker gave by Dörrie [100 great problems of elementary mathematics: Their history and solution, Courier Corporation, 1965], but we notice a mistake in it. We give a corrected version of this mistake and provide a new proof of the Abel-Ruffini theorem.

1. INTRODUCTION

Abel-Ruffini theorem plays a vital role in solving algebraic polynomials in history. Notions like the Galois Theory and solvable group originated here. For a long time, people attempted to find the expression of the root by using the coefficient of radicals and finite field operations but failed. It was not until 1824 [1] that Niels Henrik Abel, a Norwegian mathematician, discovered the proof of the theorem. Galois’s proof published in 1846 [2] after his death. Vladimir Arnold found a topological proof of this theorem in 1963 [3].

A proof based on a theorem of Kronecker was given in the reference [4], and it was only using basic algebraic knowledge. Unfortunately, there is a mistake that exists in the proof. Our work points out the mistake and gives a fixed version by Theorem 4.2. Then we use a different way to provide a new proof of Theorem 4.3 and use it to prove the Abel-Ruffini theorem.

2. A MISTAKE

The mistake in [4] is derived from a paragraph on pages 123 to 124:

“Also, with each substituted radical of our series, which still does not allow division of \( f(x) \), we will also substitute at the same time the complex conjugate radical. Though this may be superfluous, it can certainly do no harm.”

We will use the field theory to prove that the assertion is wrong. Below we provide some definitions of conventions.

**Definition 2.1.** A field extension \( K \subset P \) is called a **radical extension** if there is a prime \( p, x^p - \alpha^p \in K[x] \) is irreducible over \( K \), and \( P = K(\alpha) \).

**Definition 2.2** ([5], Section 2). A field extension \( D_0 \subset D_k \) is said to be a **radical tower** over \( D_0 \) if there is a series of intermediate fields

\[
D_0 \subset D_1 \subset D_2 \subset \cdots \subset D_{l-1} \subset D_l \subset \cdots \subset D_k
\]

such that for each \( 0 \leq j \leq k - 1 \), \( u_{j+1} b_j \in D_j, D_{j+1} = D_j (u_{j+1}) \) where \( b_j \) is a prime, and \( x^{b_{j+1}} - u_{j+1} \) is irreducible over \( D_j \). For convenience, when \( c \in D_0 \), we also call \( D_0 \subset D_0(c) \) is a **radical tower** or a **trivial extension**.

2010 Mathematics Subject Classification. Primary 12E05, 12F15.

Key words and phrases. Abel-Ruffini, quintic polynomial, solvable in radicals.
Definition 2.3. We call \( f(x) \in D_0[x] \) is \textbf{solvable in radicals} over \( D_0 \) if all the roots of \( f(x) \) belong to \( D_k \), where \( D_0 \subseteq D_k \) is a radical tower. If we do not mention what \( D_0 \) is, that means \( D_0 \) is the smallest field containing all the coefficients of \( f(x) \).

The following is an example to illustrate the mistake in [4].

We set \( \theta = e^{2\pi i/5} \) and let \( f(x) = \prod_{j=1}^{5} (x - \theta^j - \theta^{-j}) \). Because \( x^{10} + x^9 + \cdots + 1 \) is irreducible over \( \mathbb{Q} \) and all its roots are \( \theta, \theta^2, \cdots, \theta^{10} \). We obtain

\[
f(x)^2 = \prod_{j=1}^{10} (x - \theta^j - \theta^{-j}) \in \mathbb{Q}[x].
\]

So we get \( f(x) \in \mathbb{Q}[x] \) and \( |\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| \leq 5 \). If \( |\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| = 1 \) or 2 from

\[
|\mathbb{Q}(\theta) : \mathbb{Q}(\theta + \frac{1}{\theta})||\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| = 10.
\]

When \( |\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| = 1 \) or 2, set \( \beta = \theta + \frac{1}{\theta} \), because \( \theta \) is a root of

\[
x^2 - \beta x + 1 = 0,
\]

we have

\[
|\mathbb{Q}(\theta) : \mathbb{Q}(\theta + \frac{1}{\theta})| \leq 2,
\]

and

\[
|\mathbb{Q}(\theta) : \mathbb{Q}(\theta + \frac{1}{\theta})||\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| \leq 4.
\]

We obtain 10 \( \leq 4 \). That is impossible. Thus \( |\mathbb{Q}(\theta + \frac{1}{\theta}) : \mathbb{Q}| = 5 \), and \( f(x) \) is irreducible over \( \mathbb{Q} \).

We follow [4], add \( e^{2\pi i/5} \) to \( \mathbb{Q} \). By Lemma 3.1, \( f(x) \) is irreducible over \( \mathbb{Q}(e^{2\pi i/5}) \). Since \( e^{2\pi i/5} = (e^{2\pi i/5})^{-1} \), for any \( t \in \mathbb{Q}(e^{2\pi i/5}) \), we have \( \sqrt{t} \in \mathbb{Q}(e^{2\pi i/5}) \). Then we add \( e^{2\pi i/5} \sqrt{2} \) to \( \mathbb{Q}(e^{2\pi i/5}) \). By Eisenstein’s criterion, \( x^{11} - 2 \) is irreducible over \( \mathbb{Q} \). By Lemma 3.1, \( x^{11} - 2 \) is irreducible over \( \mathbb{Q}(e^{2\pi i/5}) \). By Theorem 4.1, we can find a radical tower

\[
E = \mathbb{Q}(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}) \subset E_1 \subset E_2 \cdots \subset E_k = K_{11}^E,
\]

and \( E(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}) \subseteq K_{11}^E \). Now, we find a radical tower

\[
\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/5}) \subset \mathbb{Q}(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}) \subset E_1 \subset E_2 \cdots \subset E_k,
\]

all the roots of \( f(x) \) belong to \( E_k \), and \( f(x) \) is irreducible over \( \mathbb{Q}(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}) \).

According to the method in [4], we add \( e^{-2\pi i/5} \sqrt{2} \) to \( \mathbb{Q}(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}) \). In this time, we have

\[
\left( \frac{e^{2\pi i/5} \sqrt{2}}{e^{-2\pi i/5} \sqrt{2}} \right)^6 = e^{2\pi i/5} = e^{2\pi i} = \theta.
\]

Thus all the roots of \( f(x) \) belong to \( \mathbb{Q}(e^{2\pi i/5}, e^{2\pi i/5} \sqrt{2}, e^{-2\pi i/5} \sqrt{2}) \). That shows the proof in [4] is not working under our example.
3. Some Lemmas

Lemma 3.1. Suppose \( f(x), g(x) \in E[x] \) are irreducible over \( E \), \( \deg(f) \) is a prime. Set \( x_f \) be a root of \( f(x) \), and \( x_g \) be a root of \( g(x) \). If \( f(x) \) is not irreducible over \( E(x_g) \), we have \( \deg(f) \mid \deg(g) \).

Proof. We set \( p = \deg(f), q = \deg(g) \), thus
\[
|E(x_f)(x_g) : E(x_f) : E| = |E(x_g)(x_f) : E(x_g) : E|.
\]
If \( f(x) \) is not irreducible over \( E(x_g) \), then
\[
|E(x_f)(x_g) : E(x_f)| \leq q, |E(x_g)(x_f) : E(x_g)| < p,
\]
and
\[
|E(x_f) : E| = p, |E(x_g) : E| = q.
\]
Since \( p \) and \( q \) are both prime numbers, we have \( p \mid q \). \( \square \)

Lemma 3.2. Suppose \( f(x), g(x) \in E[x] \) are irreducible over \( E \), \( \deg(f) \) and \( \deg(g) \) are both prime numbers. Let all the roots of \( g(x) \) be \( x_1, x_2, \ldots, x_{\deg(g)} \), and \( x_g \) be a root of \( g(x) \). If \( f(x) \) is not irreducible over \( E(x_g) \), we have \( f(x) \) can be factored into linear factors over \( E(x_1, x_2, \ldots, x_{\deg(g)}) \).

Proof. If \( f(x) \) is not irreducible over \( E(x_g) \), then \( f(x) \) has the form
\[
f(x) = \varphi(x, x_g) \psi(x, x_g).
\]
Since \( g(x) \in E[x] \) is irreducible over \( E \) and \( f(x) \in E[x] \), then
\[
f(x) = \varphi(x, x_1) \psi(x, x_1),
f(x) = \varphi(x, x_2) \psi(x, x_2),
\]
\[
\ldots
f(x) = \varphi(x, x_{\deg(g)}) \psi(x, x_{\deg(g)}).
\]
Due to \( x_1, x_2, \cdots, x_{\deg} \) are all the roots of \( g(x) \), we obtain
\[
F(x) = \prod_{k=1}^{\deg(g)} \varphi(x, x_k) \in E[x].
\]
As all the roots of \( F(x) \) are the roots of \( f(x) \), and \( f(x) \) is irreducible over \( E \). We get
\[
F(x) = f(x)^h.
\]
Here the \( h \) is a positive integer. According to the above results, thus
\[
\deg(\varphi(x, x_g)) \cdot \deg(g) = h \cdot \deg(f).
\]
Because of \( \deg(f) \) and \( \deg(g) \) are both prime numbers, \( \deg(\varphi(x, x_g)) < \deg(f) \), we have
\[
\deg(\varphi(x, x_g)) = 1, \deg(f) = \deg(g), h = 1.
\]
That means \( f(x) \) can be factored into linear factors over \( E(x_1, x_2, \ldots, x_{\deg(g)}) \). \( \square \)

Lemma 3.3 (Abel). Let \( p \) be a prime. The polynomial \( x^p - C \in K[x] \) is not irreducible over \( K \), if and only if there is a \( d \in K \) and \( d^p = C \).

Proof. See page 118 of [4]. \( \square \)

Lemma 3.4. Let \( p \) be a prime, \( e^{2\pi i/p} \in K \), and \( x^p - C \in K[x] \). If \( x^p - C \) is not irreducible over \( K \), we get \( x^p - C \) can be factored into linear factors over \( K \). That is to say, if \( d \) is a root of \( x^p - C \), the extension \( K \subset K(d) \) is a \( p \)th radical extension or a trivial extension.
Proof. By Lemma 3.3, if \( x^p - C \in K[x] \) is not irreducible over \( K \), there is a \( d \) belongs to \( K \), \( d^p = C \). So we get

\[
x^p - C = (x - d)(x - de^{\frac{2\pi i}{p}}) \cdots (x - de^{\frac{2\pi i(p-1)}{p}}).
\]

That means \( x^p - C \) can be factored into linear factors over \( K \). Thus \( K \subseteq K(d) \) is a trivial extension.

If \( x^p - C \in K[x] \) is irreducible over \( K \), by Definition 2.1, \( K \subset K(d) \) is a \( p \)th radical extension.

\[\square\]

Lemma 3.5. Let \( p \geq 3 \) be an integer and \( K \) be a field. For any prime \( q \leq p \), the \( q \)th root \( e^{\frac{2\pi i}{q}} \) belongs to \( K \). We set \( a^p = A \in K \), then \( K \subseteq K(a) \) is a radical tower.

Proof. Let \( p_0 = 1 \). We can find primes \( p_1, p_2, \ldots, p_k \), \( \prod_{j=1}^{k} p_j = p \). Then we have

\[
K(((\cdots (a^{p_j})^{p_{j-1}})\cdots )^{p_1}) \subseteq K(((\cdots (a^{p_{j-1}})^{p_{j-1}})\cdots )^{p_1}) \subseteq \cdots \subseteq K((a^{p_j})^{p_1}) \subseteq K(a^{p_j}).
\]

By Lemma 3.4, for each \( 1 \leq j \leq k \), the extension

\[
K(((\cdots (a^{p_{j-1}})^{p_{j-1}})\cdots )^{p_1}) \subseteq K(((\cdots (a^{p_j})^{p_{j-1}})\cdots )^{p_1})
\]

is a trivial extension or a radical extension, so that \( K \subseteq K(a) \) is a radical tower. \[\square\]

4. A New Proof

Theorem 4.1. Let \( q \geq 3 \) be a prime and \( E \) be a field. We have the extension \( E \subseteq K_q^E \) is a radical tower, and this radical tower follows \( E = E_0 = K_q^E \supseteq E(e^{\frac{2\pi i}{q}}, e^{\frac{2\pi i}{2}}, \ldots, e^{\frac{2\pi i}{p}}) \) or

\[
E = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k = K_q^E \supseteq E(e^{\frac{2\pi i}{q}}, e^{\frac{2\pi i}{2}}, \ldots, e^{\frac{2\pi i}{p}})
\]

such that for each \( 0 \leq j \leq k - 1 \), \( d_j = e^{\frac{2\pi i}{q}} \in E_j \), \( E_{j+1} = E_j(d_{j+1}) \) where \( q_j \) is a prime, and \( x^{q_j} - d_j \) is irreducible over \( E_j \).

Proof. Let us use mathematical induction to prove this proposition.

When \( n = 3 \), due to \( e^{\frac{2\pi i}{3}} \) is a root of \( x^2 + x + 1 \). Thus \( E \subseteq E(e^{\frac{2\pi i}{3}}) \) is a radical extension or a trivial extension. Then we set \( K_3^E = E(e^{\frac{2\pi i}{3}}) \).

Let \( p \) be a prime, and \( 5 \leq p \leq q \). Suppose for any prime \( n < p \), the proposition is true. We need to prove when \( n = p \), the proposition is true. We set \( m(p) = \max\{n < p : n \text{ is a prime}\} \). By Lemma 3.3 and \( (e^{\frac{2\pi i}{p}})^{p-1} = 1 \), we get \( K_{m(p)}^E \subseteq K_{m(p)}^E(e^{\frac{2\pi i}{p-1}}) \) is a radical tower. Let \( \omega = e^{\frac{2\pi i}{p}} \), \( \varepsilon_j = e^{\frac{2\pi i}{p}} \), and \( \omega^n = \omega^{2n} \). We set Lagrange resolvent

\[
\rho(\theta, \varepsilon_j) = \theta 2^0 + \varepsilon_j \theta 2^1 + \varepsilon_j^2 \theta 2^2 + \cdots + \varepsilon_j^{p-2} \theta 2^{p-2}.
\]

Thus we have

\[
\rho(\omega^n, \varepsilon_j) = \omega^{n+0} + \varepsilon_j \omega^{n+1} + \varepsilon_j^2 \omega^{n+2} + \cdots + \varepsilon_j^{p-2} \omega^{n+p-2}
\]

and

\[
\rho(\omega^n, \varepsilon_j) = \varepsilon_j^{-n} \rho(\omega^0, \varepsilon_j).
\]

Then we get

\[
A_j = (\rho(\omega^0, \varepsilon_j))^{p-1} = \varepsilon_j^{\frac{(p-1)(p-2)}{2}} \prod_{n=0}^{p-2} \rho(\omega^n, \varepsilon_j) \in K_{m(p)}^E(e^{\frac{2\pi i}{p-1}}).
\]
By Lemma 3.5 we can get $\rho(\omega^{[0]}, \varepsilon_1)$, and $\rho(\omega^{[0]}, \varepsilon_2), \ldots, \rho(\omega^{[0]}, \varepsilon_{p-1})$ by radical tower. Since we have
\[
\sum_{j=1}^{p-1} \varepsilon_j = 0, \sum_{j=1}^{p-1} \varepsilon_j^2 = 0, \ldots, \sum_{j=1}^{p-1} \varepsilon_j^{p-2} = 0.
\]
Thus we get
\[
\omega = \omega^{[0]} = \frac{1}{p-1} \sum_{j=1}^{p-1} \rho(\omega^{[0]}, \varepsilon_j).
\]
Now we find a radical tower $K^E_{m(p)} \subseteq K$, $e^{2\pi i \varepsilon} \in K$. Then we set $K^E_{p} = K$. That means when $n = p$, the proposition is true. \hfill \Box

**Corollary 4.1** (Gauss). The polynomial $x^p - 1$ is solvable in radicals.

**Proof.** Let $q$ be the minimum prime greater than $p$. By Theorem 4.1 and Lemma 3.5 we obtain $\mathbb{Q} \subseteq K^q(e^{2\pi i \varepsilon})$ is a radical tower. \hfill \Box

**Corollary 4.2.** Let $F$ be a field and $f(x) \in F[x]$. If all the roots of $f(x)$ belong to $F$, then
\[
F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{n-1} \subseteq F_n
\]
such that for each $0 \leq j \leq n - 1$, $u_j \in F_j$, $b_j \in \mathbb{N}_+$, and $F_{j+1} = F_j(u_{j+1})$. We have $f(x)$ is solvable in radicals.

**Proof.** Suppose $q = \max\{b_j\}$. By Theorem 4.1 we can find a radical tower
\[
F = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k \supseteq E(e^{2\pi i \varepsilon}, e^{\frac{2\pi i}{p}}, \ldots, e^{\frac{2\pi i}{q}}).
\]
By Lemma 3.4 and Lemma 3.5 we add $u_1, u_2, \ldots, u_n$ to $E_k$, and ignore the trivial extensions. Then we get a new radical tower $F = E_0 \subseteq E_0 = F_0$ or
\[
F = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k \cdot \cdots \cdot \subset E_d \supseteq F_n
\]
such that for each $0 \leq j \leq d - 1$, $e^{\frac{2\pi i}{p_j+1}}, a_{j+1} \in E_j$, $E_{j+1} = E_j(a_{j+1})$ where $p_j$ is a prime, and $x^{p_j+1} - a_{j+1}$ is irreducible over $E_j$. \hfill \Box

**Theorem 4.2.** Let $E$ be a field, and for any $t \in E$, $\mathcal{T} \in E$. Suppose $f(x) \in E[x]$ is irreducible over $E$ and has an odd prime degree $p$. If $f(x)$ is solvable in radicals over $E$, we can find a radical tower $E \subseteq K$, $e^{2\pi i \varepsilon} \in K$, and for any $t \in K$, we have $\mathcal{T} \in K$. In there, $f(x)$ is irreducible over $K$ but not irreducible over $K(\alpha)$, $K \subseteq K(\alpha)$ is a radical extension.

**Proof.** According to $f(x)$ is solvable in radicals over $E$, we can find a radical tower
\[
E = D_0 \subset D_1 \subset D_2 \subset \cdots \subset D_{l-1} \subset D_l \subset \cdots \subset D_m
\]
such that for each $0 \leq j \leq m - 1$, $D_{j+1} = D_j(u_{j+1})$ where $b_j$ is a prime, and $x^{b_j+1} - u_{j+1} \in D_j$ is irreducible over $D_j$.

Suppose $q = \max\{b_j, p\}$. By Theorem 4.1 we have a radical tower
\[
E = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k \supseteq E(e^{2\pi i \varepsilon}, e^{\frac{2\pi i}{p}}, \ldots, e^{\frac{2\pi i}{q}}).
\]
By Lemma 3.4 we add $u_1, u_2, \ldots, u_m$ to $K_p$, and ignore the trivial extensions. We get a new radical tower
\[
E = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k \cdot \cdots \cdot \subset E_d
\]
such that for each $0 \leq j \leq d - 1$, $e^{\frac{2\pi i}{p_j+1}}, a_{j+1} \in E_j$, $E_{j+1} = E_j(a_{j+1})$ where $p_j$ is a prime, and $x^{p_j+1} - a_{j+1}$ is irreducible over $E_j$. \hfill \Box
By Lemma 3.1 and \(e^{\frac{2\pi i}{p}} \in E_j\), if we ignore the trivial extensions in
\[E = E_0 \subseteq E_1 \subseteq E_1' \subseteq E_2 \subseteq E_2' \subseteq \cdots \subseteq E_k \subseteq E_k' \subseteq \cdots \subseteq E_d \subseteq E_d',\]
such that for each \(1 \leq j \leq d\), \(E_j' = E_j(\overline{\alpha})\). We get \(E \subseteq E_d'\) is a radical tower, for any 
\(t \in E_d',\) we have \(\overline{t} \in E_d\), and \(x_1, x_2, \cdots, x_p, e^{\frac{2\pi i}{p}} \in E_d'.\) We set this radical tower is
\[E = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_k \subseteq F_g,\]
such that for each \(0 \leq j \leq g - 1\), \(e^{\frac{2\pi i}{p_j^1}} \in F_j, \overline{h}_{j+1}^{j+1} \in F_j, (F_{g+1} = F_g), F_{j+1} = F_j(h_{j+1})\) \(\) where \(q_j\) is a prime, and \(x^{q_j-1} - h_{j+1}^{j+1}\) is irreducible over \(F_j\).
Because of all the roots of \(f(x)\) belong to \(F_g\). By Lemma 3.4, we can find a \(j_0\), and \(f(x)\) is irreducible over \(F_{j_0}\), but \(f(x)\) is not irreducible over \(F_{j_0}(h_{j_0+1})\).

If for any \(t \in F_{j_0}, \overline{t} \in F_{j_0},\) we set \(\alpha = h_{j_0+1}\) and \(K = F_{j_0}.\) Else we consider this extension
\[F_{j_0} \subseteq F_{j_0}(h_{j_0+1}, \overline{h}_{j_0+1}) \subseteq F_{j_0}(h_{j_0+1}, h_{j_0+1}, h_{j_0+1}) = F_{j_0}(h_{j_0+1}, h_{j_0+1}, h_{j_0+1}).\]

If \(f(x)\) is irreducible over \(F_{j_0}(h_{j_0+1}, h_{j_0+1}, h_{j_0+1})\), we set \(\alpha = h_{j_0+1}\) and \(K = F_{j_0}(h_{j_0+1}, h_{j_0+1}).\) If \(f(x)\) is not irreducible over \(F_{j_0}(h_{j_0+1}, h_{j_0+1}, h_{j_0+1})\), we set \(\alpha = h_{j_0+1}, h_{j_0+1}, h_{j_0+1}\) and \(K = F_{j_0}.\)

**Remark 4.1.** Theorem 4.2 shows a correct way to add “the complex conjugate radical” and this way gives a fix to the mistake in [4].

**Theorem 4.3 (Kronecker).** Let \(E\) be a field, and for any \(t \in E, \overline{t} \in E.\) Suppose \(f(x) \in E[x]\) is irreducible over \(E\) and has a prime degree \(p \geq 3.\) If \(f(x)\) is solvable in radicals over \(E\) and has a pair of complex conjugate roots, then \(f(x)\) only has one real root.

**Proof.** By Theorem 4.2, there is a radical tower \(E \subseteq K, \) and \(e^{\frac{2\pi i}{p}} \in K\). We have \(f(x)\) is irreducible over \(K, \) but \(f(x)\) is not irreducible over \(K(\alpha)\). In there, \(q\) is a prime, \(\alpha\) is a root of \(x^q - \alpha^q \in K[x], \) and \(x^q - \alpha^q\) is irreducible over \(K.\) By Lemma 3.1, we get \(q = p.\)

By Lemma 3.4, \(x^2 - \alpha^p\) is not irreducible over \(K(\alpha).\) By Lemma 3.2 \(f(x)\) can be factored into linear factors over \(K(\alpha)\). So we have
\[x_j = \sum_{t=0}^{p-1} w_t(\alpha e^{\frac{2\pi i}{p}})^t, (w_t \in K, j = 1, 2, \cdots, p).\]

In there, for any \(k \in \mathbb{Z},\) we have \(x_k = x_{k'}, 1 \leq k' \leq p, \) and \(k \equiv k' \mod p.\) Since \(f(x)\) has a pair of complex conjugate roots, we set they are \(x_f, x_g.\) Thus \(x_g = \overline{x_f}.\) We get
\[\sum_{t=0}^{p-1} w_t\left(\alpha e^{\frac{2\pi i}{p}}\right)^t = \sum_{t=0}^{p-1} \overline{w_t}\left(\overline{\alpha} e^{-\frac{2\pi i}{p}}\right)^t.\]

We have two cases.

**CASE I.** When \(\alpha \in \mathbb{R},\) By Equation 4.1, we have
\[\sum_{t=0}^{p-1} \left(w_t e^{\frac{2\pi i}{p}}\right)^t = \sum_{t=0}^{p-1} \left(\overline{w_t} e^{-\frac{2\pi i}{p}}\right)^t = \left(\sum_{t=0}^{p-1} \left(w_t e^{\frac{2\pi i}{p}}\right)^t\right)^{\alpha}.\]

Since \(x^p - \alpha^p \in K[x]\) is irreducible over \(K, \) and \(e^{\frac{2\pi i}{p}}, w_t, \overline{w_t} \in K.\) We can change the \(\alpha\) in Equation 4.2 to \(\alpha e^{\frac{2\pi i}{p}}\) for any \(j \in \{1, 2, \cdots, p\}.\) Thus for each \(1 \leq j \leq p,\) the following formula holds
\[x_{g+j} = \overline{x_{f-j}}.\]
When $g + j \equiv l - j \mod p$, we get $j \equiv \frac{l - g}{p} \mod p$. Since $f(x)$ is irreducible over $E$, thus it does not have repeated roots. We have $x_k = x_d$ if and only if $k \equiv d \mod p$. By Equation (4.3) we get $f(x)$ has exactly one real root.

CASE II. When $\alpha \notin \mathbb{R}$, we set $\beta = \alpha \overline{\alpha} = (\alpha e^{\frac{2\pi i}{p}})(\overline{\alpha} e^{-\frac{2\pi i}{p}})$. If $f(x)$ is not irreducible over $K(\beta)$, this will give us the situation of Case I. If $f(x)$ is irreducible over $K(\beta)$, we get $x^p - \alpha^p \in K(\beta)[x]$ is irreducible over $K(\beta)$. Otherwise, by Lemma 3.3, we have $\alpha, e^{\frac{2\pi i}{p}} \in K(\beta)$. That means $f(x)$ is not irreducible over $K(\beta) \supseteq K(\alpha)$, which contradicts our premise. By Equation (4.1) we have

$$
\sum_{t=0}^{p-1} \left( w_t e^{\frac{2\pi i t}{p}} \right) \alpha^t = \sum_{t=0}^{p-1} \left( \overline{w_t} e^{-\frac{2\pi i t}{p}} \beta^t \right) \left( \frac{1}{\alpha} \right)^t.
$$

Since $x^p - \alpha^p \in K(\beta)[x]$ is irreducible over $K(\beta)$, and $e^{\frac{2\pi i}{p}}, w_t, \overline{w_t} \in K(\beta)$. We can change the $\alpha$ in Equation (4.4) to $\alpha e^{\frac{2\pi i}{p}}$ for any $j \in \{1, 2, \cdots, p\}$. Thus for each $1 \leq j \leq p$, the following formula holds

$$
x_{g+j} = \overline{x_{l+j}}.
$$

By Equation (4.5) for each $1 \leq j \leq p$, we have

$$
x_{l+j} = x_{l+(l-g)+j} = x_{l+2(l-g)+j} = x_{l+3(l-g)+j} = \cdots = x_{l+(p-1)(l-g)+j} = x_{l+p(l-g)+j} = x_{l+j}.
$$

It follows that $f(x)$ only has real roots, but this contradicts our premise. \hfill \Box

**Theorem 4.4 (Abel-Ruffini).** The general quintic polynomial is not solvable in radicals.

**Proof.** Set $f(x) = x^5 - 10x + 5$. Thus $x^5 - 10x + 5$ has exactly three real roots. By Eisenstein’s criterion, $x^5 - 10x + 5$ is irreducible over $\mathbb{Q}$. According to the Theorem 4.3, $x^5 - 10x + 5$ is not solvable in radicals. \hfill \Box

5. Conclusions

We give a new proof of the Abel-Ruffini theorem and strengthen the version of the Kronecker theorem (see Proposition 3 in [4]). Moreover, we provide a corrected version of the mistake in [4] and show a short proof of Corollary 4.1 that does not use group theory.

**REFERENCES**

[1] Niels Henrik Abel, Mémoire sur les équations algébriques: où on démontre l’impossibilité de la résolution de l’équation générale du cinquième degré, Librarian, Faculty of Science, University of Oslo, 1824.

[2] E Galois, Sur les conditions de résolubilité des équations par radicaux, Journal de mathématiques pures et appliquées 11 (1846), 417–444.

[3] Valerij Borisovič Alekseev, Abels theorem in problems and solutions: Based on the lectures of professor vi arnold, Springer Science & Business Media, 2004.

[4] Heinrich Dörrie, 100 great problems of elementary mathematics: Their history and solution, ch. 25, pp. 116–127, Courier Corporation, 1965.

[5] Michael I Rosen, Niels hendrik abel and equations of the fifth degree, The American mathematical monthly 102 (1995), no. 6, 495–505.

**DEPARTMENT OF MATHEMATICS, HENAN INSTITUTE OF SCIENCE AND TECHNOLOGY, XINXIANG CITY, CHINA 453003**

**E-mail address:** ypan@stu.hist.edu.cn

**DEPARTMENT OF MATHEMATICS, HENAN INSTITUTE OF SCIENCE AND TECHNOLOGY, XINXIANG CITY, CHINA 453003**

**E-mail address:** chenyuzhenjg@nuaa.edu.cn