Proceedings of the 2nd International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2023)
DOI: 10.54254/2753-8818/5/20230277

Reducibility of quartic polynomials and its relation to Galois groups

Jinhe Huang[1,*], Yicheng Ai[2], Yuhao Wen[3]

[1]The Experimental High School Attached to Beijing Normal University, Beijing, 100032, China
[2]Tsinglan School, Dongguan, 523808, China
[3]Department of Mathematics, University of London, WC1E 6 bt, China

*Corresponding author email: yanhuangheshi@163.com

Abstract. This paper deals with special classes of quartic polynomials and properties pertaining to their Galois groups and reducibility over certain fields. The existence of quartic polynomials irreducible over Q but reducible over every prime field is first proven, after which criteria are established for the Galois group of polynomials with this property. By constructing classes of V_4-generic polynomials and comparing them with criteria put forth in previous studies for determining polynomials with this property, it can be shown that a polynomial of the biquadratic form $x^4 + ax^2 + b$ has this property if and only if it can be written as $\boldsymbol{x^4 - 2(u+v)x^2 + (u-v)^2}$ with u, v $\in \mathbb{Q}$ such that none of u, v, or uv can be expressed as ratio of two squares, and $2(u+v), (u-v)^2 \in \mathbb{Z}$. The general form for biquadratic polynomials irreducible over $\mathbb{Q}$ and reducible modulo every integer n is found to have a general form similar to this one.

Keywords: quartic polynomials, Galois groups, math.

1. Introduction

The relation between polynomials has been an interesting topic for mathematicians in the past few decades.

Several previous studies focused on how to represent groups such as S_n and A_n as Galois groups of polynomials [1-3], and others tried to find out properties about these polynomials [4]. Among these studies, we found that the reducibility of quartic polynomials is especially appropriate for us to investigate. Both Rotman and Driver et. al included this topic in their researches [5-6]. This paper aims to review some important properties of quartic polynomials and open up room for further exploration.

We expand on problems put forward in the textbooks of Rotman as well as Dummit and Foote about classifying the family of quartic polynomials that are reducible in all prime fields [5,7]. Additionally, we address the question of constructing a generic polynomial for a given Galois group - something which is of high relevance to the inverse Galois problem.

2. Polynomials reducible modulo every prime p

The topic of polynomials irreducible over $\mathbb{Q}$ but reducible modulo every prime number p is a recurring concept in textbooks of Galois Theory: the works of Dummit and Foote, Milne[8], and Rotman have all

DOI: 10.54254/2753-8818/5/20230277

touched on and discussed its properties. For convenience, we shall call polynomials with this property *hollow*[1]in *p*.

Example 2.1 $f(x) = x^4 + 1$

It can be shown, by forming equations from the coefficients of the potential factorizations of f(x), that there exists no factorization of f(x) in $\mathbb{Q}$. We can also use Eisenstein's criterion after the substitution $x \rightarrow x + 1$ to examine this result.

Now consider f(x) over a finite field $\mathbb{Z}_p$, where p is a prime. We wish to check if f(x) is reducible in $(\mathbb{Z}/p\mathbb{Z})[x]$ for every prime p:

$$x^4 + 1 \mod p$$

Proof 2.1 It can be easily seen that, for p = 2,

$$x^4 + 1 \equiv (x + 1)^4 \mod 2$$

But for p >2, it is more difficult to find a factor for f(x). To further show this, we must rely on the Legendre symbol, which is defined for some integer α coprime to as

$$\begin{cases} \left(\frac{\alpha}{p}\right) = 1 \ if \ \alpha \equiv X^2 \mod p \\ \left(\frac{\alpha}{p}\right) = -1 \ if \ \alpha \not\equiv X^2 \mod p \end{cases} \quad \text{for } X \in \mathbb{Z}_P$$

Lemma 2.2 Supplement 1 to the Law of Quadratic Reciprocity [9]

$$\left(\frac{-1}{P}\right) = \begin{cases} 1, & if \ p \equiv 1 \mod 4 \\ -1, & if \ p \equiv 3 \mod 4 \end{cases}$$

Proof 2.2 This is a simple consequence of Euler's Criterion, which states that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

The result directly follows from this.

Lemma 2.3 Supplement 2 to the Law of Quadratic Reciprocity [9]

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & if \ p \equiv 1 \ or \ -1 \mod 8 \\ -1, & if \ p \equiv 3 \ or \ -3 \mod 8 \end{cases}$$

Proof 2.3 The proof for this is slightly lengthier: denote X to be

$$exp\left(\frac{\pi i}{4}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$X^4 = -1 \Rightarrow X^{-1} = -X^3 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

$$Let \ G = X + X^{-1} = X - X^{-3} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} = \sqrt{2}$$

G can therefore be thought of as the integer, if it exists, such that

$$G^2 \equiv 2 \mod p$$

Consider $G^p = X^p + X^{-p} \mod p$. Since $X^8 = (X^{-1})^8 = 1$, if $p \equiv 1$ or $-1 \mod 8$, then

$$X^P + X^{-P} = X + X^{-1} = G$$

if $p \equiv 3$ *or* $-3 \mod 8$, then

[1]We have not taken this coinage from any previous work: we came up with it here for conciseness

DOI: 10.54254/2753-8818/5/20230277

$$X^P + X^{-P} = X^3 + X^{-3} = -X^{-1} - X = -G$$

This implies

$$G^p \equiv -1^{\frac{p^2-1}{8}} G \quad mod \ p$$

At the same time,

$$G^p = G^{p-1}G = (G^2)^{\frac{P-1}{2}} G = 2^{\frac{P-1}{2}} G \equiv \left(\frac{2}{P}\right) G \quad mod \ p$$

Combining the two above equations, we can get

$$-1^{\frac{p^2-1}{8}} G \equiv \left(\frac{2}{p}\right) G \quad mod \ p$$

$$-1^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right)$$

which is what we want.

Remark 2.4 For Legendre symbols, the property $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ holds.

This implies $\left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right)$,

where $\left(\frac{-2}{p}\right) = 1$ if either $\left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = 1 \ or \ \left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = -1$

The first case holds if p ≡ 1 mod 4 and p ≡ 1 or −1 mod 8, so it is true when

$$p \equiv 1 \quad \text{mod } 8$$

The second case holds if p ≡ 3 mod 4 and p ≡ 3 or −3 mod 8, so it is true when

$$p \equiv 3 \quad \text{mod } 8$$

Going back to x^4+1 mod p, we now see that we can consider three possible cases based on the possible modular values of p:

(i) p ≡ 1 **or** −1 mod 8 ∃α :$\alpha^2 = 2$, then
$x^4+1 \equiv x^4+2x^2+1-2x^2 \equiv (x^2+1)^2-\alpha^2 \equiv (x^2-\alpha+1)(x^2+\alpha+1)$ mod p

(ii) p ≡ 3 mod 8 ∃α :$\alpha^2 = -2$, then
$x^4+1 \equiv x^4-2x^2+1+2x^2 \equiv (x^2-1)^2-\alpha^2 \equiv (x^2-\alpha-1)(x^2+\alpha-1)$ mod p

(iii) p ≡ 1 mod 4 ∃α :$\alpha^2 = -1$, then $x^4 + 1 \equiv x^4 - (\alpha^2) \equiv (x^2-\alpha)(x^2+\alpha)$ mod p

It should be obvious that every odd prime p will fall into one of the categories listed above. Therefore, we have shown that f(x) is reducible modulo every prime.

Using the same approach, it follows that $g(x) = x^4 + \gamma^4$ for some $\gamma \in \mathbb{Z}$ are hollow, but can we classify any other such polynomials besides g(x)? Let us exclusively examine hollow polynomials of degree 4.

Example 2.5 [2] Determine whether $f(x) = x^4 - 10x^2 + 1$ is hollow.

We notice that the coefficient of the x^3 and x terms are 0, meaning we can f(x) as either

$$(x-a)(x^3 + ax^2 + bx + ab),$$

or

$$(x^2-ax + b)(x^2 + ax + b), a,b \in \mathbb{Q}$$

In the first case, we obtain

[2] This approach is borrowed from Rotman's textbook [5], which shows the 'hollowness' of this exact polynomial in Example 26, p.66 as does Dummit and Foote [7]

DOI: 10.54254/2753-8818/5/20230277

$$10 = a^2 - b,$$

$$a^2 b = -1,$$

solving for which gives us $b^2 + 10b + 1 = 0$, from which we can see that b is not rational. Likewise, in the second case we find that

$$b^2 = 1,$$

$$a^2 - 2b = 10,$$

and a is not rational, meaning $f(x)$ is irreducible.

For factorization modulo p, we first complete the square;

$$f(x) = (x^2 - 5)^2 - 24$$

we now focus on the square root of 24, which is $2\sqrt{6}$. We write this as 2m, where m is the integer such that $m^2 \cong 6 \bmod p$: for p such that m is solvable, $f(x)$ can be factorized as $(x^2 - 5 + 2m)(x^2 - 5 - 2m)$.

For p such that m has no solution in $\mathbb{Z}p$, we try the next approach and try to find an element $j + km$ in the field extension $\mathbb{Z}p[m]$ such that $5+2m = (j+km)^2$. Lining up the coefficients gives us

$$j^2 + 6k^2 = 5,$$

$$jk = 1.$$

From this we note that $k = j^{-1}$, and that the resultant equation
$j^4 - 5j^2 + 6 \rightarrow (j^2 - 2)(j^2 - 3)$, must have a solution, for if

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = -1$$

then $\left(\frac{6}{p}\right) = 1$. We notice that, since $(j + j^{-1}m)^2 = 5 + 2m$, $(j - j^{-1}m)^2 = 5 - 2m$, and we write $(x^2 - 5 + 2m)(x^2 - 5 - 2m)$ as

$(x^2 - (j - j^{-1}m)^2)(x^2 - (j + j^{-1}m)^2)$
$\rightarrow ((x-j) + j^{-1}m)((x + j) - j^{-1}m)((x - j) - j^{-1}m)((x + j) + j^{-1}m)$
$\rightarrow ((x-j) + j^{-1}m)((x - j) - j^{-1}m)((x + j) + j^{-1}m)((x + j) - j^{-1}m)$
$\rightarrow ((x-j)^2 - 6j^{-1})((x + j)^2 - 6j^{-1})$
and we are done.

Theorem 2.6 (Dedekind) [3] Let f(x) be a polynomial over $\mathbb{Z}[x]$ with Galois group G and a factorization modulo some prime p

$$f(x) = \prod_{i=1}^{j} h_i(x) \quad mod\ p$$

where each $h_i(x)$ is a distinct, irreducible, monic factor such that

$$\sum_{i=1}^{j} deg\ (h_i) = deg\ (f)$$

Then G must contain a cycle of type:
$(\deg(h_1),\deg(h_2),...,\deg(h_j))$

Remark 2.7 An irreducible quartic polynomial is hollow if and only if it has the Galois groups V_4 or A_4

[3] See [1] Conrad Section 3 for a complete proof of this theorem.

DOI: 10.54254/2753-8818/5/20230277

Proof 2.4 It follows from Dedekind's Theorem (2.6) that a polynomial of degree n has an n-cycle in its Galois group if and only if it is irreducible for some prime p. This means we can say that an irreducible polynomial is reducible modulo every prime p if and only if it has no n-cycle in its Galois group. However, a polynomial with a Galois group that is not transitive [4]in S_n must be reducible([6], Theorem 2.9, pg.3). In the case of quartic polynomials, the only transitive subgroups of S_4 that satisfy this condition are V_4 and A_4.

3. Biquadratic polynomials and the V_4 group

3.1. Irreducible polynomials with Galois group V_4

In the following section we will consider hollow polynomials with Galois group V_4.

Definition 3.1 Define the minimal polynomial a(x) of α ∈ E/F for some Galois extension E/F as the unique, irreducible monic polynomial with Galois group

Gal(E/F). This is given by

$$\alpha(x) = \prod_{\sigma \in Gal(E/F)} (x - \sigma(\alpha))$$

when the stabilizer group of the Galois action Stab(α) = 1. Alternately, we define the minimal polynomial of α as

$$\alpha(x) = \prod_{\sigma \in G/S} (x - \sigma(\alpha))$$

where G = Gal(E/F) and S = Stab(α)

Example 3.2 Find the minimal polynomial of the element α = 5 $\sqrt{6}$ in the extension E/F = $\mathbb{Q}$ ($\sqrt{2}$, $\sqrt{3}$). We have $\mathbb{Q}$($\sqrt{2}$,$\sqrt{3}$) = $\mathbb{Q}$ ($\sqrt{2}$) ×$\mathbb{Q}$ ($\sqrt{3}$)), so Gal(E/F) ≅V_4.

Examining the Galois action δ(α), δ∈ Gal(E/F), we see that |Stab(α) = 2| and Orb(α) = {α,−α}. The minimal polynomial is then given by

$$a(x) = (x - 5\sqrt{6})(x + 5\sqrt{6}) = x^2 - 150.$$

As we can see, although α is an element of E/F where Gal(E/F) ≅ V_4, its minimal polynomial is not quartic and therefore does not have Galois group V_4. We gather that the degree of the minimal extension is determined by the cardinality of its stabilizer group and that an element α in E/F has Galois group equal to Gal(E/F)if and only if it has a trivial stabilizer group under the action of the group Gal(E/F). In other words, it holds if α is not fixed by any non-trivial automorphism of E/F.

We now consider when Gal(E/F) ≅ V_4:

Lemma 3.3 The Galois extension E/F = $\mathbb{Q}(\sqrt{j}, \sqrt{k})$ is equivalent to $\mathbb{Q}$ ($\sqrt{j}$+$\sqrt{k}$)

Proof 3.1 Define j and k as distinct, square-free[5] j,k/ ∉ $\mathbb{Q}$) Let G = Gal(E/F); it can be shown that G≅V_4. Let K denote the intermediate field F ⊂ K ⊂E generated by$\sqrt{j}$+$\sqrt{k}$. Then the Galois group of the extension E/K is, by definition, the group of automorphisms of E/K fixing K. Since E^{FK}, Gal(E/K)(E/F). We see that since the three non-trivial elements of Gal(E/F) respectively fix$\sqrt{j}$, $\sqrt{k}$, and $\sqrt{jk}$, no element fixes $\sqrt{j}$+$\sqrt{k}$. Therefore |Gal(E/K)| = |Aut(E/K)| = 1. By the Fundamental Theorem of Galois Theory, we have

$$E^{Gal(E/F)} = K \to E = K$$

It follows that$\sqrt{j}$+$\sqrt{k}$ is a primitive element of E/F, so, as desired, $\mathbb{Q}$ ($\sqrt{j}$, $\sqrt{k}$) ≅ $\mathbb{Q}$ ($\sqrt{j}$+$\sqrt{k}$).

[4] A subgroup E of S_n, the permutation group of the set N, is transitive if, $\exists \sigma \in E$ such that $\sigma(n_1) = n_2$, $\forall n_1, n_2 \in N$

[5] Define an integer to be square-free if it is not divisible by any square other than 1

DOI: 10.54254/2753-8818/5/20230277

Corollary 3.4 We can express an element in the extension generated by$\sqrt{j}$+$\sqrt{k}$ as $a\sqrt{j}$+$b\sqrt{k}$, where j and k are distinct square free integers, not necessarily

positive, and a,b$\in\mathbb{Q}$.

Remark 3.5 We further apply the argument presented in Lemma 3.3 to elements in E/F of the form l+ $\sqrt{j}$+$\sqrt{k}$ + $\sqrt{jk}$, and show that this too is a primitive element of E/F. Note that the dimension of the extension is 4, also the number of basis vectors in this element. It follows that every element in the extension E/F where Gal(E/F) ≅ V_4 can be written in the form a + $b\sqrt{j}$+$c\sqrt{k}$ + $d\sqrt{jk}$, where a,b,c,d$\in$ $\mathbb{Q}$. The same condition from Corollary 3.4 applies for j,k, and jk. Noting that we do not necessarily need jkto be square free, as that would restrict j and k to be co-prime.

We are now able to use this result to find the V_4-generic class of irreducible polynomials.

Theorem 3.6 If a polynomial is irreducible over Q and has Galois group V_4, then it can be written in the form

$$\prod_{\sigma\in G/S}(x-\sigma(a+b\sqrt{j}+c\sqrt{k}+d\sqrt{jk}))$$

or, written out,

$$\left(x-\left(a+b\sqrt{j}+c\sqrt{k}+d\sqrt{jk}\right)\right)(x-\left(a+b\sqrt{j}-c\sqrt{k}-d\sqrt{jk}\right))$$

$$\left(x-\left(a-b\sqrt{j}+c\sqrt{k}-d\sqrt{jk}\right)\right)(x-\left(a-b\sqrt{j}-c\sqrt{k}+d\sqrt{jk}\right))$$

We will not provide the fully expanded form due to its being too intricate[6], but it can be shown that the coefficient of the x^3 term is −4a. By setting a to 0, we instead consider all reduced quartic polynomials, and have removed one parameter from the expression, giving

$$\left(x-\left(b\sqrt{j}+c\sqrt{k}+d\sqrt{jk}\right)\right)(x-\left(b\sqrt{j}-c\sqrt{k}-d\sqrt{jk}\right))$$

$$\left(x-\left(-b\sqrt{j}+c\sqrt{k}-d\sqrt{jk}\right)\right)(x-\left(-b\sqrt{j}-c\sqrt{k}+d\sqrt{jk}\right))$$

This, too, cannot be easily manipulated. In the next theorem, we shall only consider two parameters.

Definition 3.7 Define a quartic polynomial to be ”biquadratic” if it can be written as

$$x^4+\text{a}\,x^2+\text{b}$$

for some a,b$\in\mathbb{Q}$.

Theorem 3.8 A biquadratic polynomial p(x) is irreducible in Q and has Galois group V_4 if and if only if it can be written in the form

$$x^4-2(u+v)x^2+(u-v)^2 \tag{3.1}$$

where u and v are distinct rationals such that none of u, v or uvcan be written as a ratio of two squares.

Proof 3.2 Let us set one of b,c, or d to 0. There are now no simpler polynomials that we can construct, as removing any more parameters will result in a non-trivial stabilizer group. We now have either

$$\alpha=\sqrt{b^2j}+\sqrt{c^2k},$$

$$\alpha=\sqrt{c^2k}+\sqrt{d^2jk},$$

Or

[6] The reader may check these via WolframAlpha

DOI: 10.54254/2753-8818/5/20230277

$$\alpha = \sqrt{b^2 j} + \sqrt{d^2 jk}$$

Without loss of generality, we can write any three of these as

$$\alpha = \sqrt{u} + \sqrt{v}$$

with distinct u,v $\in \mathbb{Q}$. We must further restrict u and v in a way that is equivalent to the conditions given in 3.4 and 3.5. It must hold that neither $\sqrt{u}$ or $\sqrt{v}$ are in $\mathbb{Q}$. We must further restrict u and v such that $\sqrt{u} + \sqrt{v}$ cannot be written as a single radical, in which case Stab(α) = 2, so we end up with the conditions u,v, and uv cannot be written as ratio of two square integers. From this, the computation of the orbit group of Gal(E/F) on α should follow easily, and we find the minimal polynomial of α to be

$$a(x) = \left(x - \sqrt{u} - \sqrt{v}\right)(x + \sqrt{u} + \sqrt{v})(x - \sqrt{u} + \sqrt{v})(x + \sqrt{u} - \sqrt{v})$$

Which we write as

$$a(x) = \left(x^2 - \left(\sqrt{u} + \sqrt{v}\right)^2\right)\left(x^2 - \left(\sqrt{u} - \sqrt{v}\right)^2\right),$$

And finally as

$$a(x) = x^4 - 2(u + v)x^2 + (u - v)^2,$$

Corollary 3.9 Since there are no other ways to construct a minimal polynomial a(x) with the Galois group V_4 such that a(x) is of the form

$$x^4 + ax^2 + b,$$

we conclude that all irreducible polynomials of the form$x^4 + ax^2 + b$ must also be of the form of equation (3.1)

Corollary 3.10 All hollow polynomials of the form $x^4 + ax^2 + b$ can be written as equation (3.1)

3.2. Biquadratic Polynomials Modulo p

We have found an exclusive family of irreducible biquadratic polynomials which contains all hollow polynomials for V_4. We now attempt to find an exclusive family of hollow polynomials for V_4; we do this by first generalizing the argument to all biquadratic polynomials, and considering the conditions under which they are reducible modulo p.

Theorem 3.11 A biquadratic polynomial

$$f(x) = x^4 + \alpha x^2 + \beta$$

is irreducible in $\mathbb{Q}$ but reducible mod p for every prime p if and only if

$$\alpha^2 - 4\beta \neq \square,\ \beta = \square,\ 2\sqrt{\beta} - \alpha \neq \square,\ -2\sqrt{\beta} - \alpha \neq \square$$

where □ indicates a perfect square number. [7]

Remark 3.12 Let us take the minimal biquadratic polynomial of V_4,

$$a(x) = x^4 - 2(u + v)x^2 + (u - v)^2,$$

with the same constraints on u and v and with the added condition that 2(u + v),(u −v) $\in \mathbb{Z}$ and examine it using the criteria above:

$$(-2(u + v))^2 - 4(u - v)^2 = 16uv,$$

which by our hypothesis is not a square.
$(u - v)^2 = \square$ always holds, of course, and

[7] For a full proof, see [6] Driver et al., Theorem 5 as well as [10]Carlitz

DOI: 10.54254/2753-8818/5/20230277

$$2\sqrt{(u-v)^2} - (-2(u+v)) = 4u$$
$$-2\sqrt{(u-v)^2} - (-2(u+v)) = -4v$$

both of which are by hypothesis not squares.

Since we have shown that all biquadratic hollow polynomials must be of the form

$$a(x) = x^4 - 2(u+v)x^2 + (u-v)^2,$$

then it follows that polynomials that all biquadratic polynomials of the form

$$a(x) = x^4 - 2(u+v)x^2 + (u-v)^2,$$
$$2(u+v),(u-v) \in \mathbb{Z}$$

must be hollow.

Example 3.13 Consider x^4+1, which we have previously shown to be hollow. By lining up the coefficients, we have

$$u + v = 0$$
$$|u - v| = 1,$$

and we conclude that $x^4 + 1$ is the minimal polynomial of $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$

3.3. Biquadratic Polynomials Modulo n

Up until now, we have dealt with polynomials that are hollow in p, but it turns out that there exist polynomials that are hollow in every integer n greater than 1.

Example 3.14 The polynomial $f(x) = x^4 - 72x^2 + 4$ is irreducible over $\mathbb{Q}$ but reducible modulo every integer n >1. To show that $f(x)$ is irreducible over $\mathbb{Q}$, we consider

$$f(x+1) = (x^4 + 4x^3 + 6x^2 + 4x + 1) - 72(x^2 + 2x + 1) + 1$$
$$x^4 + 4x^3 - 66x^2 - 140x - 71,$$

which is irreducible by Eisenstein's criterion [10]. Additionally, we can see that f(x) is hollow in p, by Theorem 3.11. We will use the following theorem to complete our proof for this claim.

Theorem 3.15 A polynomial of the form

$$f(x) = x^4 - 2(s_1 + s_2)x^2 + (s_1 - s_2)^2$$

is irreducible over Z but reducible modulo n for every integer n greater than 1 if s_1 and s_2 are distinct odd primes that satisfy

$$s_1 \equiv 1 (mod\ 8), \quad \left(\frac{s_2}{s_1}\right) = 1$$

Proof 3.3 In order to prove the hollowness for n, we need to prove that f(x) is reducible modulo p^k for each arbitrary positive integer k. We first define $t = s_1 - s_2$. Then we can easily find that

$$\alpha^2 - 4t^2 = 16s_1s_2 \neq \square, -\alpha + 2t = 4s_1 \neq \square, -\alpha - 2t = 4s_2 \neq \square$$

Because $s_1 \equiv 1 \pmod 8$, $-\alpha+2t$ modulo 2^k can only be a square. As $\left(\frac{s_2}{s_1}\right) = 1$ $-\alpha - 2t$ is a square modulo p^k. By the law of quadratic reciprocity

$$\left(\frac{s_1}{s_2}\right)\left(\frac{s_2}{s_1}\right) = (-1)^{\frac{s_1-1}{2}\frac{s_2-1}{2}}$$

DOI: 10.54254/2753-8818/5/20230277

we can get $\left(\frac{s_2}{s_1}\right) = 1$ and $-\alpha - 2t$ modulo q_2^k is a square. If $\left(\frac{s_\alpha}{p}\right) = 1$ (where a = 1 or 2), then $-\alpha \pm 2t$ is a square modulo p^k. While if $\left(\frac{s_\alpha}{p}\right) = -1$, then $\left(\frac{s_1 s_2}{p}\right) = 1$ and $\alpha^2 - 4t^2$ modulo p^k is a square. Therefore, f(x) is hollow for p^k. Since every integer greater than 1 can be factorized into a form of $p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ and $p_n^{k_n}$'s are co-prime, we can use Chinese Remainder Theorem to get lemma 3.16 [11].

Lemma 3.16 If f(x) is reducible modulo all p^k for all prime p, then it's reducible modulo n for all n. Therefore, we can easily end the proof.

Remark 3.17 We notice the similarity between the respective expressions for biquadratic polynomials hollow in p and in n. The reader can check that the smallest pair of primes satisfying Theorem 3.15 are 2 and 17, the corresponding polynomial of which is $x^4 - 38x^2 + 225$. The next smallest pair of primes of primes are 13 and 17, which gives $x^4 - 60x^2 + 16$, the third smallest, 17 and 19, gives us the polynomial considered in Example 3.14.

References

[1] Conrad K. Recognizing Galois groups Sn and An[J]. Lecture Notes, University of Connecticut, 2017.

[2] Garver R. Quartic equations with certain groups[J]. Annals of Mathematics, 1928: 47-51.

[3] Kappe L C, Warren B. An elementary test for the Galois group of a quartic polynomial[J]. The American Mathematical Monthly, 1989, 96(2): 133-137.

[4] Conrad K. Galois groups of cubics and quartics (not in characteristic 2)[J]. Expository papers, 2010, 10.

[5] Rotman J. Galois theory[M]. Springer Science & Business Media, 1998.

[6] Driver E, Leonard P A, Williams K S. Irreducible quartic polynomials with factorizations modulo p[J]. The American Mathematical Monthly, 2005, 112(10): 876-890.

[7] Dummit D S, Foote R M. Abstract algebra[M]. Hoboken: Wiley, 2004.

[8] Milne, J. S. Fields and Galois Theory, 2020.

[9] Almuteri A N. Quadratic Reciprocity: Proofs and Applications[J]. 2019.

[10] Carlitz L. Note on a quartic congruence[J]. The American Mathematical Monthly, 1956, 63(8): 569-571.

[11] Miller K. The Chinese Remainder Theorem[J]. 2017.