

Reducible over any Finite Field but Irreducible over \mathbb{Q}

Kelly J. Pearson and Tan Zhang

Department of Mathematics and Statistics
Murray State University, Murray, KY 42071-0009, USA
kelly.pearson@murraystate.edu
tan.zhang@murraystate.edu

Abstract

We give a simple argument to show if $a \neq b \in \mathbb{Z}$ so that no prime p has the property $p^2|a$ or $p^2|b$, then the minimal polynomial of $\sqrt{a} + \sqrt{b}$ over \mathbb{Q} , although irreducible over \mathbb{Q} by definition, is reducible over any finite field. This provides infinitely many polynomials with the property that they are irreducible over \mathbb{Q} yet reducible over any finite field and is a generalization of previous work by M.A. Lee. We also give conditions for the minimal polynomial to have linear factors over \mathbb{Z}_p and for the minimal polynomial to have multiple roots in an extension field of \mathbb{Z}_p .

Mathematics Subject Classification: 12F10, 02A05

Keywords: irreducibility, minimal polynomial

A polynomial $p(x)$ in $F[x]$ is reducible if there is a factorization $p(x) = f(x)g(x)$ for $f(x), g(x)$ in $F[x]$ where $f(x)$ and $g(x)$ are not units. A polynomial is irreducible if it is not reducible. If a is algebraic over a field F , then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$. This polynomial is called the minimal polynomial of a over F . Moreover, the degree of $p(x)$ is equal to the degree of the field extension $F(a)$ over F ; that is, $\deg p(x) = [F(a) : F]$.

In [3], Lee illustrated a class of polynomials which are reducible mod p for all p but which are irreducible over the integers. This note is an extension of this paper and uses elementary techniques which can be found in [2].

The goal of this article is to give an elementary proof of the following result:

Theorem 0.1 *Let $a \neq b \in \mathbb{Z}$ be so that no prime p has the property $p^2|a$ or $p^2|b$, then the minimal polynomial of $\sqrt{a} + \sqrt{b}$ over \mathbb{Q} is reducible over \mathbb{Z}_p for any prime p .*

The proof of the theorem combines key ideas from group theory and field theory; thus, it is accessible to anyone who has had some exposure to abstract algebra. First, we shall establish a few basic facts which will be needed in the proof of the theorem.

Lemma 0.2 *If $a \neq b \in \mathbb{Z}$, then $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.*

Proof: It is obvious that $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$. To show containment the other way, we note

$$\frac{1}{a-b}(\sqrt{a} - \sqrt{b}) = \frac{1}{\sqrt{a} + \sqrt{b}} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}).$$

Hence, $\sqrt{a} - \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Consequently, $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. \square

Lemma 0.3 *Let $a \neq b \in \mathbb{Z}$ so that no prime p has the property $p^2|a$ or $p^2|b$, then*

$$[\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 4.$$

Proof: Since $x^2 - a$ is the minimal polynomial for \sqrt{a} over \mathbb{Q} and $[\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}(\sqrt{a})] \cdot [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}]$, it suffices to show $[\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = 2$. We note that \sqrt{b} is a root of $x^2 - b \in \mathbb{Q}(\sqrt{a})[x]$. Suppose $x^2 - b$ is reducible over $\mathbb{Q}(\sqrt{a})$, then there exist $c_0, c_1 \in \mathbb{Q}$ so that $\sqrt{b} = c_0 + c_1\sqrt{a}$, i.e. $b = c_0^2 + c_1^2a + 2c_0c_1\sqrt{a} \in \mathbb{Q}$. It follows that $\sqrt{a} \in \mathbb{Q}$, a contradiction. Hence, $[\mathbb{Q}(\sqrt{a} + \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = [\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$. \square

Lemma 0.4 *Let $a, b \in \mathbb{Z}_p$. If there is no $\gamma \in \mathbb{Z}_p$ so that $\gamma^2 = a$ or $\gamma^2 = b$, then there exists a $\gamma_0 \in \mathbb{Z}_p$ so that $\gamma_0^2 = ab$; that is, if neither a nor b has a square root in \mathbb{Z}_p , then ab must have a square root in \mathbb{Z}_p .*

Proof: Let \mathbb{Z}_p^* be the set of units of \mathbb{Z}_p . We define $\psi : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ by $\psi(x) := x^2$. Let $H := \text{Im } \psi$. Since $\text{Ker } \psi = \{1, p-1\}$, the First Isomorphism Theorem gives us $H \cong \mathbb{Z}_p^*/\text{Ker } \psi$. Hence, we have $|H| = \frac{p-1}{2}$. By Lagrange's Theorem, $[\mathbb{Z}_p^* : H] = |\mathbb{Z}_p^*|/|H| = 2$. Subsequently, $H = a^2H = aH \cdot bH$, and $ab \in H$ as required. \square

We now return to the proof of our main theorem.

Proof of Theorem: The polynomial $\phi(x) = x^4 - 2(a+b)x^2 + (a-b)^2$ has $\sqrt{a} + \sqrt{b}$ as a root. Since $\phi(x) \in \mathbb{Q}[x]$ has degree 4, by Lemma 2, $\phi(x)$ is the minimal polynomial for $\sqrt{a} + \sqrt{b}$ over \mathbb{Q} , and hence is irreducible over \mathbb{Q} . We now consider $\phi_{[p]}(x)$, the homomorphic image of $\phi(x)$, by taking the coefficients modulo a prime p . If $p = 2$, then $\phi_{[2]}(x) = x^4 + (a+b)^2 = (x^2 - (a+b))(x^2 + (a+b))$; hence $\phi_{[2]}(x)$ is reducible. Suppose $p \geq 3$. If there exists $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 = a$, then $\mathbb{Z}_p(\sqrt{a} + \sqrt{b}) = \mathbb{Z}_p(\sqrt{b})$, so $[\mathbb{Z}_p(\sqrt{a} + \sqrt{b}) : \mathbb{Z}_p] = 2$, which implies $\phi_{[p]}(x)$ is reducible over \mathbb{Z}_p . Similarly,

if there exists $\beta \in \mathbb{Z}_p$ such that $\beta^2 = b$, then $\phi_{[p]}(x)$ is reducible over \mathbb{Z}_p . If neither a nor b has a square root in \mathbb{Z}_p , by Lemma 3, there exists a $\gamma_0 \in \mathbb{Z}_p$ so that $\gamma_0^2 = ab$, whence

$$\begin{aligned} \phi_{[p]}(x) &= x^4 - 2(a+b)x^2 + (a-b)^2 = (x^2 - (a+b))^2 - 4ab \\ &= (x^2 - a - b)^2 - (2\gamma_0)^2 = ((x^2 - a - b) - 2\gamma_0)((x^2 - a - b) + 2\gamma_0), \end{aligned}$$

so $\phi_{[p]}(x)$ is reducible over \mathbb{Z}_p . This can also be seen by noticing $\sqrt{a} + \sqrt{b}$ is a root of $x^2 - (a+b) - 2\sqrt{ab} \in \mathbb{Z}_p[x]$. \square

As a consequence, we have the following

Corollary 0.5 *Let $a \neq b \in \mathbb{Z}$ be so that no prime p has the property $p^2|a$ or $p^2|b$, then the minimal polynomial of $\sqrt{a} + \sqrt{b}$ over \mathbb{Q} is reducible over any finite field.*

The next corollary is the result in [3]:

Corollary 0.6 *Let $a \in \mathbb{Z}$ be so that no prime p has the property $p^2|a$. Then the polynomial $x^4 + 2(1-a)x^2 + (1+a)^2$ is irreducible over \mathbb{Q} but reducible over \mathbb{Z}_p for any prime p .*

Proof: Take $b = -1$ in $\phi(x)$. \square

For the remainder of this note, we determine the factorization of $\phi_{[p]}(x)$ over \mathbb{Z}_p . The observations are in regards to whether $\phi_{[p]}(x)$ has linear factors in $\mathbb{Z}_p[x]$ or multiple roots in an extension of \mathbb{Z}_p .

Theorem 0.7 (Linear Factors) *In $\mathbb{Z}_2[x]$, the polynomial $\phi_{[2]}(x)$ always factors into linear factors. There exists a linear factor of $\phi_{[p]}(x)$ in $\mathbb{Z}_p[x]$ ($p > 2$) if and only if $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a \equiv b \pmod{p}$. Moreover, if $(ab)^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, then there are no linear factors.*

Proof: In an extension field, K , of \mathbb{Z}_p , let $\alpha^2 = a$, $\beta^2 = b$, $\gamma^2 = ab$. We find the four roots of $\phi_{[p]}(x)$ to be $\pm(\alpha + \beta)$, $\pm(\alpha - \beta)$.

If $p = 2$, then $\alpha, \beta \in \mathbb{Z}_2$; hence, all four roots are in \mathbb{Z}_2 .

Suppose $p \geq 3$. If there exists a linear factor of $\phi_{[p]}(x)$ in $\mathbb{Z}_p[x]$ ($p > 2$), then $\alpha + \beta$ or $\alpha - \beta$ must be in \mathbb{Z}_p . But this implies both α and β are in \mathbb{Z}_p or $a \equiv b \pmod{p}$. By Euler's Criterion, this implies $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a \equiv b \pmod{p}$. Moreover, since $(\alpha \pm \beta)^2 = a + b \pm 2\gamma$, we see that $\gamma \in \mathbb{Z}_p$. Contrapositively, $(ab)^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ implies, by Euler's Criterion, that $\gamma \notin \mathbb{Z}_p$; this implies $\alpha \pm \beta \notin \mathbb{Z}_p$, and there is not linear factor in $\mathbb{Z}_p[x]$.

Conversely, if $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a \equiv b \pmod{p}$, then $\alpha, \beta \in \mathbb{Z}_p$ or $\alpha + \beta$ or $\alpha - \beta$ is in \mathbb{Z}_p and hence there are linear factors over $\mathbb{Z}_p[x]$. \square

Example 0.8 Let $a = 2$, $b = 3$, $p = 5$ and $\phi_{[5]}(x) = x^4 + 1 = (x^2 + 2)(x^2 + 3)$. Notice that $\gamma \in \mathbb{Z}_5$ but there are no linear factors in $\mathbb{Z}_5[x]$. The roots of $x^2 + 2$ are $\pm(\alpha - \beta)$. The roots of $x^2 + 3$ are $\pm(\alpha + \beta)$.

We now consider whether $\phi_{[p]}(x)$ has multiple roots in any extension field of \mathbb{Z}_p .

Theorem 0.9 (Multiple Roots) The polynomial $\phi_{[p]}(x)$ has multiple roots in an extension of \mathbb{Z}_p if and only if one of the following conditions hold:

1. $a \equiv b \pmod{p}$
2. $a \equiv 0 \pmod{p}$
3. $b \equiv 0 \pmod{p}$.

Proof: Multiple roots will occur if and only two of the roots $\phi(x)$ to be $\pm(\alpha + \beta)$, $\pm(\alpha - \beta)$ are equal. This occurs exactly in the conditions (1) - (3). \square

We can generalize the polynomial $\phi(x)$ to higher dimensions. In particular, for $k \geq 3$ let

$$\phi_{k,a,b}(x) = x^{2k} - 2(a+b)x^k + (a-b)^2$$

and notice the same proofs will hold to show that $\phi_k(x)$ is irreducible over \mathbb{Q} . However, reducibility over \mathbb{Z}_p does not necessarily hold for any p . If we set $a = 2, b = 3, p = 17$, then $\phi_{3,2,3} = x^6 - 10x^3 + 1$ is irreducible over \mathbb{Z}_{17} . If $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and hence there is a $\gamma_0 \in \mathbb{Z}_p$ with $\gamma_0^2 = ab$, then the polynomial is reducible since $\phi_{k,a,b}(x) = ((x^k - a - b) - 2\gamma_0)((x^k - a - b) + 2\gamma_0)$. It may also be the case that the polynomial is reducible yet ab does not have a square root in \mathbb{Z}_p . For example, if we take $a = 2, b = 3, p = 13$, then 6 does not have a square root in \mathbb{Z}_{13} yet $\phi_{3,2,3} = x^6 - 10x^3 + 1 = (x^2 + 5x + 9)(x^2 + 6x + 1)(x^2 + 2x + 3)$.

The computation of the Galois groups is studied via Maple in [4].

References

- [1] David M. Burton, *Elementary Number Theory, second edition*, Wm. C. Brown Publishers, 1989.
- [2] Thomas W. Hungerford, *Algebra*, Springer-Verlag, 1974.
- [3] M.A. Lee, Some Irreducible Polynomials which are Reducible Mod p for all p *The American Mathematical Monthly*, **76** No. 10 (1969), 1125.
- [4] Irene Smith, The Galois Groups of a Special Class of Polynomials, *Master's Thesis at Murray State University*, 2006.

Received: February 20, 2008