A NOTE ON THE ROOTS OF QUINTIC POLYNOMIALS

COURTNEY GIBBONS, JACOB HELZNER

Abstract. This is a short note on the solvability of quintic polynomials. Using results from our undergraduate course in modern algebra, we demonstrate that $p(x) = x^5 - 15x^2 + 5$ is not solvable by radicals over $\mathbb{Q}$.

Contents

1. Introduction

We start with a brief discussion of the historical effort to determine a quintic formula, and its role in the development of abstract algebra.

First, consider the quadratic equation $ax^2 + bx + c = 0$ where $a \neq 0$. Many people know of the existence of the quadratic formula,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1.1}$$

for finding the solutions to this equation. We can arrive at the quadratic formula through a process called completing the square. First, notice that for any quadratic $ax^2 + bx + c$ with $a = 1$, there exists a square whose expansion differs only by some constant k. This square may be written as,

$$(x + \frac{1}{2}b)^2 = x^2 + bx + \frac{1}{4}b^2 \tag{1.2}$$

Date: June 16, 2025.

where $k = c - \frac{1}{4}b^2$. Factoring out a from $ax^2 + bx + c$, we apply this formula for k and determine that any quadratic may be written as:

$$a(x + \frac{1}{2a}b)^2 + (c - \frac{1}{4a}b^2) \tag{1.3}$$

Solving for the roots of this expression yields (1.1), the quadratic formula.

During the 18th and 19th century, mathematicians tried to determine if higher-degree polynomials are solvable by radicals. A radical is recursively defined as some nth root or power of an expression consisting of any number of radicals, rational numbers and the usual arithmetic operations. We know that a general polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is solvable by radicals if its roots can be expressed as a formula consisting of radicals, such as the quadratic formula. To this end, Lagrange in the 18th century developed a method to determine the roots of cubic and quartic polynomials. His method used the fact that the roots of a cubic polynomial could be written as $x = u + v$ where u^3 and v^3 are the roots of some quadratic, and that u and v could be written as rational expressions built from the roots of the cubic [3]. Picking up where LaGrange left off, Gauss eventually developed modular arithmetic and the concept of an equivalence class [3]. Around 1830, Galois - without needing to derive formulas - used the concept of a field and a group to determine if a certain degree polynomial was solvable, ultimately giving a definitive answer to Lagrange's and Gauss' questions.

As it goes in the mathematical mythos, Galois was a very young French mathematician who died in a duel at the age of 20. Despite his age, his contributions would play an important role in the development of modern algebra. The major tool which Galois used to show the unsolvability of quintic polynomials is now eponymously named the Galois group, a group of automorphisms take a general element of $\mathbb{Q}$ adjoin the roots of some polynomial and permutes the roots while fixing the rational components. Using an one to one homomorphism from the Galois group to a permutation group, if we can establish certain equivalent conditions for solvability in the resulting permutation, we know whether the given polynomial is solvable by radicals.

We take this opportunity to note that all definitions are courtesy of [4] unless otherwise stated.

2. Acknowledgements

The author acknowledges Rhea Ding and Clifford Yen, collaborators on the writing assignments in MATH-325W which comprise a large portion of this paper.

3. Polynomial rings, algebraic elements, and irreducibility

One of the most important results in modern algebra is the relationship between roots of polynomial equation with complex coefficients and degree one factors of the polynomial in $\mathbb{C}[x]$. We present the following theorem without proof.

Theorem 3.1. *For all $f(x) \in \mathbb{C}[x]$ of positive degree n, there exist unique complex numbers r_i for $0 \leq i \leq n$ (not necessarily distinct) such that*

$$f(x) = r_0(x - r_1)(x - r_2) \cdots (x - r_n).$$

This factorization of $f(x)$ is unique up to rearranging the factors. In particular, $r \in \mathbb{C}$ is a root of $f(x)$ if and only if $x - r$ divides $f(x)$ in $\mathbb{C}[x]$.

Furthermore, if $f(x)$ has real coefficients, $r \in \mathbb{C}$ is a root of $f(x)$ if and only if its complex conjugate $\overline{r}$ is a root of $f(x)$.

When $f(x)$ is a polynomial with rational coefficients and we consider divisibility in $\mathbb{Q}[x]$, the relationship between roots and factors is a bit more complicated. Recall that the algebraic elements over $\mathbb{Q}$ are the roots of nonzero polynomials in $\mathbb{Q}[x]$, and that the minimal polynomial of an algebraic element over $\mathbb{Q}$ is the unique monic, irreducible polynomial in $\mathbb{Q}[x]$ for which that algebraic element is a root.

With that in mind, we want to show that for some field F, if $F[x]$ is a principal ideal domain, then each algebraic element over F has a unique minimal polynomial in $F[x]$. To start, recall that a principal ideal domain is an integral domain where each of its ideals is principal. As our first step, we want to show that for any field F, $F[x]$ is a principal ideal domain. If I is the zero ideal, we can express it as $\langle 0 \rangle$, the principal ideal generated by the zero polynomial. Otherwise, we wish to show there must be some generator $f(x)$ in $F[x]$ which divides all the polynomials in our nonzero I, and it follows that $f(x)$ is nonzero and of minimal degree. We can use the well ordering principle to show that this polynomial exists, and we can further establish that $I = \langle f(x) \rangle$ through a double inclusion proof. By virtue of being an ideal, its easy to show that $I \subseteq \langle f(x) \rangle$; since $f(x)$ is in I, all polynomial multiples are as well. The rest of the proof uses the division algorithm to show that any element of I may be expressed as a multiple of $f(x)$. Towards a contradiction, we suppose some element of I divided by $f(x)$ has a nonzero remainder r; since r has a smaller degree, this would imply $f(x)$ doesn't have minimal degree, and thus all elements of I are multiples of $f(x)$, which further implies that $\langle f(x) \rangle \subseteq I$. From this proof, we may further note that if I is a nonzero ideal of $F[x]$, I has a monic generator, and nonzero polynomials in I are generators of I if and only if they are of minimal degree in I. These corollaries are left to the reader.

Our goal is still to show that when $F[x]$ is a principal ideal domain, every algebraic element over F has a minimal polynomial. Let I be the set of polynomials in $F[x]$ for which some algebraic element r is a root. We leave it to the reader to verify that I is an ideal of $F[x]$ by checking the conditions of the Ideal Theorem. Because r is algebraic over F and $F[x]$ is a principal ideal domain, I is a nonzero principal ideal of $F[x]$. As we have noted, it then follows that I has a monic generator $m(x)$ of minimal degree in I. From here, we can show that $m(x)$ is also irreducible through a short proof by contradiction. Now, it only remains to show that $m(x)$ is unique. Because $m(x)$ is monic, all of its scalar multiples in I are no longer candidates, and thus $m(x)$ is unique.

We frequently rely on the results below to verify that a given polynomial is irreducible over a particular field. When the field is $\mathbb{Q}$, Eisenstein's Irreducibility Criterion is a good first choice.

Lemma 3.2 (Eisenstein's Irreducibility Criterion via [4])**.** *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of positive degree where*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

This polynomial is irreducible over $\mathbb{Q}[x]$ if there exists a prime p such that

(1) *p does not divide a_n,*
(2) *p divides $a_{n-1}, a_{n-2}, \ldots, a_0$, and*
(3) *p^2 does not divide a_0.*

When the coefficient field is not $\mathbb{Q}$, or when Eisenstein's Irreducibility Criterion is inconclusive, we can use the following result for polynomials of degree at most three.

Lemma 3.3 (Low-Degree Irreducibility Lemma via [4])**.** *Let F be a field and let $f(x) \in F[x]$ be a polynomial of positive degree.*

(1) *If $\deg(f(x)) = 1$, then $f(x)$ is irreducible.*
(2) *If $2 \leq \deg(f(x)) \leq 3$, then $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.*

We conclude this section with one more useful fact about polynomials that we will rely on later.

Proposition 3.4. *The polynomial $f(x) \in \mathbb{Q}[x]$ has a repeated root $r \in \mathbb{C}$ if and only if r is also a root of its derivative, $f'(x)$.*

Proof. To start, suppose that $f(x) \in \mathbb{Q}[x]$ has a repeated root $r \in \mathbb{C}$. Then by the product rule, for some $q(x) \in \mathbb{Q}[x]$ we have:

$$f'(x) = ((x-r)^2 q(x))' = (x-r)(2q(x) + q'(x)(x-r))$$

Since $(x-r)$ divides $f'(x)$ in $\mathbb{C}[x]$, by Theorem 3.1, r is also a root of $f'(x)$.

Conversely, if $f(x)$ has degree n and r is a root of $f(x)$ but not a repeated root, Theorem 3.1 guarantees that

$$f(x) = r_0(x - r_1)\cdots(x - r_n)$$

for complex numbers r_0, r_1, ..., r_n where, without loss of generality, $r = r_1$ but not any of the other roots r_2, ..., r_n.

Setting $q(x) = r_0(x - r_2)\cdots(x - r_n)$, we have that $f(x) = (x - r)q(x)$ and thus $f'(x) = (x - r)q'(x) + q(x)$. By assumption, r is not a root of $q(x)$ and hence $x - r$ does not divide $q(x)$. It follows that $x - r$ does not divide $f'(x)$. Thus, by Theorem 3.1, r is not a root of $f'(x)$. □

4. Galois groups and solvability by radicals

We turn our attention to a quintic polynomial that is solvable by radicals.

Example 4.1. The polynomial $q(x) = x^5 + 3x^3 - 7x^2 - 21 \in \mathbb{Q}[x]$ is solvable by radicals. Since $q(x) = (x^3 - 7)(x^2 + 3)$, we know that the roots of $q(x)$ are $\sqrt[3]{7}$, $\sqrt[3]{7}\zeta_3$, $\sqrt[3]{7}\zeta_3^2$, $\sqrt{3}$, and $-\sqrt{3}$. Let $U = \mathbb{C}$, an extension field of $\mathbb{Q}$ that contains all these roots. From the definition of solvable by radicals, we wish to show for some $r_1, r_2, \ldots, r_m \in \mathbb{C}$ and positive integers $k_1, k_2, \ldots, k_m$ that

(1) $(r_1)^{k_1} \in \mathbb{Q}$,
(2) $(r_i)^{k_i} \in \mathbb{Q}(r_1, r_2, \ldots, r_{i-1})$ for $1 < i < m$, and,
(3) $\mathbb{Q}^{q(x)} \subseteq \mathbb{Q}(r_1, r_2, \ldots r_m)$.

Let $r_1 = \sqrt[3]{7}$, $k_1 = 3$, $r_2 = \zeta_3$, $k_2 = 3$, $r_3 = \sqrt{3}$, and $k_3 = 2$. Then $r_1^{k_1} \in \mathbb{Q}$, $r_2^{k_2} \in \mathbb{Q}(r_1)$, and $r_3^{k_3} \in \mathbb{Q}(r_2)$. Furthermore, $\mathbb{Q}^{q(x)} \subseteq \mathbb{Q}(r_1, r_2, r_3)$ by field closure under addition and multiplication, since $\mathbb{Q}(r_1, r_2, r_3)$ contains all the roots of $q(x)$ and therefore all of $\mathbb{Q}^{q(x)}$.

In contrast, in Theorem 5.1, we will ultimately show that there exists a quintic polynomial $p(x)$ that is not solvable by radicals. Our primary tool for investigating the solvability of polynomials is the Galois group. Given a polynomial with n distinct roots, we may view its Galois group as a subgroup of S_n.

Example 4.2. The polynomial $g(x) = x^5 - 11 \in \mathbb{Q}[x]$ has a Galois group isomorphic to a subgroup of S_5, and each element in $\mathrm{Gal}(\mathbb{Q}^{g(x)}/\mathbb{Q})$ can be associated with a distinct permutation in that subgroup. [1]

Let $p(x) = x^5 - 11$, with roots $a_1 = \sqrt[5]{11}$, $a_2 = \sqrt[5]{11}\zeta_5$, $a_3 = \sqrt[5]{11}\zeta_5^2$, $a_4 = \sqrt[5]{11}\zeta_5^3$, and $a_5 = \sqrt[5]{11}\zeta_5^4$. By Proposition 17.5 via [4], we can define a one-to-one group homomorphism $T : G =$

[1] We discuss this Galois group in more detail in Appendix .

$Gal(\mathbb{Q}^{p(x)}/\mathbb{Q}) \to S_5$ as the following, where S_5 is the set of all 5-cycles:

$$T(\varphi \in G) = \varphi|_{a_1,a_2,a_3,a_4,a_5} \in S_5 \tag{4.1}$$

We now demonstrate some applications of T to homomorphisms in G. For our first homomorphism, let $\varphi \in G$ satisfy $\varphi(\sqrt[5]{11}) = \sqrt[5]{11}\zeta_5$ and $\varphi(\zeta_5) = \zeta_5^3$. We start with a_1, and see that $\varphi(a_1) = a_2$. Since φ is an automorphism that preserves the group operation, we then obtain a_5 from $\varphi(a_2)$, a_4 from $\varphi(a_5)$, and a_1 from $\varphi(a_4)$. Furthermore, $\varphi(a_2) = a_2$, so we obtain the cycle $(1254) \in S_5$. For our next homomorphism, let $\psi \in G$ satisfy $\psi(\sqrt[5]{11}) = \sqrt[5]{11}\zeta_5^2$ and $\psi(\zeta_5) = \zeta_5^4$. Again, we start with a_1, and see that $\psi(a_1) = a_3$. We know ψ is an automorphism that preserves the group operation, so $\psi(a_3) = a_1$, $\psi(a_2) = a_2$, $\psi(a_4) = a_5$ and $\psi(a_5) = a_4$, and we obtain the cycle $(13)(45) \in S_5$.

One very useful proposition is due to Cauchy, and we will state this without proof.

Proposition 4.3 (Cauchy's Theorem)**.** *If p is a prime and divides the order of a group G, then G contains an element of order p.*

Corollary 4.4. *Every finite group G with order divisible by 5 has an element of order 5. Furthermore, if $G = S_5$, that element must be a 5-cycle.*

5. An unsolvable quintic

In this section, we demonstrate the existence of a quintic polynomial that is not solvable by radicals.

Theorem 5.1. *The polynomial $p(x) = x^5 - 15x^2 + 5 \in \mathbb{Q}[x]$ is not solvable by radicals.*

To prove this theorem, we will need to use solvable groups and normal subgroups.

Definition 5.2. A group G is called ***solvable*** if there exists a chain of subgroups

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k = \{e\}$$

such that for all $1 \leq i \leq k$,

(1) $H_i \triangleleft H_{i-1}$;
(2) H_{i-1}/H_i is Abelian.

Example 5.3. The group S_3 is solvable. By definition, we know that $S_3^{(2)} = \{e\}$, $S_3^{(1)} = \{e, (123), (132)\}$, and $S_3 = \{e, (12), (13), (23), (123), (132)\}$. From [4, Example 26.7], $S_3^{(1)}$ is Abelian and that $S_3^{(k)} = \{e\}$ for all $k \geq 2$. By [4, Proposition 26.8], for any group S, $S^i \triangleleft S$ for all $i \geq 1$. Notice the following chain of subgroups:

$$S_3 \supset S_3^{(1)} \supset S_3^{(2)} = \{e\},$$

Thus, $S_3^{(2)} \triangleleft S_3^{(1)}$, and $S_3^{(1)} \triangleleft S_3$. By [4, Proposition 26.5], $S_3/S_3^{(1)}, S_3^{(1)}/S_3^{(2)}$ are Abelian. By the definition above, we conclude that S_3 is a solvable group.

Another useful result follows. We can use it directly to show that a group is solvable, or we can use its contrapositive to show that a polynomial is not solvable by radicals.

Proposition 5.4. *If $f(x) \in F[x]$ is solvable by radicals, then* $\mathrm{Gal}\left(F^{f(x)}/F\right)$ *is a solvable group.*

Example 5.5 (A direct application of Proposition 5.4)**.** We can verify that S_3 is solvable group by finding a polynomial $f(x) \in \mathbb{Q}[x]$ where $\mathrm{Gal}(\mathbb{Q}^{f(x)}/\mathbb{Q}) \cong S_3$ and $f(x) = 0$ is solvable by radicals. The polynomial $f(x) = x^3 - 7 \in \mathbb{Q}[x]$ will satisfy these conditions.

We know that the roots of $f(x)$ are $\sqrt[3]{7}$, $\sqrt[3]{7}\zeta_3$, and $\sqrt[3]{7}\zeta_3^2$. Let $U = \mathbb{C}$, an extension field of $\mathbb{Q}$ that contains all these roots. Applying the definition of solvable by radicals as in Example 4.1, let $r_1 = \sqrt[3]{7}$, $k_1 = 3$, $r_2 = \zeta_3$, and $k_2 = 3$. Then $r_1^{k_1} \in \mathbb{Q}$ and $r_2^{k_2} \in \mathbb{Q}$. Furthermore, $\mathbb{Q}^{q(x)} \subseteq \mathbb{Q}(r_1, r_2)$ by field closure under addition and multiplication, since $\mathbb{Q}(r_1, r_2)$ contains all the roots of $f(x)$ and therefore all of $\mathbb{Q}^{f(x)}$.

By [4, Proposition 14.8], we know that

$$\begin{aligned} |\operatorname{Gal}(\mathbb{Q}^{f(x)}/\mathbb{Q})| &= [\mathbb{Q}(r_1, r_2) : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}] \\ &= [r_2 : \mathbb{Q}(r_1)][r_1 : \mathbb{Q}] \end{aligned}$$

Because $x^3 - 7$ is irreducible over $\mathbb{Q}$ by Lemma 3.2 with $p = 7$, $[r_1 : \mathbb{Q}] = 3$. By Lemma 3.3, $x^2 + x + 1$ is irreducible over $\mathbb{Q}(r_1)$, since its roots $\zeta_3, \zeta_3^2 \notin \mathbb{Q}(r_1)$ - thus $[r_2 : \mathbb{Q}(r_1)] = 2$. Multiplying, we get $|\operatorname{Gal}(\mathbb{Q}^{f(x)}/\mathbb{Q})| = 6$. From here, we see that $|\operatorname{Gal}(\mathbb{Q}^{f(x)}/\mathbb{Q})| = |S_3| = 3! = 6$, and so our translation homomorphism T from $|\operatorname{Gal}(\mathbb{Q}^{f(x)}/\mathbb{Q})|$ to S_3 must be onto. This means T is an isomorphism. Since $f(x) = x^3 - 7$ is solvable by radicals and its Galois group is isomorphic to S_3, it follows that S_3 is a solvable group.

One of the main results of our modern algebra course this semester was the fact that S_5 is not a solvable group. This allows us to prove our main result.

Let $p(x) = x^5 - 15x^2 + 5 \in \mathbb{Q}[x]$ and let $G = \mathrm{Gal}(\mathbb{Q}^{p(x)}/\mathbb{Q})$. We first show that $p(x)$ has three real nonrepeated roots. Since $p(x)$ is a continuous function and $p(-1) = -10$, $p(0) = 5$, $p(1) = -10$ and $p(3) = 113$, we know by the Intermediate Value Theorem that there exists an $r_1 \neq r_2 \neq r_3 \in \mathbb{R}$ where $p(r_1) = p(r_2) = p(r_3) = 0$. By Proposition 3.4, these roots are not repeated, because the roots of $p'(x) = 5x(x^3 - 6)$ are $r \in \{0, \sqrt[3]{6}, \sqrt[3]{6}\zeta_3, \sqrt[3]{6}\zeta_3^2\}$, for which none have $p(r) = 0$. We know there are at most three real roots by looking at the intervals on which $p(x)$ is increasing and decreasing - since $p'(x)$ is negative between 0 and $\sqrt[3]{6}$ and otherwise positive, $p(x)$ must cross the

x-axis at most three times. Furthermore, because $p(x)$ is degree 5, $p(x)$ has two complex roots which are conjugates by Theorem 3.1.

We now consider the one-to-one homomorphism $T : \mathrm{Gal}\left(\mathbb{Q}^{p(x)}/\mathbb{Q}\right) \to S_5$. Since $\psi : \mathbb{Q}^{r(x)} \to \mathbb{Q}^{p(x)}$ defined by $\psi(a+bi) = a-bi$ is an automorphism that fixes $\mathbb{Q}$, $\psi \in G$. We also know $T(\psi) = (4,5)$, since r_4 and r_5 are conjugates, and thus $T(G)$ contains a 2-cycle.

From here, we must establish that G contains an element of order 5. To that end, we know from [4, Proposition 14.8] that

$$\begin{aligned} |G| &= [\mathbb{Q}^{p(x)} : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}] \\ &= [\mathbb{Q}^{p(x)} : \mathbb{Q}(r_1)][r_1 : \mathbb{Q}] \end{aligned}$$

Since $p(x) = x^5 - 15x^2 + 5$ is irreducible over $\mathbb{Q}$ by Eisenstein's Irreducibility Criterion with $p = 5$, $[r_1 : \mathbb{Q}] = 5$ and thus 5 divides the order of the G. By Corollary 4.4, G contains an element of order 5. Furthermore, since one-to-one homomorphisms preserve the order of an element, the mapping onto S_5 contains an element of order 5, which must be a 5-cycle.

Now that we have a 5-cycle and a 2-cycle, we know that the image of G is all of S_5 by [4, Proposition 19.9]. Since G and its image are isomorphic and S_5 is not solvable, we know from Proposition 5.4 that $p(x)$ is not solvable by radicals.

As we have just demonstrated, there cannot be a quintic formula, and it's thanks to centuries of mathematicians' work that this very problem gave rise to the field of abstract algebra. (And ring, and group, and ideal, etc.)

References

1. A. Gardiner, *The art of problem solving*, in: T. Gowers (Ed.), *The Princeton Companion to Mathematics*, Princeton University Press, 2008, pp. 955–966
2. C. Gibbons, course notes, 2024.
3. T. Gowers (Ed.), *The Princeton Companion to Mathematics*, Princeton University Press, 2008.
4. R. Redfield, *Abstract Algebra: A Concrete Introduction* Addison Wesley Longman, Inc., 2001.

Appendix A. An Interesting Galois Group

The polynomial $g(x) = x^5 - 11 \in \mathbb{Q}[x]$ discussed in Example 4.2 is solvable by radicals over $\mathbb{Q}$ and has a Galois group isomorphic to a twenty-element subgroup of S_5.

Indeed, taking $r_1 = \sqrt[5]{11}$, $r_2 = \zeta_5$, $k_1 = 5$, and $k_2 = 5$, we see that $r_1^{k_1} \in \mathbb{Q}$ and $r_2^{k_2} \in \mathbb{Q}(\sqrt[5]{11})$. We also have that

$$\mathbb{Q}^{g(x)} = \mathbb{Q}\left(\sqrt[5]{11}, \sqrt[5]{11}\zeta_5, \sqrt[5]{11}\zeta_5^2, \sqrt[5]{11}\zeta_5^3, \sqrt[5]{11}\zeta_5^4\right) = \mathbb{Q}(r_1, r_2),$$

and therefore $g(x)$ is solvable by radicals over $\mathbb{Q}$.

To verify that $|\operatorname{Gal}(\mathbb{Q}^{g(x)}/\mathbb{Q})| = 20$, observe that $g(x) = x^5 - 11$ is irreducible over $\mathbb{Q}$ by Lemma 3.2 with prime $p = 11$. This means that

$$[\mathbb{Q}(\sqrt[5]{11} : \mathbb{Q}] = [\sqrt[5]{11} : \mathbb{Q}] = \deg(g(x)) = 5.$$

Also observe that $m(x) = x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of ζ_5 over $\mathbb{Q}$ by Lemma 3.2 applied to $m(x+1)$ with prime $p = 5$; indeed, $m(x+1) = x^4 + 5x^3 + 10x^2 + 10x + 5$. This means that

$$[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = [\zeta_5 : \mathbb{Q}] = \deg(m(x)) = 4.$$

Finally, define $d = [\mathbb{Q}(\sqrt[5]{11}, \zeta_5) : \mathbb{Q}(\sqrt[5]{11})]$. These dimensions are captured in Figure 1.

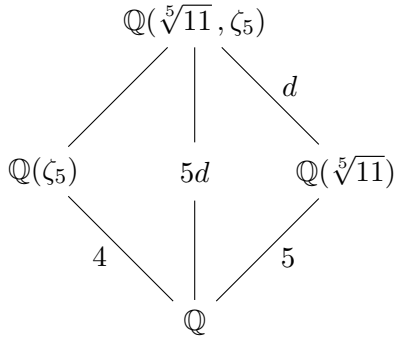

Figure 1. The field extension $\mathbb{Q}(\sqrt[5]{11}, \zeta_5)$ over $\mathbb{Q}$.

Since vector space dimension is well-defined, we see that $[\mathbb{Q}(\sqrt[5]{11}, \zeta_5) : \mathbb{Q}] = 5d$ and that $5d$ must be divisible by 4.

We can further show that $m(x)$ remains the minimal polynomial of ζ_5 over $\mathbb{Q}(\sqrt[5]{11})$. We know that by defnition, the minimal polynomial of the algebraic element ζ_5 is the unique monic generator of the ideal $I = \{f(x) \in \mathbb{Q}(\sqrt[5]{11})[x] | f(\zeta_5) = 0\}$. Furthermore, by [4, Corollary 9.11], any nonzero monic polynomial of minimal degree in I is also the unique generator of I. Since the coefficients of $m(x)$ are in $\mathbb{Q} \supset \mathbb{Q}(\sqrt[5]{11})$, $m(x) \in I$. From here, we only need to show that $m(x)$ is of minimal

degree in I. Since d must be divisible by 4, we have that if $n(x)$ generates I, $deg(n(x)) \geq 4$. Since $m(x) \in I$, it must be that $m(x) = n(x)s(x)$ for some $s(x) \in \mathbb{Q}(\sqrt[5]{11})[x]$, and thus by properties of polynomial degrees, $deg(n(x)) \leq 4$. Therefore, $deg(m(x)) = 4$ is minimal in I.