A Guide for Finding Minimal Polynomials of Algebraic Numbers

Robert Sweeney Blanco

Contents

1 Introduction

Finding minimal polynomials is a classic Abstract Algebra problem, but most Field Theory texts don't give readers a good method for finding them. This guide provides some helpful tools and formulas that can help find the minimal polynomials of simple and very complicated algebraic numbers.

2 The Resultant

This section will define the resultant, a powerful tool with a wide range of applications. The resultant will be the primary tool this guide will use for finding minimal polynomials.

Definition. *The Sylvester Matrix of two polynomials $P_1(x) = a_m x^m + ... + a_0$ and $P_2(x) = b_n x^n + ... + b_0$ is the $(m+n) \times (m+n)$ square matrix S such that*

$$S_{i,j} = \begin{cases} a_{m+i-j} & i \leq n \quad and \quad j \leq m+i \quad and \quad j \geq i \\ b_{i-j} & i > n \quad and \quad j \leq i \quad and \quad j \geq i-n \\ 0 & otherwise \end{cases}$$

Example. *Suppose $P_1(x) = x^3 - x^2 - 10x + 8$ and $P_2(x) = x^2 + 2x - 3$, then the corresponding Sylvester Matrix is*

$$\begin{bmatrix} 1 & -1 & -10 & 8 & 0 \\ 0 & 1 & -1 & 10 & 8 \\ 1 & 2 & -3 & 0 & 0 \\ 0 & 1 & 2 & -3 & 0 \\ 0 & 0 & 1 & 2 & -3 \end{bmatrix}$$

Next we will define a useful concept known as the resultant, which has a wide range of applications in several fields of mathematics, most noticeably in Number Theory. There are different conventions of defining what a resultant is, so I will provide the two most common ones.

Definition 1. *Given $P(x) = p_n x^n + p_{n-1} x^{n-1} + ... + p_0 \in K[x] \quad p_n \neq 0$ with roots $\alpha_i \quad 1 \leq i \leq n$ and $Q(x) = q_m x^m + q_{m-1} x^{m-1} + ... + q_0 \in K[x] \quad q_m \neq 0$ with roots $\beta_j \quad 1 \leq j \leq m$, the resultant with respect to x is $Res_x(P, Q) = p_n^m q_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$.*

Definition 2. *The resultant of two polynomials is the determinant of their Sylvester Matrix*

Both these definitions can be shown to be equivalent. We will be using the latter for the majority of this expository. Many sources may use the convention of compute the resultant using the transpose of the Sylvester Matrix, which by the property of determinants has no effect on the result. However, the first definition of the resultant provides a useful application of resultants, which is states in the following theorem.

Theorem 1. *Two polynomials $P_1(x)$ and $P_2(x)$ have a shared root iff their resultant equals 0.*

Proof. Let $P(x) = p_n x^n + p_{n-1} x^{n-1} + ... + p_1 x + p_0 \in K[x]$ where $p_n \neq 0$ with roots $\alpha_i \quad 1 \leq i \leq n$ and $Q(x) = q_m x^m + q_{m-1} x^{m-1} + ... + q_1 x + q_0 \in K[x]$ where $q_m \neq 0$ with roots $\beta_j \quad 1 \leq j \leq m$
($\Rightarrow$) Suppose P and Q have a shared root. Then $\exists i, j$ s.t. $\alpha_i = \beta_j \Rightarrow (\alpha_i - \beta_j) = 0 \Rightarrow p_n^m q_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = 0 \Rightarrow Res_x(P, Q) = 0$
($\Leftarrow$) Suppose $Res_x(P, Q) = 0 \Rightarrow p_n^m q_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = 0$. Since K is a field, it has no zero divisors, which implies $\exists i, j$ s.t. $\alpha_i = \beta_j$. □

One can use this theorem to show that the two polynomials featured in Example 1 have a common root without having to factor them. The main purpose of the resultant in this section of the paper is to compute minimal polynomials.

3 Irreducibility over $\mathbb{Q}$

Every minimal polynomial must be irreducible by definition. This section provides methods for checking if a polynomial is irreducible. The easiest cases to check for irreducibility are quadratic and cubic polynomials.

Theorem. *Let F be a field and $f \in F[x]$ be a quadratic or cubic. Then f is irreducible over F iff f has no zeros in F.*

Corollary. *A monic quadratic polynomial $x^2 + a_1 x + a_0 \in \mathbb{Q}[x]$ is irreducible iff its discriminant $a_1^2 - 4a_0$ is not a perfect square.*

For cubic polynomials, one can take advantage of the rational root theorem for determining irreducibility over $\mathbb{Q}$.

Theorem. *The rational roots of the monic polynomial $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$ are integer factors of a_0.*

Corollary. *A monic cubic polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ iff there is not an integer factor of the constant term that is a root of the polynomial.*

For determining the irreducibility of a polynomial of degree greater than three, one can use the famous Eisenstein's Criterion stated below.

Theorem. *A monic polynomial $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$ is irreducible if there exists a prime p such that $p|a_i$ $\forall i$ and $p^2 \nmid a_0$.*

Although the Eisenstein Criterion is extremely useful, it may sometimes fail to apply. Notice that the theorem is not an 'if and only if' statement, so there are some polynomials that are irreducible but cannot be proven with the Eisenstein Criterion. In such situations, it may be useful to study the problem in a finite field. The following section will explain how modular arithmetic can help determine irreducibility.

4 Irreducibility over finite fields

In cases where the Eisenstein Criterion fails to prove irreducibility, it may be useful to tackle the problem in a finite field. The following theorem demonstrates how modular arithmetic can lend a helping hand. This theorem can be helpful in cases where the Eisenstein Criterion fails to apply or the coefficients of the polynomial are extremely large and difficult to work with.

Theorem. *For any monic polynomial $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$, if there exists a prime p such that $x^n + \widehat{a}_{n-1}x^{n-1} + ... + \widehat{a}_1x + \widehat{a}_0$ is irreducible in $\mathbb{Z}_p$ where $\widehat{a}_i \equiv a_i \pmod{p}$ and , then the polynomial is irreducible.*

In order to check for irreducibility in $\mathbb{Z}_p$, one can use Rabin's algorithm, which is based on the theorem below.

Theorem. *Let $d_1, d_2, ..., d_k$ be all the prime divisors of n and denote $\frac{n}{d_i} = n_i$ for $1 \leq i \leq k$. A polynomial $f \in \mathbb{Z}_p[x]$ (where p is prime) of degree n is irreducible in $\mathbb{Z}_p[x]$ iff $gcd(f, x^{p^{n_i}} - x) = 1$ for $1 \leq i \leq k$, and f divides $x^{p^n} - x$. [**?**]*

This is a very useful theorem but can be a bit of a challenge to use considering it is used in the context of $\mathbb{Z}_p$, so the traditional Euclid's algorithm is not applicable. There are many ways of finding the greatest common divisor in $\mathbb{Z}_p$, however it may be easiest to use the resultant from the earlier section.

Theorem. *Let $a, b \in \mathbb{Z}[x]$ and p be a prime number not dividing the leading coefficients of both a and b. Define $c = gcd(a, b)$ over $\mathbb{Z}$. Then $p \nmid Res_x(\frac{a}{c}, \frac{b}{c}) \Rightarrow gcd(a_p, b_p) = c \pmod{p}$ where a_p and b_p are the images of a and b modulo p. [**?**]*

These theorems, in combination, can be used to help prove irreducibility. When working in a finite field, however, there are usually only a small number of possible irreducible polynomials for any given degrees. The following theorem can help us generate irreducible polynomials.

Theorem. *Let $n \geq 1$. In $\mathbb{Z}_p$, $x^{p^n} - x = \prod_{d|n} \prod_{\substack{deg(\pi)=d \\ \pi \text{ is monic}}} \pi(x)$, where π is an irreducible polynomial. [?]*

Notice this theorem makes perfect sense based on our previous theorems. The theorem for Rabin's algorithm can be seen as a corollary to this theorem. Using this theorem, one can make a list of irreducible polynomials given some finite field and degree.

Example. *Here we will produce a list of irreducible polynomials in $\mathbb{Z}_2$. We know that the product of all linear, irreducible polynomials in $\mathbb{Z}_2$ equals $x^2 - x = x(x+1)$. For finding quadratic, irreducible polynomials in $\mathbb{Z}_2$, factor $x^4 - x$ knowing that both x and $x+1$ will be factors. This results in $x^4 - x = x(x+1)(x^2+x+1)$. For finding cubic, irreducible polynomials in $\mathbb{Z}_2$, factor $x^8 - x$ knowing x and $x+1$ will be factors. This results in $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$. For finding quartic, irreducible polynomials in $\mathbb{Z}_2$, factor $x^{16} - x$ knowing x, $x+1$, and x^2+x+1 will be factors. This results in $x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$. Working out higher degrees gives the following table of irreducible polynomials in $\mathbb{Z}_2[x]$*

Degree	*Irreducibles in $\mathbb{Z}_2$*
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1
4	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$
5	x^5+x^2+1, x^5+x^3+1, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x+1$, $x^5+x^4+x^3+x^2+1$
6	x^6+x+1, x^6+x^3+1, $x^6+x^4+x^2+x+1$, $x^6+x^4+x^3+x+1$, x^6+x^5+1, $x^6+x^5+x^2+x+1$, $x^6+x^5+x^3+x^2+1$, $x^6+x^5+x^4+x+1$, $x^6+x^5+x^4+x^2+1$

When working out all the irreducible polynomials in some finite field, it is often useful to know how many of them there should be. Luckily there is a theorem that can provide that information.

Theorem. *The number of irreducible polynomials of degree n in $\mathbb{Z}_p$ equals $\frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})p^d$, where μ is the Mobius function. [?]*

One can use this formula to check that the chart above has the correct number of irreducible polynomials. Thanks to the formula, we know that in order to expand the chart to include polynomials of degree 7, there would need to be exactly 18 polynomials in that category. Using the Eisenstein Criterion and reducing the polynomial to a finite field should be able to prove irreducibility in almost any case. Using the techniques above, one can check whether a polynomial is irreducible in order to qualify it as being the minimal polynomial of some algebraic number. The following sections will provide techniques for finding possible minimal polynomials of algebraic numbers.

5 Minimal polynomials of roots

We begin by showing how to find the minimal polynomial of a root of any algebraic number given that we know the minimal polynomial of the number itself. Let $P(x) \in K[x]$ be the minimal polynomial for α.

Formula 1. *The minimal polynomial of* $\sqrt[r]{\alpha}$ *divides* $R(t) = P(t^r)$

Example. *Find the minimal polynomial of* $\sqrt{p}$ *for any prime* p *over* $\mathbb{Q}$

Since $p \in \mathbb{Q}$*, its minimal polynomial is simply* $P(x) = x - p$*. Thus* $\sqrt{p}$ *is a root of* $R(t) = P(t^2) = t^2 - p$*. This must be the minimal polynomial since it satisfies the Eisenstein Criterion using* p *as the prime.*

Example. *One of the most famous constants in mathematics is the Golden Ratio,* ϕ*. It is the limit of the ratio of consecutive terms in the Fibonacci Sequence. Given the fact that* $\phi^2 = \phi + 1$*, find the minimal polynomial of* $\sqrt[3]{\phi}$ *over* $\mathbb{Q}$*.*

Since $\phi \notin \mathbb{Q}$*, the degree of the field extension* $[\mathbb{Q}(\phi) : \mathbb{Q}]$ *is at least two. Thus* $x^2 - x - 1$ *is the minimal polynomial of* ϕ*. Using the formula above, one can see that the minimal polynomial of* $\sqrt[3]{\phi}$ *divides* $R(t) = P(t^3) = t^6 - t^3 - 1$*. Writing the coefficients in* $\mathbb{Z}_2$ *gives* $\widehat{R}(t) = t^6 + t^3 + 1$*, which is irreducible by the chart in the previous section. Thus* $t^6 - t^3 - 1$ *is the minimal polynomial of* $\sqrt[3]{\phi}$*.*

6 Minimal polynomials of sums

This section will allow us to find the minimal polynomials for any linear combination of elements in a field extension for which we know their minimal polynomial. Let $P(x) \in K[x]$ be the minimal polynomial for α and $Q[x] \in K[x]$ be the minimal polynomial for β.

Formula 2. *The minimal polynomial of* $\alpha + \beta$ *divides* $R(t) = Res_x(P(t - x), Q(x))$

Example. *Calculate the minimal polynomial for* $1 + \sqrt{3}$ *over* $\mathbb{Q}$

Let $\alpha = 1$ with minimal polynomial $P(x)$ and $\beta = \sqrt{3}$ with minimal polynomial $Q(x)$. We know from the previous section $P(x) = x - 1$ and $Q(x) = x^2 - 3$. Using the formula above calculates a polynomial with $1 + \sqrt{3}$ as a root as

$$Res_x(t - x - 1, x^2 - 3) = \begin{vmatrix} -1 & t-1 & 0 \\ 0 & -1 & t-1 \\ 1 & 0 & -3 \end{vmatrix} = t^2 - 2t - 2.$$

The discriminant of this quadratic polynomial is 12, thus it is irreducible, making it the minimal polynomial of $1 + \sqrt{3}$ over $\mathbb{Q}$.

Example. *Calculate the degree of the field extension from the rationals to the cyclotomic field for the cubic root of unity $\zeta_3 = e^{\frac{2\pi i}{3}}$*

Let $\alpha = \Re(\zeta_3) = \frac{-1}{2}$ and $\beta = \Im(\zeta_3) = \frac{\sqrt{3}}{2}$. Let $P(x) = x + \frac{1}{2}$, the minimal polynomial of α, and $Q(x) = x^2 + \frac{3}{4}$, the minimal polynomial of β. By the formula, the minimal polynomial of ζ_3 equals $Res_x(t - x + \frac{1}{2}, x^2 + \frac{3}{4})$

$= \begin{vmatrix} -1 & t+\frac{1}{2} & 0 \\ 0 & -1 & t+\frac{1}{2} \\ 1 & 0 & \frac{3}{4} \end{vmatrix} = t^2 + t + 1$. *The discriminant of this polynomial is -3, thus it is irreducible, which makes it the minimal polynomial.*
$\therefore [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$

As a matter of fact, it can be shown that for any prime p, the pth primitive root of unity ζ_p, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. This result can be generalized to show that the nth primitive root of unity ζ_n, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ where ϕ is the Euler totient function. This extension can be shown to be a Galois extension, meaning the extension is normal and separable.

7 Minimal polynomials of quotients and products

Let $P(x) \in K[x]$ be the minimal polynomial for α and $Q[x] \in K[x]$ be the minimal polynomial for β.

Formula 3. *The minimal polynomial of $\frac{\alpha}{\beta}$ divides $R(t) = Res_x(P(tx), Q(x))$*

Example. *Find the minimal polynomial of $\frac{\sqrt[3]{4}}{i+1}$ over $\mathbb{Q}$*

Using methods provided in earlier sections, one can show that $P(x) = x^2 - 2x + 2$ and $Q(x) = x^3 - 4$. Using the formula, the minimal polynomial of $\frac{\sqrt[3]{4}}{i+1}$ divides

$$Res_x(t^3x^3-4, x^2-2x+2) = \begin{vmatrix} t^3 & 0 & 0 & -4 & 0 \\ 0 & t^3 & 0 & 0 & -4 \\ 1 & -2 & 2 & 0 & 0 \\ 0 & 1 & -2 & 2 & 0 \\ 0 & 0 & 1 & -2 & 2 \end{vmatrix} = 8t^6+16t^3+16,$$

thus it also divides t^6+2t^3+2, which is irreducible by the Eisenstein Criterion using 2 as the prime. Thus t^6+2t^3+2 is the minimal polynomial of $\frac{\sqrt[3]{4}}{i+1}$

It is possible to come up with a formula for the minimal polynomial of the product of two algebraic numbers by using the formula for the quotient. one just has to realize that $\alpha\beta = \frac{\alpha}{\frac{1}{\beta}}$.

Formula 4. *The minimal polynomial of $\alpha\beta$ divides $R(t) = Res_x(P(xt), Res_y(xy-1, Q(y)))$*

Example. *Find the minimal polynomial of $5\zeta_3$ over $\mathbb{Q}$.*

We know from an earlier section that the minimal polynomial of ζ_3 is x^2+x+1 and it should be obvious that the minimal polynomial of 5 is $x-5$. Thus the minimal polynomial we are looking for divides $R(t) = Res_x(tx-5, Res_y(xy-1, y^2+y+1))$. $Res_y(xy-1, y^2-y+1) = \begin{vmatrix} x & -1 & 0 \\ 0 & x & -1 \\ 1 & 1 & 1 \end{vmatrix}$

$= x^2+x+1$ $Res_x(tx-5, x^2+x+1) = \begin{vmatrix} t & -5 & 0 \\ 0 & t & -5 \\ 1 & 1 & 1 \end{vmatrix} = t^2+5t+25$. The discriminant of this polynomial is -75, thus it is irreducible. Note this may be an obvious result, but it demonstrates the method well.

8 Summary

Combining all the sections above provides ample tools for finding minimal polynomials of complicated algebraic numbers.

Formula 1. *The minimal polynomial of $\sqrt[r]{\alpha}$ divides $R(t) = P(t^r)$*

Formula 2. *The minimal polynomial of $\alpha+\beta$ divides $R(t) = Res_x(P(t-x), Q(x))$*

Formula 3. *The minimal polynomial of $\frac{\alpha}{\beta}$ divides $R(t) = Res_x(P(tx), Q(x))$*

Formula 4. *The minimal polynomial of $\alpha\beta$ divides $R(t) = Res_x(P(xt), Res_y(xy-1, Q(y)))$*

Example. *Define ψ as the only real root of $x^5 - x - 1$. ψ is not in a radical extension of $\mathbb{Q}$, a property only roots of polynomials of degree greater than four can have as proven by the Abel-Ruffini Theorem. Also allow ϕ be the Golden Ratio as mentioned in a previous section and ζ_3 be the primitive cube root of unity $e^{\frac{2\pi i}{3}}$. Find the minimal polynomial of $\sqrt{\frac{\psi\sqrt[3]{\phi}}{\zeta_3+1}}$ over $\mathbb{Q}$.*

In order to solve this challenging problem, we must break it into smaller pieces. First, to find the minimal polynomial of $\zeta_3 + 1$. Using formula 2, we can see this polynomial divides $Res_x(-x+t-1, x^2+x+1) = \begin{vmatrix} -1 & t-1 & 0 \\ 0 & -1 & t-1 \\ 1 & 1 & 1 \end{vmatrix}$ $= t^2 - t + 1$. The discriminant of this polynomial is -3, thus it is irreducible which makes it the minimal polynomial of $\zeta_3 + 1$. Next find the minimal polynomial of $\psi\sqrt[3]{\phi}$. We know from Section 3 that the minimal polynomial of $\sqrt[3]{\phi}$ is $x^6 - x^3 - 1$. Using formula 4, we see that the minimal polynomial of $\psi\sqrt[3]{\phi}$ is $Res_x(t^5x^5 - tx - 1, Res_y(xy-1, y^6 - y^3 - 1))$.

$$Res_y(xy-1, y^6-y^3-1) = \begin{vmatrix} x & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & x & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & x & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & x & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & x & -1 \\ 1 & 0 & 0 & -1 & 0 & 0 & -1 \end{vmatrix} = -x^6 - x^3 + 1.$$

Thus the minimal of $\psi\sqrt[3]{\phi}$ is $Res_x(t^5x^5 - tx - 1, -x^6 - x^3 + 1) =$

$$\begin{vmatrix} t^5 & 0 & 0 & 0 & -t & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & t^5 & 0 & 0 & 0 & -t & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & t^5 & 0 & 0 & 0 & -t & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & t^5 & 0 & 0 & 0 & -t & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & t^5 & 0 & 0 & 0 & -t & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & t^5 & 0 & 0 & 0 & -t & -1 \\ -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 1 \end{vmatrix}$$

$= t^{30} - 12t^{21} - 7t^{18} - 11t^{15} - 9t^{12} - 3t^9 - 8t^6 + t^3 - 1$. *Using formula 3, the minimal polynomial of $\frac{\psi\sqrt[3]{\phi}}{\zeta_3+1}$ equals $Res_x((xt)^{30} - 12(xt)^{21} - 7(xt)^{18} - 11(xt)^{15} -$*

$$9(xt)^{12} - 3(xt)^{9} - 8(xt)^{6} + (xt)^{3} - 1, x^2 - x + 1) =$$

$$\begin{vmatrix}
t^{30} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -12 * t^{21} & 0 & 0 & -7 * t^{18} & 0 & 0 & -11 * t^{15} & 0 & 0 & 9 * t^{12} & 0 & 0 & -3 * t^{9} & 0 & 0 & -8 * t^{6} & 0 & 0 & t^{3} & 0 & 0 & -1 & 0 \\
0 & t^{30} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -12 * t^{21} & 0 & 0 & -7 * t^{18} & 0 & 0 & -11 * t^{15} & 0 & 0 & 9 * t^{12} & 0 & 0 & -3 * t^{9} & 0 & 0 & -8 * t^{6} & 0 & 0 & t^{3} & 0 & 0 & -1 \\
1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 1
\end{vmatrix}$$

$= (t^{30} + 12t^{21} - 7t^{18} + 11t^{15} + 9t^{12} + 3t^{9} - 8t^{6} - t^{3} - 1)^2$. *Thus the minimal polynomial must divide* $t^{30} + 12t^{21} - 7t^{18} + 11t^{15} + 9t^{12} + 3t^{9} - 8t^{6} - t^{3} - 1$. *Finally to account for the square root, we can use the first equation to say that the minimal polynomial divides* $t^{60} + 12t^{42} - 7t^{36} + 11t^{30} + 9t^{24} + 3t^{18} - 8t^{12} - t^{6} - 1$. *This polynomial does not satisfy the Eisenstein Criterion and is also not irreducible in* $\mathbb{Z}_2$. *Although it is possible to prove this polynomial is irreducible using theorems presented in previous sections, the computational work required is extremely heavy. One can simply use Wolfram Alpha to check if the polynomial has a factorization over* $\mathbb{Q}$, *which it doesn't. This method can also be used to check that each polynomial found in every step of this problem was indeed irreducible. This gives the result that the minimal polynomial of* $\sqrt{\frac{\psi \sqrt[3]{\phi}}{\zeta_3 + 1}}$ *over* $\mathbb{Q}$ *is* $t^{60} + 12t^{42} - 7t^{36} + 11t^{30} + 9t^{24} + 3t^{18} - 8t^{12} - t^{6} - 1$.

References

[1] Daniel Panario, Boris Pittel, Bruce Richmond, and Alfredo Viola *Analysis Of Rabin's Irreducibility Test For Polynomials Over Finite Fields*

[2] Franz Winkler *Polynomial Algorithms in Computer Algebra*

[3] Keith Conrad *Roots and Irreducibles*

[4] Lindsay N. Childs *A Concrete Introduction to Higher Algebra*