Galois Theory: On Algebraic Expressions

Research Question: What are the implications of Galois theory on the algebraic expressions of the roots of unity and the roots of polynomials?

Abstract

The scope of Galois theory encompasses both group theory and field theory. It characterizes polynomial equations using the Galois groups of field extensions, which may be utilized to show certain properties of algebraic numbers and their algebraic expressions involving rational numbers and the algebraic operations ($+$, $-$, $\times$, $\div$, nth-roots). In this essay, I investigate how Galois theory can be used to determine the existence and the types of roots needed in the algebraic expressions of the roots of unity, i.e. $\zeta_n \coloneqq \mathrm{e}^{2\pi i/n}$ where $n \in \mathbb{Z}^+$. Then I show that the solvability of a polynomial's Galois group is a necessary and sufficient condition for the existence of algebraic expressions for its roots, hence concluding that polynomial equations of degree 5 or higher are not in general solvable by radicals.

Preliminaries

To facilitate discussion, I will use terminologies and employ certain notations common in Galois theory repeatedly; their definitions may be found in Appendix A. Lemmas or other minor assumptions not important to the main discussion are either proven in Appendix B or cited with a reference.

In this essay, I work only with groups of finite order, algebraic number fields, i.e. fields F such that $[F : \mathbb{Q}]$ is finite[1], and unless otherwise specified, polynomials have distinct roots[2].

Lemma 1. Let E/F be a field extension and $\phi \in \mathrm{Gal}(E/F)$. If $f \in F[x]$ is a polynomial of which $x \in F$ is a root, then so is $\phi(x)$.

Lemma 2. Let $E = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$ be obtained as a series of simple extensions of F:
(1) If $m = 1$, and f is the minimal polynomial of $\alpha \coloneqq \alpha_1$ over F, then $[E : F] = \deg f$;
(2) For every $z \in E$, there exists $g \in F[x_1, x_2, \cdots, x_m]$ such that $z = g(\alpha_1, \alpha_2, \cdots, \alpha_m)$;
(3) Every $\phi \in \mathrm{Gal}(E/F)$ is uniquely determined by $\phi(\alpha_i)$ for all $1 \leq i \leq m$.

Lemma 3. Let M/F be a field extension:
(1) If M/F is Galois, any irreducible polynomial in $F[x]$ with one root in M splits over M;
(2) If M/F is Galois, then $|\mathrm{Gal}(M/F)| = [M : F]$;
(3) M/F is Galois if and only if M is the splitting field of some $f \in F[x]$ over F.

Lemma 4 (Fundamental Theorem of Galois Theory (FTGT)). If M/F is a Galois extension, then there exists a one-to-one correspondence from the subgroups $H \subseteq \mathrm{Gal}(M/F)$ to the intermediate subfields $F \subseteq K \subseteq M$, given by:

$$H \to M^H \qquad \text{or} \qquad K \to \mathrm{Gal}(M/K)$$

Lemma 5. Let $F \subseteq K \subseteq M$ where M/F is Galois, and define $G \coloneqq \mathrm{Gal}(M/F)$ and $N \coloneqq \mathrm{Gal}(M/K)$:
(1) K/F is Galois if and only if $N \trianglelefteq G$;
(2) If K/F is Galois, $\mathrm{Gal}(K/F) \cong G/N$.

Lemma 6. Let G be a group:
(1) (Lagrange's Theorem) Every subgroup $H \subseteq G$ has order dividing $|G|$;
(2) If $N \trianglelefteq G$, then $|G/N| = |G|/|N|$.

[1] Therefore $\mathbb{Q}$ is the smallest field I will consider.

[2] Minimal polynomials have distinct roots, see Proposition 26.

Section 1: Roots of Unity

By Euler's formula, $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$. These values for certain n are well-known:

$$\begin{cases} \sin 2\pi/12 = 1/2 \\ \sin 2\pi/8 = \sqrt{2}/2 \\ \sin 2\pi/6 = \sqrt{3}/2 \\ \sin 2\pi/4 = 1 \end{cases}, \quad \begin{cases} \cos 2\pi/12 = \sqrt{3}/2 \\ \cos 2\pi/8 = \sqrt{2}/2 \\ \cos 2\pi/6 = 1/2 \\ \cos 2\pi/4 = 0 \end{cases}$$

Using these values, the algebraic expressions of the sine and cosine of other angles, which are the sums and differences of these angles, may be written accordingly using the compound angle formulae. But the algebraic expressions of other angles, such as $\sin(2\pi/360)$ cannot be derived using this method[3]; is it, then, still possible to express ζ_{360} and other ζ_n's algebraically, and if so, what of its properties may be derived using Galois theory?

Section 1.1: Taking n-th Roots

I will build an algebraic expression using the following method: start with $\mathbb{Q} \coloneqq F_0$, the field of rational numbers. At each step of the process, adjoin to F_i the n_ith-root of some $a \in F_i$ to obtain F_{i+1}. If the target value is contained in some F_m, then it has an algebraic expression. Thus, the condition for an algebraic expression is equivalent to requiring a field F_m containing the target value to be a radical extension of $\mathbb{Q}$, i.e. a series of simple radical extensions of $\mathbb{Q}$.

If I instead start with a field F (dubbed the 'base field') already containing all sufficient roots of unity to reach the final field E, i.e.

$$F \coloneqq F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_m = E \tag{1}$$

then each F_{i+1}/F_i is also Kummer and therefore Galois by Lemma 3, for then $F_{i+1} = F_i\left(\sqrt[n_i]{a}\right)$ will be a splitting field of $x^{n_i} - a$ over F_i with roots $\zeta_{n_i}^k \sqrt[n_i]{a} \in F_{i+1}$ for $0 \leq k \leq n_i - 1$. This allows for an easy characterization of its Galois group, since by Lemma 2, every automorphism is completely determined by where it sends $\sqrt[n_i]{a}$ to, i.e. $\zeta_{n_i}^k \sqrt[n_i]{a}$ for some k by Lemma 1, thus each automorphism corresponds to an integer k between 0 and $n_i - 1$.

Proposition 7. Define $\alpha \coloneqq \sqrt[n]{a}$ where $a \in F$, so that $F(\alpha)/F$ is simple radical, and $G \coloneqq \operatorname{Gal}(F(\alpha)/F)$:
(1) If $\zeta_n \notin F$, then $G \cong \{e\}$;
(2) Otherwise, let $\phi_k \in G$ be the unique automorphism such that $\phi_k(\alpha) = \zeta_n^k \alpha$, and q the

[3] Converting to degrees, the angles stated above are all multiples of 3. Thus $2\pi/360 = 1°$ is not reachable using the compound angle formulae.

smallest non-zero integer for which $\phi_q \in G$. Then $G = \langle \phi_q \rangle \cong \mathbb{Z}_{n/q}$, which is non-trivial unless the extension itself is trivial.

Proof (Statement 1). By Lemma 1, every automorphism must send α to itself for it is the only root of $x^n - a$, i.e. $\phi(\alpha) = \alpha$, which completely determines the full automorphism by Lemma 2. Hence $|G| = 1$, and $G \cong \{e\}$.

Proof (Statement 2). If $\zeta_n \in F$, then $F(\alpha)/F$ is Galois; by Lemma 3, then, $|G| = [F(\alpha) : F] \neq 1$ if the extension is not trivial, therefore G is not trivial. Now, for any k such that $\phi_k \in G$,

$$\phi_k(\alpha) = \zeta_n^k \alpha = \zeta_n^{pq+r} \alpha$$

where $p, r \in \mathbb{Z}$ and $0 \leq r < q$ by the division algorithm. Since $\phi_q \in G$, so is any ϕ_{-pq}, the inverse of $\phi_{pq} = (\phi_q)^p$. Then

$$(\phi_{-pq} \circ \phi_k)(\alpha) = \phi_{-pq}(\zeta_n^{pq+r} \alpha) = \zeta_n^{pq+r} \phi_{-pq}(\alpha) = \zeta_n^r \alpha$$
$$\therefore \phi_{-pq} \circ \phi_k = \phi_r \in G$$

by closure, but since $r < q$ which is already the smallest non-zero integer for which the equation holds true, $r = 0$, and

$$(\phi_{-pq} \circ \phi_k)(\alpha) = \alpha$$
$$\therefore \phi_k(\alpha) = \phi_{pq}(\alpha)$$

Hence $\phi_k = (\phi_q)^p$ and therefore $G = \langle \phi_q \rangle$. Furthermore,

$$\phi_q^{n/q}(\alpha) = (\zeta_n^q)^{n/q} \alpha = \alpha$$

Thus $(\phi_q)^{n/q}$ is the identity, and by definition, $G \cong \mathbb{Z}_{n/q}$. QED.

Proposition 7 allows concluding the cyclicality of the Galois group of an extension given the fact that it is simple radical. In particular, the Galois group is non-trivial if there exists the corresponding root of unity in the base field, so that the extension is a Kummer extension. In fact, the converse is also true: if the Galois group of an extension is cyclic and the base field contains the appropriate root of unity, then the extension must be Kummer. That is,

Proposition 8. Let E/F be a Galois extension where $\zeta_n \in F$. Then if

$$G \coloneqq \mathrm{Gal}(E/F) \cong \mathbb{Z}_n$$

then $E = F(\sqrt[n]{a})$ where $a \in F$, so that E/F is a Kummer extension.

Proof. Let $G = \langle \phi \rangle$ and $\beta \in E$. Consider

$$\alpha = \sum_{i=0}^{n-1} \zeta_n^{-i} \phi^i(\beta)$$

Hence

$$\phi(\alpha) = \sum_{i=0}^{n-1} \zeta_n^{-i} \phi^{i+1}(\beta) = \zeta_n \sum_{i=0}^{n-1} \zeta_n^{-(i+1)} \phi^{i+1}(\beta) = \zeta_n \sum_{i=0}^{n-1} \zeta_n^{-i} \phi^{i}(\beta) = \zeta_n \alpha \qquad (2)$$

$$\therefore \phi(\alpha^n) = [\phi(\alpha)]^n = (\zeta_n \alpha)^n = \alpha^n$$

which means $a \coloneqq \alpha^n \in F$ since E/F is Galois. Then

$$\alpha = \zeta_n^i \sqrt[n]{a}$$

where $0 \leq i \leq n-1$, and therefore, E contains $F(\alpha) = F\left(\zeta_n^i \sqrt[n]{a}\right) = F\left(\sqrt[n]{a}\right)$, and $F(\alpha)/F$ is Kummer and Galois by Lemma 3 for $F(\alpha)$ is the splitting field of $x^n - a \in F[x]$. But since

$$F \subseteq F(\alpha) \subseteq E$$

I can invoke FTGT and Lemma 5 to write

$$G \trianglerighteq H \trianglerighteq \{e\}$$

and use Proposition 7 (where $q = 1$ due to (2)) to conclude that

$$\text{Gal}(F(\alpha)/F) \cong G/H \cong \mathbb{Z}_n$$

But $G \cong \mathbb{Z}_n$, which implies that $H \cong \{e\}$, for $|H| = |G|/|G/H| = 1$. Invoking FTGT again concludes that $E = F(\alpha) = F\left(\sqrt[n]{a}\right)$. QED.

Naively speaking, then, if it can be shown that all the ζ_n's have algebraic expressions, then there exists a base field F containing all sufficient ζ_n's that is obtained as a radical extension of $\mathbb{Q}$; and if there is a field E containing the targeted value satisfying (1) where each $\text{Gal}(F_{i+1}/F_i)$ is cyclic, then E is a radical extension of F and therefore $\mathbb{Q}$, implying that the target value has an algebraic expression.

However, this approach is recursive if the target values are the roots of unity, as it assumes the truth for ζ_n in the base field F.

Section 1.2: Cyclotomic Extensions

Perhaps a good starting point will be the Galois group of a cyclotomic extension, as this may be helpful in utilizing Proposition 8 to show that the individual extensions are Kummer and therefore the radicality of the whole extension:

Proposition 9. Let $F(\zeta_n)/F$ be a cyclotomic extension. Then $G \coloneqq \text{Gal}(F(\zeta_n)/F) \cong \mathbb{Z}_n^\times$.

Proof. By Lemma 2, every $z \in F(\zeta_n)$ can be expressed as

$$z = \sum_{i=0}^{m} c_i \zeta_n^i$$

where $c_i \in F$ and $m = \deg f - 1$ where f is the minimal polynomial of ζ_n over F. Now let $\phi_k : F(\zeta_n) \to F(\zeta_n)$ be a homomorphism fixing F such that $\phi_k(\zeta_n) = \zeta_n^k$. It is an automorphism and is in G if and only if ϕ_k is bijective, if and only if there exists an inverse $\phi_l = \phi_k^{-1}$, where

$$(\phi_l \circ \phi_k)(z) = \sum_{i=0}^{m} c_i(\phi_l \circ \phi_k)(\zeta_n^i) = \sum_{i=0}^{m} c_i \phi_l(\zeta_n^{ik}) = \sum_{i=0}^{m} c_i \zeta_n^{ikl} = \sum_{i=0}^{m} c_i \zeta_n^i = z$$

which implies $kl \equiv 1 \pmod{n}$, if and only if k is coprime to n and therefore in $\mathbb{Z}_n^\times$. This means that

$$\phi_k \in G \Leftrightarrow k \in \mathbb{Z}_n^\times$$

Henceforth, the mapping $\sigma : G \to \mathbb{Z}_n^\times$ defined by $\sigma(\phi_k) = k$ is bijective, and for $\phi_j, \phi_k \in G$,

$$(\phi_j \circ \phi_k)(\zeta_n) = \phi_j(\zeta_n^k) = [\phi_j(\zeta_n)]^k = \zeta_n^{jk} = \phi_{jk}(\zeta_n)$$
$$\therefore \sigma(\phi_j \circ \phi_k) = \sigma(\phi_{jk}) = jk = \sigma(\phi_j)\sigma(\phi_k)$$

thus σ is an isomorphism, and $G \cong \mathbb{Z}_n^\times$. QED.

It is rather tempting to try and prove that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is radical. This is true for some n, for example, $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is Galois since ζ_3 can be expressed as

$$\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$$[4]

which includes only a square root, implying that $\zeta_3 \in \mathbb{Q}(\sqrt{-3})$. However, in general, this claim is false; for example, there exists a cube root in the algebraic expression for ζ_7, so achieving the field $\mathbb{Q}(\zeta_7)$ from $\mathbb{Q}$ requires adjoining a cube root $\sqrt[3]{a}$ to some intermediate field in the process. But this would imply that $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ is not Galois, for $\zeta_3 \notin \mathbb{Q}(\zeta_7)$ implies that $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ must fix $\sqrt[3]{a} \notin \mathbb{Q}$ (since the other roots of $x^3 - a$, i.e. $\zeta_3\sqrt[3]{a}$ and $\zeta_3^2\sqrt[3]{a}$ are not in $\mathbb{Q}(\zeta_7)$), which means $\mathbb{Q}$ is not the fixed field of the Galois group. However, $\mathbb{Q}(\zeta_7)$ is the splitting field of $x^7 - 1$ over $\mathbb{Q}$, so by Lemma 3, it is Galois, hence contradiction.

Fortunately, this issue can be resolved by first adjoining ζ_3 and then ζ_7. Luckily, as previously established, a field containing ζ_3 can itself be obtained as a radical extension of $\mathbb{Q}$, and it remains only to prove that $\mathbb{Q}(\zeta_3, \zeta_7)/\mathbb{Q}(\zeta_3)$ is radical. Generalizing this to any ζ_n, it seems likely that the expression for ζ_n only requires p-th roots with $p < n$, which will then only require the radicality of a field containing ζ_p before actually adjoining the root of unity ζ_n. If this is the case, then one may proceed by strong induction on n as follows.

Claim that, for any arbitrary F, there exists a radical extension E/F so that $\zeta_n \in E$ for positive n. Here I also claim that E/F can be expressed as a series of Kummer extensions. The base case $n = 1$ is trivial, since $\zeta_1 = 1 \in \mathbb{Q}$ is the smallest possible field. No extensions are needed, and the claim holds vacuously.

For the inductive step, consider the decomposition series of $\mathbb{Z}_n^\times$:

$$\{e\} \coloneqq H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m \coloneqq \mathbb{Z}_n^\times \qquad (3)$$

[4] Solving $x^3 - 1 = (x-1)(x^2 + x + 1) = 0$ shows that the roots are $x = 1$ and $x = (-1 \pm i\sqrt{3})/2$ (by the quadratic formula), and since $\zeta_3 = e^{2\pi i/3}$ lies in the upper half of the complex plane, it must be chosen that $\zeta_3 = (-1 + i\sqrt{3})/2$.

and conjecture that if every

$$H_{i+1}/H_i \cong \mathbb{Z}_{d_i}, \qquad d_i < n \tag{4}$$

then there exists $\tilde{F}$ containing all ζ_{d_i}'s such that $\tilde{F}/F$ is radical and composed of a series of Kummer extensions by the inductive hypothesis, obtained by extending to a field containing ζ_{d_i} for each i. Let the desired field containing ζ_n be

$$E = \tilde{F}(\zeta_n)$$

so that $\mathrm{Gal}(E/F) \cong \mathbb{Z}_n^\times$ by Proposition 9 (if ζ_n is already in $\tilde{F}$ then the proof is done), which has a decomposition series given by (3). Since, by Lemma 3, $E/\tilde{F}$ is Galois for E is the splitting field of $x^n - 1$ over $\tilde{F}$, one may invoke FTGT to obtain (1) (with $\tilde{F}$'s replacing F's), where each $\tilde{F}_{i+1}/\tilde{F}_i$ is Galois by Lemma 5. Since

$$\mathrm{Gal}(F_{i+1}/F_i) \cong H_{i+1}/H_i \cong \mathbb{Z}_{d_i}$$

and $\zeta_{d_i} \in \tilde{F} \subseteq \tilde{F}_i$, by Proposition 8, then, each $\tilde{F}_{i+1}/\tilde{F}_i$ is Kummer, and $E/\tilde{F}$ is radical and composed of a series of Kummer extensions, therefore so is E/F, proving the claim, for $\zeta_n \in E$. Then apply the claim to $F = \mathbb{Q}$ to obtain the desired result.

The verification of the claim relies on the truth of the conjecture in (4), i.e. the factors of $\mathbb{Z}_n^\times$ must not only be cyclic, but of an order less than n. Since the factors of a group are a property of the group itself and not the field it represents, in the following section, it suffices to limit my attention to group theory to prove the cyclicality of its factors.

Section 1.3: Composition Factors of Abelian Groups

I need only prove that $\mathbb{Z}_n^\times$ factors into cyclic groups of order less than n for verifying the existence of algebraic expressions for ζ_n. As a general observation:

Proposition 10. Every group has a simple cyclic subgroup.

Proof. For any group G and arbitrary $g \in G$, by closure, G contains the set

$$H \coloneqq \{g^k | k \geq 1\}$$

which must be finite, so there exists $i < j$ where $g^i = g^j$, implying that $g^{j-i} = e$. Then by definition, G has as its subgroup $H = \langle g \rangle$ which is cyclic. For further reduction to a simple subgroup, pick a prime p dividing $|H|$ and notice that $\langle g^{|H|/p} \rangle \cong \mathbb{Z}_p$, which is simple[5] and a subgroup of G. QED.

This is especially convenient as any subgroup N of an abelian group G is normal, since for $g \in G$ and $n \in N$,

$$gng^{-1} = gg^{-1}n = n \in N$$

implying that $N \trianglelefteq G$. Hence $\mathbb{Z}_p$ is a simple and normal subgroup of G, and therefore a factor

[5] Sheng, G. (2022). On the Classification of Finite Simple Groups. *Massachusetts Institute of Technology*, p. 5–6. https://math.mit.edu/research/highschool/primes/circle/documents/2022/Gracie.pdf

of G. Any abelian group, then, must have at least one cyclic factor. This applies to $\mathbb{Z}_n^\times$ as it is abelian due to the commutativity of multiplication.

What about the remaining factors? One may conjecture that, in general, analogous to natural numbers, factors of any group G that are not factors of some $N \trianglelefteq G$ are the factors of G/N. To see this, first notice that if $N \subseteq H \subseteq G$, then

$$H \trianglelefteq G \Rightarrow H/N \trianglelefteq G/N$$

since

$$(gN)(hN)(g^{-1}N) = (ghg^{-1})N \in H/N$$

Hence, from a partially refined decomposition series of G:

$$\{e\} \trianglelefteq N \coloneqq H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m \coloneqq G$$

where H_{i+1}/H_i is simple, I can write

$$\{e\} \cong H_0/N \lhd H_1/N \lhd H_2/N \lhd \cdots \lhd H_m/N = G/N \tag{5}$$

for $N \trianglelefteq H_i$ because $N \trianglelefteq G$ and therefore $h_i n h_i^{-1} \in N$ where $h_i \in H_i \subseteq G$. This looks like a full decomposition series for G/N with factors $(H_{i+1}/N)/(H_i/N)$. In fact,

Proposition 11 (Third Isomorphism Theorem). If $N \subseteq H \subseteq G$ and both N and H are normal in G,

$$G/H \cong (G/N)/(H/N)$$

Proof. Consider the map $\sigma : G/H \to (G/N)/(H/N)$ defined by

$$\sigma(gH) = (gN)(H/N)$$

First, check if σ is well-defined. Let some coset be expressed in two ways $gH = g'H$ where $g' = gh$ for some $h \in H$. Then

$$\begin{aligned}\sigma(g'H) &= (g'N)(H/N) = \big((gh)N\big)(H/N)\\ &= \big((gN)(hN)\big)(H/N)\\ &= (gN)(H/N) = \sigma(gH)\end{aligned}$$

where the penultimate equality holds since $hN \in H/N$. Now, since every element in $(G/N)/(H/N)$ is of the form $(gN)(H/N)$ where $g \in G$ and is thus mapped from gH, σ is surjective; and since both groups have the same order, i.e. $|G|/|H|$, σ is bijective. For satisfying the homomorphism property,

$$\begin{aligned}\sigma\big((gH)(g'H)\big) &= \sigma\big((gg')H\big)\\ &= \big((gg')N\big)(H/N) = \big((gN)(g'N)\big)(H/N)\\ &= \big((gN)(H/N)\big)\big((g'N)(H/N)\big)\\ &= \sigma(gH)\sigma(g'H)\end{aligned}$$

where $g, g' \in G$. Thus, σ is an isomorphism and the two groups are isomorphic. QED.

Thus, the individual quotient subgroups in (5) are isomorphic to H_{i+1}/H_i, which by construction are simple; thus (5) is indeed a full decomposition series, and the various

H_{i+1}/H_i, the factors of G that are not factors of N, are indeed factors of G/N. I can now proceed with the main proof of the conjecture (4):

Proposition 12. Let G be abelian. Then it factors into cyclic groups of prime order according to the prime factorization of $n \coloneqq |G|$. That is, if

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$$

then the factors of G include k_1 copies of $\mathbb{Z}_{p_1}$, k_2 copies of $\mathbb{Z}_{p_2}$... and k_m copies of $\mathbb{Z}_{p_m}$.

Proof. Proceed with strong induction on n. For the base case $n = 1$, I have $G = \{e\}$ which has no factors, therefore the claim holds vacuously. For the inductive step, by Proposition 10, there exists $\mathbb{Z}_p \trianglelefteq G$ for some prime p. As argued above, the factors of G excluding $\mathbb{Z}_p$ are the factors of $G/\mathbb{Z}_p$. Its order may be written in terms of the prime factorization of $n = |G|$, where without loss of generality,

$$p|G/\mathbb{Z}_p| = n = p^{k_0} q_1^{k_1} q_2^{k_2} \cdots q_m^{k_m} = p \cdot \left(p^{k_0 - 1} q_1^{k_1} q_2^{k_2} \cdots q_m^{k_m}\right)$$

Notice that $|G/\mathbb{Z}_p| = n/p < n$, and it is abelian, since for $g\mathbb{Z}_p, g'\mathbb{Z}_p \in G/\mathbb{Z}_p$,

$$(g\mathbb{Z}_p)(g'\mathbb{Z}_p) = (gg')\mathbb{Z}_p = (g'g)\mathbb{Z}_p = (g'\mathbb{Z}_p)(g\mathbb{Z}_p)$$

where the second equality results since G is abelian. Thus, I can apply the inductive hypothesis to conclude that all its factors are cyclic according to the prime factorization of $|G/\mathbb{Z}_p|$. Comparing G to $G/\mathbb{Z}_p$, the prime factorization of n has an additional p that matches the additional factor of $\mathbb{Z}_p$ for G. Hence, all factors of G are cyclic according to the prime factorization of n, hence proven. QED.

Proposition 12 confirms that $\mathbb{Z}_n^\times$ has cyclic factors. Their orders also divide n by Lemma 6, so they must be smaller than n, proving the conjecture (4). Hence, as argued in Section 1.2:

Theorem 13. For any positive integer n and field F, there exists radical E/F which can be expressed as a series of Kummer extensions such that $\zeta_n \in E$.
(Partial) Corollary. Every ζ_n has an algebraic expression[6].

Section 1.4: The Algebraic Expressions for ζ_n

In the preceding sections I have guaranteed the existence of algebraic expressions for all roots of unity. However, their specific expressions themselves cannot be obtained from Galois theory, and elementary methods must be used to a certain extent. However, some information may be extracted, specifically, the types of nth roots present in the algebraic expression, without resorting to elementary methods.

Consider that for instance the algebraic expression for ζ_{23} be investigated. To do so I would need the smallest radical extension of $\mathbb{Q}$ that contains ζ_{23}; a natural first candidate is the

[6] Obtained by setting $F = \mathbb{Q}$.

field $\mathbb{Q}(\zeta_{23})$, but as argued in Section 1.2 it is not necessarily a radical extension of $\mathbb{Q}$, because it may contain roots whose corresponding root of unity is not in $\mathbb{Q}(\zeta_{23})$. However, instead of starting from the roots in the algebraic expression for ζ_{23} (which I am trying to find the properties of), I can utilize Section 1.3 to prove that $\mathbb{Q}(\zeta_{23})/\mathbb{Q}$ is not radical as follows.

Observe that $\mathrm{Gal}(\mathbb{Q}(\zeta_{23})/\mathbb{Q}) \cong \mathbb{Z}_{23}^{\times}$ by Proposition 9. Since $|\mathbb{Z}_{23}^{\times}| = 22$ (since 23 is prime and every number below 23 is necessarily coprime to it), by Proposition 12, it has factors $\mathbb{Z}_2$ and $\mathbb{Z}_{11}$ and a decomposition series like

$$\{e\} \lhd \mathbb{Z}_{11} \lhd \mathbb{Z}_{23}^{\times}$$

which I may invoke FTGT upon to get

$$\mathbb{Q}(\zeta_{23}) \supset K \supset \mathbb{Q}$$

for some intermediate subfield K. Notice that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2$[7], so K cannot contain ζ_{11}, otherwise $\mathbb{Q} \subset \mathbb{Q}(\zeta_{11}) \subseteq K$, and invoking FTGT would mean that $\mathrm{Gal}(\mathbb{Q}(\zeta_{11})/\mathbb{Q}) \cong \mathbb{Z}_{11}^{\times}$ is a quotient subgroup of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2$, which is false[8]. Now suppose for contradiction that $\mathbb{Q}(\zeta_{23})$ is a radical extension of K. Since there are no intermediate subfields, it must be the case that

$$\mathbb{Q}(\zeta_{23}) = K\left(\sqrt[p]{a}\right)$$

for some $a \in K$ and p prime. I need to show that $G \coloneqq \mathrm{Gal}\left(K\left(\sqrt[p]{a}\right)/K\right)$ cannot be $\mathbb{Z}_{11}$. By Proposition 7, G is either $\mathbb{Z}_p$ or $\{e\}$ depending on if $\zeta_p \in K$, which means that I need only consider the case $p = 11$. But $\zeta_{11} \notin K$ implies $G \cong \{e\}$, hence contradiction[9], and $\mathbb{Q}(\zeta_{23})/\mathbb{Q}$ is not radical.

In line with the pattern for ζ_7 in Section 1.2, the main issue is the absence of the root of unity ζ_{11} in the base field, so instead I first extend to a field containing ζ_{11}. However, applying the same argument reveals that I must extend to a field containing ζ_5 first, before adjoining ζ_{11} and ζ_{23}. Luckily, $\mathbb{Q}(\zeta_5)$ is a radical extension of $\mathbb{Q}$, since the factors of $\mathbb{Z}_5^{\times}$ include only two copies of $\mathbb{Z}_2$, and the corresponding root of unity $\zeta_2 = -1$ is already in $\mathbb{Q}$. Consequently, to build up to a field containing ζ_{23}, I must perform cyclotomic extensions in the sequence:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\zeta_5, \zeta_{11}) \subset \mathbb{Q}(\zeta_5, \zeta_{11}, \zeta_{23})$$

where the Galois groups of the individual extensions are the groups $\mathbb{Z}_5^{\times}$, $\mathbb{Z}_{11}^{\times}$, and $\mathbb{Z}_{23}^{\times}$ respectively. Applying FTGT on the decomposition series for each of them and employing Proposition 8 gives:

[7] $\mathrm{Gal}(\mathbb{Q}(\zeta_{23})/K) \cong \mathbb{Z}_{11}/\{e\} \cong \mathbb{Z}_{11}$, so $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the other factor of $\mathbb{Z}_{23}^{\times}$, i.e. $\mathbb{Z}_2$.

[8] $\mathbb{Z}_2$ is simple, thus its only quotient subgroup is $\mathbb{Z}_2$.

[9] A similar argument for the other decomposition series of $\mathbb{Z}_{23}^{\times}$ ($\{e\} \lhd \mathbb{Z}_2 \lhd \mathbb{Z}_{23}^{\times}$) can be constructed.

$$\begin{cases} \mathbb{Z}_5^\times \rhd \mathbb{Z}_2 \rhd \{e\} \\ \mathbb{Z}_{11}^\times \rhd \mathbb{Z}_5 \rhd \{e\} \\ \mathbb{Z}_{23}^\times \rhd \mathbb{Z}_{11} \rhd \{e\} \end{cases} \xrightarrow{\text{FTGT}} \begin{cases} \mathbb{Q} \subset \mathbb{Q}\left(\sqrt{a}\right) \subset \mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right) = \mathbb{Q}(\zeta_5) \\ \mathbb{Q}(\zeta_5) \subset \mathbb{Q}\left(\zeta_5, \sqrt{c}\right) \subset \mathbb{Q}\left(\zeta_5, \sqrt{c}, \sqrt[5]{d}\right) = \mathbb{Q}(\zeta_5, \zeta_{11}) \\ \mathbb{Q}(\zeta_5, \zeta_{11}) \subset \mathbb{Q}\left(\zeta_5, \zeta_{11}, \sqrt{e}\right) \subset \mathbb{Q}\left(\zeta_5, \zeta_{11}, \sqrt{e}, \sqrt[11]{f}\right) = \mathbb{Q}(\zeta_5, \zeta_{11}, \zeta_{23}) \end{cases} \tag{6}$$

which explicitly illustrates the radicality of $\mathbb{Q}(\zeta_5, \zeta_{11}, \zeta_{23})$. As seen, obtaining this field requires adjoining 4 square roots, 1 fifth root, and 1 eleventh root, hence the same roots are present in the (most 'simplified' version of the) algebraic expression for ζ_{23}.

It should be noted that composite roots are taken as separate prime roots, e.g. a fourth root is considered two square roots, a sixth root is considered a square root and a cube root, etc. This means that it may be the case that ζ_{23} is expressible in a single $2^4 \cdot 5 \cdot 11 = 880$-th root, although unlikely. Additionally, two roots are considered distinct if the expression under it is also distinct, not merely how many times it appears in an expression. For example, the expression $\sqrt{1+\sqrt{5}} + \sqrt{4-\sqrt{5}}$ is said to contain three square roots, not four, for $\sqrt{5}$ is repeated twice.

This method, of obtaining the smallest radical extension of $\mathbb{Q}$ containing the desired ζ_n, makes use of the property of the multiplicative groups and avoids making explicit reference to the algebraic expression of the root of unity. This is advantageous as it allows for generalization to any integer n; the only obstacle is the determination of factors of any multiplicative group.

Proposition 12 and Lemma 6 conclude that all factors are cyclic of order dividing $|\mathbb{Z}_n^\times|$. This value, by definition, is the number of integers less than n coprime to n, which is given by the Euler totient function, $\phi(n)$. Thus,

$$|\mathbb{Z}_n^\times| = \phi(n)$$

and from the prime factorization of $\phi(n)$, then, I can directly read off its cyclic factors as in the statement for Proposition 12.

Using the procedure for ζ_{23} as a reference, for general n, consider each prime factor of $\phi(n)$ not equal to 2. Investigate its totient, and for each of those primes not equal to 2, investigate its totient again... Repeat this process until all 'final' factors are equal to 2. For each number, then, I can obtain a 'tree':

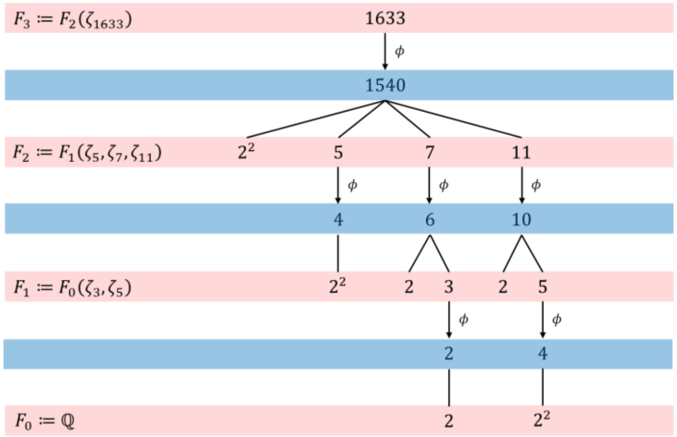

$F_3 \coloneqq F_2(\zeta_{1633})$
1633
ϕ
1540
$F_2 \coloneqq F_1(\zeta_5, \zeta_7, \zeta_{11})$
2^2
5
7
11
ϕ
ϕ
ϕ
4
6
10
$F_1 \coloneqq F_0(\zeta_3, \zeta_5)$
2^2
2
3
2
5
ϕ
ϕ
2
4
$F_0 \coloneqq \mathbb{Q}$
2
2^2

Fig. 1: Example of a 'tree', $n = 1633$

As in Fig. 1, each 'level' of prime factors is highlighted in red, and building up to a field containing the desired ζ_n requires adjoining to the base field $\mathbb{Q}$ the various prime roots of unity (ignoring factors of 2) on each level in order from lowest to highest, as illustrated by the sequence of F_i's on the left, where the final field (in this case F_3) contains the desired root of unity. The radicality of $F_3/\mathbb{Q}$ may be explicitly illustrated in a similar fashion to (6).

To know the kinds of roots present in the algebraic expressions for ζ_n, notice that at each step of the cyclotomic extension in the adjoining process, its Galois group with the series (3) has factors satisfying (4), which means invoking FTGT and Proposition 8 concludes that the whole extension is composed of Kummer extensions each obtained by adjoining d_i-th roots, and by Proposition 12, the d_i's can be directly read off the prime factorization of $\phi(n)$. Hence, looking at the prime factorization after multiplying the totient at each step of the extension, i.e. numbers in the blue strips without repeat (e.g. $\phi(5) = 4$ appears twice in Fig. 1), would give the total amount of roots required to achieve the full extension. As an illustration, for ζ_{1633}, with reference to Fig. 1,

$$2 \cdot 4 \cdot 6 \cdot 10 \cdot 1540 = 739200 = 2^7 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$$

which means that there are 7 square roots, 1 cube root, 2 fifth roots, 1 seventh root, and 1 eleventh root in the algebraic expression for ζ_{1633}.

In Appendix C, I used Python to compile a list of the types of roots present in the algebraic expressions for the nth root of unity from 1 to 100. Past ζ_2, all roots of unity require square roots, and as the degree of the root increases, they appear less frequently in the algebraic expressions (e.g. only ζ_{83} requires a 41st-root), although the frequency increases slightly with higher roots of unity (e.g. square, cube and fifth roots are significantly more concentrated and have higher frequency at the bottom). This is expected since in general, as n increases, so does its totient, and there are higher prime factors in their respective 'trees'.

To conclude this section, I have proven the existence of algebraic expressions for the roots of unity and devised a method to obtain the p-th roots necessary to build them. Intuitively, it is expected that algebraic expressions for roots of unity exist, since they are roots of the polynomial $x^n - 1$, which is quite simple; it would be surprising if solutions to this equation cannot be expressed algebraically. It is then natural to ask if all roots of polynomials are this way too.

Section 2: Roots of Polynomials

The solution to the quadratic equation $ax^2 + bx + c = 0$, the quadratic formula, is well-known:

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

Interestingly, there are also cubic and quartic formulae, respectively for the cubic $ax^3 + bx^2 + cx + d = 0$ and the quartic $ax^4 + bx^3 + cx^2 + dx + e = 0$, which utilizes only the algebraic operations in the coefficients. This guarantees the existence of algebraic expressions for roots of polynomial equations of degree less than or equal to 4. Can the same be said for all polynomial equations, in particular, quintic equations (degree-5 polynomial equations)? If not, when can the roots of a polynomial be solved by radicals?

Section 2.1: Solvability as a Necessary Condition

As argued at the start of Section 1.1, the required condition is to have the root be contained in a field that is a radical extension of the field the coefficients of the polynomial exist in (the base field). Alternatively, to accommodate all the roots of the polynomial, the whole splitting field L of the polynomial over the base field F must be contained in a radical extension of F.

Consider that I start with a radical extension E/F with $L \subseteq E$, and a series like (1) with each $F_{i+1} = F_i\left(\sqrt[d_i]{a_i}\right)$ where $a_i \in F_i$. For applying the main theorems discussed above, I need to modify this series such that it meets several conditions. First, to conclude the cyclicality of the Galois groups of the individual extensions, Proposition 7 requires the extensions to also be Kummer (otherwise the Galois group is trivial), which necessitates the existence of all ζ_{d_i}'s in the base field. This can be done by defining $N = d_0 d_1 d_2 \cdots d_{m-1}$ and extending to a field $\tilde{F}$ containing ζ_N first. By Theorem 13, this does not violate radicality.

Next, for applying FTGT, I need the full extension to be Galois. By Lemma 3, this can be done by requiring that the final field $\tilde{E}$ be a splitting field; specifically, if $f_i \in F[x]$ is the minimal polynomial of $\sqrt[d_i]{a_i}$ over F, then I aim to have $\tilde{E}$ be the splitting field of $f_0 f_1 f_2 \cdots f_{m-1}$. At each step of the extension, then, in addition to adjoining $\sqrt[d_i]{a_i}$, adjoin also the other roots of f_i, so that the resulting field is a splitting field of f_i over the previous field.

Summarizing the two modifications, the resulting tower of fields is

$$F \subseteq \tilde{F} \coloneqq \tilde{F}_0 \subseteq \tilde{F}_1 \subseteq \tilde{F}_2 \subseteq \cdots \subseteq \tilde{F}_m \coloneqq \tilde{E} \tag{7}$$

where $\tilde{F}_{i+1}$ is the splitting field of $f_i \in F[x]$ over $\tilde{F}_i$. It remains to show that this sequence remains radical.

Define $r_{i,j}$ where $1 \leq j \leq \deg f_i$ as the roots of f_i and without loss of generality write $r_{i,1} = \sqrt[d_i]{a_i}$. Any $\phi \in G \coloneqq \mathrm{Gal}(\tilde{E}/F)$ is going to send $r_{i,1}$ to any of the $r_{i,j}$'s, and I conjecture that there exists $\phi \in G$ sending $r_{i,1}$ to every other root. If this is the case, then since $r_{i,1}^{d_i} = a_i \in \tilde{F}_i$, for all j there exists ϕ such that

$$r_{i,j}^{d_i} = [\phi(r_{i,1})]^{d_i} = \phi(r_{i,1}^{d_i}) = \phi(a_i) \tag{8}$$

By construction of F_i and Lemma 2,

$$a_i = g_i(r_{1,1}, r_{2,1}, \cdots, r_{i-1,1})$$

where $g_i \in F[x_1, x_2, \cdots, x_{i-1}]$. Thus

$$\phi(a_i) = g_i\left(\phi(r_{1,1}), \phi(r_{2,1}), \cdots, \phi(r_{i-1,1})\right)$$

where by Lemma 1, each $\phi(r_{k,1}) = r_{k,l} \in \tilde{F}_{k+1} \subseteq \tilde{F}_i$ for some l and all $1 \leq k \leq i-1$. Thus, by closure, $\phi(a_i) \in \tilde{F}_i$, and due to (8), I may write

$$r_{i,j} = \zeta_{d_i}^{n_{i,j}} \sqrt[d_i]{x_{i,j}}$$

for some $0 \leq n_{i,j} \leq d_i - 1$ and some $x_{i,j} \in \tilde{F}_i$, which are not necessarily distinct. Since $\zeta_{d_i} \in \tilde{F} \subseteq \tilde{F}_i$, and $\tilde{F}_{i+1}$ is the splitting field of f_i over $\tilde{F}_i$,

$$\tilde{F}_{i+1} = \tilde{F}_i(r_{i,1}, r_{i,2}, \cdots, r_{i,\deg f_i}) = \tilde{F}_i\left(\sqrt[d_i]{x_{i,1}}, \sqrt[d_i]{x_{i,2}}, \cdots, \sqrt[d_i]{x_{i,\deg f_i}}\right)$$

Hence $\tilde{F}_{i+1}/\tilde{F}_i$ is radical, and therefore $\tilde{E}/\tilde{F}$ and $\tilde{E}/F$ are radical. By construction, then, $\tilde{E}$ is obtained as a series of Kummer extensions of $\tilde{F}$ (since $\zeta_{d_i} \in \tilde{F}$) which itself can be constructed as a series of Kummer extensions of F by Theorem 13.

For proving the conjecture,

Proposition 14. Let E/F be a Galois extension and $f \in F[x]$ irreducible over F that splits over E. Then $G \coloneqq \mathrm{Gal}(E/F)$ acts transitively on the roots of f, i.e. for any pair of roots, there exists $\phi \in G$ sending one root to the other.

Proof. Suppose for contradiction that G does not act transitively. Let r and r' be roots of f such that there does not exist $\phi \in G$ where $\phi(r) = r'$. Now, define

$$\mathcal{O} = \{\phi(r) | \phi \in G\}$$

Evidently, $r' \notin \mathcal{O}$. Consider the polynomial

$$g(x) = \prod_{s \in \mathcal{O}} (x - s) \neq f(x)$$

because it is missing at least a factor of $x - r'$. By closure, for every $s \in \mathcal{O}$ and any $\psi \in G$, $\psi(s) \in \mathcal{O}$. Since ψ is bijective, it permutes $\mathcal{O}$, which means $\psi(g(x))$ only permutes the order of the products and is hence equal to $g(x)$. Thus the coefficients of g are fixed by G. Since E/F is Galois, $g \in F[x]$, and by construction, it also divides f, meaning that f is not irreducible over F, hence contradiction. QED.

Since minimal polynomials are irreducible, Proposition 14 applies to all $f_i \in F[x]$ and the extension $\tilde{E}/F$. Since $G = \mathrm{Gal}(\tilde{E}/F)$ acts transitively on the roots of f_i, there exists $\phi \in G$ such that $\phi(r_{i,1}) = r_{i,j}$ for all j, proving the conjecture.

Thus, if I have a radical extension E/F written like (1), then I can write down another tower of fields (7) which is both Galois and obtained as a series of Kummer extensions. That means

$$F \coloneqq K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{m'} \coloneqq \tilde{E}$$

where $\tilde{E}/F$ is Galois and each K_{i+1}/K_i is Kummer. This allows for the application of FTGT, thereby obtaining a series of descending normal subgroups:

$$G \coloneqq \mathrm{Gal}(\tilde{E}/F) \coloneqq H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_{m'} \cong \{e\}$$

and by Proposition 7, $\mathrm{Gal}(K_{i+1}/K_i) \cong H_i/H_{i+1}$ is cyclic. Refine this into a full decomposition series to conclude that $\mathrm{Gal}(\tilde{E}/F)$ has cyclic factors, i.e. it is a solvable group.

I can arrive at a necessary condition for the inclusion of the splitting field L in a radical extension by noting that

$$F \subseteq L \subseteq \tilde{E}$$

and since both L/F and $\tilde{E}/F$ are Galois, after invoking FTGT, I can write

$$G \trianglerighteq H \trianglerighteq \{e\}$$

with G solvable. $H \trianglelefteq G$ is also solvable, since all the factors of G, and hence H, are cyclic. By Lemma 5, $\mathrm{Gal}(L/F) \cong G/H$, and as argued in Section 1.3, its factors include that of G that are not factors of H, so it also has cyclic factors. Hence $\mathrm{Gal}(L/F)$ is solvable too.

Thus, I have derived the solvability of a polynomial's Galois group as a necessary condition for the splitting field to be included in a radical extension of the base field. In the next section, I will prove the converse of this result, i.e. that solvability is also a sufficient condition.

Section 2.2: Solvability as a Sufficient Condition

Consider $f \in F[x]$ and L its splitting field over F such that $\mathrm{Gal}(L/F)$ is solvable. This means that from its full decomposition series,

$$\{e\} \cong H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m \coloneqq \mathrm{Gal}(L/F)$$

I can invoke FTGT (since L/F is Galois by Lemma 3) to yield

$$L \coloneqq F_0 \supset F_1 \supset F_2 \supset \cdots \supset F_m \coloneqq F$$

with each $\mathrm{Gal}(F_i/F_{i+1}) \cong H_{i+1}/H_i \cong \mathbb{Z}_{d_i}$ for some d_i by construction. In similar fashion to Section 2.1, I need to modify this tower of fields to utilize Proposition 8. I need the F_i's to also contain the various ζ_{d_i}'s, so first define $N \coloneqq d_0 d_1 d_2 \cdots d_{m-1}$. By Theorem 13, there exists $\tilde{F}$ containing ζ_N which is a radical extension of F that can be expressed as a series of Kummer extensions of F, i.e. it is obtained by adjoining a sequence of radicals to F:

$$\tilde{F} = F(\alpha_1, \alpha_2, \cdots, \alpha_k)$$

So, for each $0 \leq i \leq m$, adjoin to F_i all the α_j's, i.e. $\tilde{F_i} = F_i(\alpha_1, \alpha_2, \cdots, \alpha_k)$, and define $\tilde{F} = \tilde{F_m}$. Then I will obtain a new tower of fields

$$F \subseteq \tilde{F} \coloneqq \tilde{F_m} \subset \tilde{F}_{m-1} \subset \tilde{F}_{m-2} \cdots \subset \tilde{F_1} \subset \tilde{F_0} \coloneqq \tilde{L}$$

It remains to show that each $\tilde{F_i}/\tilde{F}_{i+1}$ remains radical. First note that since F_i/F_{i+1} is Galois by Lemma 5, by Lemma 3 it is the splitting field of some $f_i \in F_i[x]$, hence by definition,

$$F_i = F_{i+1}\left(r_{i,1}, r_{i,2}, \cdots, r_{i,\deg f_i}\right)$$

where $r_{i,j}$ are the roots of f_i. By construction, $\tilde{F_i}$ remains the splitting field of f_i over $\tilde{F}_{i+1}$, since

$$\begin{aligned} \tilde{F_i} &= F_i(\alpha_1, \alpha_2, \cdots, \alpha_k) \\ &= F_{i+1}\left(\alpha_1, \alpha_2, \cdots, \alpha_k;\ r_{i,1}, r_{i,2}, \cdots, r_{i,\deg f_i}\right) \\ &= \tilde{F}_{i+1}\left(r_{i,1}, r_{i,2}, \cdots, r_{i,\deg f_i}\right) \end{aligned}$$

Hence, $\tilde{F_i}/\tilde{F}_{i+1}$ is Galois. Now, I conjecture that each $\text{Gal}\left(\tilde{F_i}/\tilde{F}_{i+1}\right)$ remains cyclic, this time, of some order $\tilde{d_i}$ dividing N, since this would allow for the application of Proposition 8, because $\zeta_{\tilde{d_i}}$ as a power of ζ_N is in $\tilde{F} \subseteq \tilde{F}_{i+1}$, to conclude that each $\tilde{F_i}/\tilde{F}_{i+1}$ is Kummer, so that $\tilde{L}/\tilde{F}$ is radical and therefore $\tilde{L}/F$ too by Theorem 13. Hence $L \subseteq \tilde{L}$ is contained in a radical extension of F.

The conjecture is proven below:

<u>Proposition 15.</u> Let

$$\begin{cases} F \subseteq K \subseteq M \\ F \subseteq E \subseteq M \end{cases}$$

where E is the splitting field of some $f \in F[x]$ over F, and M is the splitting field of the same f over K. Then $\text{Gal}(M/K)$ is isomorphic to a subgroup of $\text{Gal}(E/F)$.

<u>Proof.</u> By Lemma 3, E/F is Galois, and the minimal polynomial f of any $x \in E$ over F completely splits in E. By Lemma 1, then, any automorphism of M sends x to a root of f which is in E, so $\phi(x) \in E$. Additionally, any $\psi \in \text{Gal}(M/K)$ fixes $F \subseteq K$, which means that ψ also induces an automorphism in $E \subseteq M$ over F. Consider the mapping $\sigma : \text{Gal}(M/K) \to \text{Gal}(E/F)$ defined by

$$\sigma(\psi) = \psi|_E$$

It satisfies the homomorphism property as for any $\chi, \chi' \in \text{Gal}(M/K)$,

$$\sigma(\chi \circ \chi') = (\chi \circ \chi')|_E = \chi|_E \circ \chi'|_E = \sigma(\chi) \circ \sigma(\chi')$$

I now need to prove that σ is injective. Let r_i where $1 \leq i \leq \deg f$ be the roots of f. Then

$$\begin{cases} E = F\left(r_1, r_2, \cdots, r_{\deg f}\right) \\ M = K\left(r_1, r_2, \cdots, r_{\deg f}\right) \end{cases}$$

By Lemma 2, any $x \in M$ is of the form $x = g\left(r_1, r_2, \cdots, r_{\deg f}\right)$, where $g \in K\left[x_1, x_2, \cdots, x_{\deg f}\right]$.

Now suppose $\psi|_E = \psi'|_E$, and write

$$\begin{cases} \psi(x) = g\left(\psi(r_1), \psi(r_2), \cdots, \psi\left(r_{\deg f}\right)\right) \\ \psi'(x) = g\left(\psi'(r_1), \psi'(r_2), \cdots, \psi'\left(r_{\deg f}\right)\right) \end{cases}$$

But since all $r_i \in E$, and $\psi|_E(r_i) = \psi'|_E(r_i)$, $\psi(r_i) = \psi'(r_i)$, which means $\psi(x) = \psi'(x)$, hence σ is injective. This means that $\mathrm{Gal}(M/K)$ is isomorphic to its image, which is a subgroup of $\mathrm{Gal}(E/F)$. QED.

Utilizing Proposition 15 by recognizing the towers of fields

$$\begin{cases} F_{i+1} \subseteq \tilde{F}_{i+1} \subseteq \tilde{F}_i \\ F_{i+1} \subseteq F_i \subseteq \tilde{F}_i \end{cases}$$

where $\tilde{F}_i$ and F_i are the splitting fields of the same polynomial f_i over $\tilde{F}_{i+1}$ and F_{i+1} respectively, I can prove that $\mathrm{Gal}\left(\tilde{F}_i/\tilde{F}_{i+1}\right)$ is isomorphic to a subgroup of $\mathrm{Gal}(F_i/F_{i+1}) \cong \mathbb{Z}_{d_i}$, which means it must be cyclic of order $\tilde{d}_i$ dividing d_i which divides N, therefore proving the conjecture.

Thus, as argued above, if the Galois group of a polynomial is solvable, then its splitting field is contained in a radical extension of the base field. Combining this with the result of Section 2.1, I arrive at:

Theorem 16. Let $f \in F[x]$ and L its splitting field over F. L is contained in a radical extension of F if and only if $\mathrm{Gal}(L/F)$ is solvable.
Corollary. A polynomial is solvable by radicals if and only if its Galois group is solvable.

Section 2.3: Galois Groups of Polynomials

Theorem 16 is a profound and widely known result, and is a very useful tool for discerning the solvability of a polynomial by radicals through its Galois group, bypassing the necessity for direct and explicit determination of its roots, which usually involves a very complicated and tedious procedure.

Let $f \in F[x]$, and L its splitting field over F. Without loss of generality, I can assume all roots of f to be distinct, so there are $n \coloneqq \deg f$ roots: $r_1, r_2, \cdots, r_n$, which makes $L = F(r_1, r_2, \cdots, r_n)$. Since any $\phi \in \mathrm{Gal}(L/F)$ is bijective, Lemma 1 implies that ϕ permutes the roots of f, which means each automorphism acts as a permutation of n elements; and by Lemma 2, each permutation completely determines the full automorphism, so $\mathrm{Gal}(L/F)$ can be seen as a group of permutations on the n roots of f, and is therefore isomorphic to a subgroup of S_n, the group of all permutations of n elements.

For polynomials of degree 4 or lower, since they have at most 4 distinct roots, their Galois groups are isomorphic to subgroups of S_n for $n \leq 4$, and their full decomposition series are:

n	**Decomposition Series**	**Factors**[10]
1	$\{e\} \cong S_1$	N/A
2	$\{e\} \lhd \mathbb{Z}_2 \cong S_2$	$\mathbb{Z}_2$
3	$\{e\} \lhd \mathbb{Z}_3 \lhd S_3$	$\mathbb{Z}_3, \mathbb{Z}_2$
4	$\{e\} \lhd \mathbb{Z}_2 \lhd V^{11} \lhd A_4{}^{12} \lhd S_4$	$\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2$

Table 1: Decomposition Series and Factors of S_n, $n \leq 4$

Since all the factors are cyclic, S_n for $n \leq 4$ are all solvable. It is a fact that subgroups of solvable groups are also solvable:

Lemma 17. Let G be solvable, and $H \subseteq G$. Then H is solvable.

Hence the Galois group of any polynomial with degree less than or equal to 4 is solvable by radicals. This explains the existence of an 'algebraic formula' for the linear, quadratic, cubic, and quartic equations, since their roots are necessarily expressible in the algebraic operations. However, this changes for the quintic and above, since the subgroups of S_n for $n \geq 5$ are not necessarily solvable. In fact, their decomposition series are:

$$\{e\} \lhd A_n \lhd S_n$$

where A_n is a simple group[13] which is not cyclic. This implies that S_n is not solvable, and any polynomial with such a Galois group by Theorem 16 is not solvable by radicals.

It remains to show that there actually exists a polynomial with a non-solvable Galois group to demonstrate that solving polynomial equations by radicals is in general impossible. A natural choice is to pick the Galois group S_n for a degree-n polynomial; however, proving that a counterexample exists for each S_n requires solving the inverse Galois problem for $S_n{}^{14}$ for all $n \geq 5$, which is in itself a complex topic worth dedicated discussion. In the following I show that there exist quintic polynomials with the non-solvable Galois group S_5.

Section 2.4: Insolvability of the Quintic

Here, I use the counterexample $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Let L be the splitting field of f over $\mathbb{Q}$; I aim to prove that the Galois group of f, i.e. $G \coloneqq \mathrm{Gal}(L/\mathbb{Q}) \cong S_5$. Firstly, and perhaps most importantly, I need to confirm that $f(x)$ has 5 distinct roots, which can be easily done with a numerical approximation:

[10] The factors are listed in order from left to right corresponding to the quotient subgroup of each pair of adjacent groups in the decomposition series.

[11] V is the Klein-four group, isomorphic to $\{e, a, b, ab\}$, where $a^2 = b^2 = (ab)^2 = e$. It is abelian.

[12] A_n is the alternating group of degree n, defined as the group of even permutations of n elements.

[13] Sheng, 2022, p. 6

[14] The inverse Galois problem for a group G asks if there exists a polynomial in $\mathbb{Q}[x]$ with Galois group G.

$$\begin{cases} r_1 \approx -1.51851 \\ r_2 \approx 0.508499 \\ r_3 \approx 1.2436 \\ r_4 \approx -0.116792 - 1.43845i \\ r_5 \approx -0.116792 + 1.43845i \end{cases} \qquad [15] \tag{9}$$

So G is indeed isomorphic to a subgroup of S_5. Now I need to prove that it is isomorphic to the whole S_5, by showing that it contains all possible permutations of its roots. Intuitively, any permutation in S_n can be expressed as a composition of transpositions, i.e. permutations that swap only two elements while leaving others fixed[16]. Now, I claim that:

Proposition 18. Let $\sigma, \tau \in G \subseteq S_p$ where p is a prime, such that σ has order p and τ is a transposition. Then $G \cong S_p$.

Proof. Without loss of generality, let the elements of G permute the set

$$\mathcal{S} = \{k | 1 \leq k \leq p\}$$

where τ is a transposition between 1 and $q + 1$ for some $q < p$, and σ is defined by $\sigma(k) = k + 1$ for all $k \in \mathcal{S}$ (here, $k \pm m$ denotes the element m spaces after and before k respectively, which cycles back to 1 if larger than p and p if smaller than 1). Now, let $k \in \mathcal{S}$, and define the permutation $\phi_k \coloneqq \sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)}$. Since

$$\begin{cases} \phi_k(k) = \left(\sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)}\right)(k) = (\sigma^{k-1} \circ \tau)(1) = \sigma^{k-1}(q+1) = k + q \\ \phi_k(k+q) = \left(\sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)}\right)(k+q) = (\sigma^{k-1} \circ \tau)(q+1) = \sigma^{k-1}(1) = k \\ \phi_k(l) = \left(\sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)}\right)(l) = (\sigma^{k-1} \circ \tau)(l - k + 1) = \sigma^{k-1}(l - k + 1) = l \end{cases}$$

where $l \neq k, k + q$, ϕ_k is a transposition swapping k and $k + q$. Next, claim that there exists a transposition $\psi_k \in G$ swapping 1 and any $k \in \mathcal{S}$. Since p is prime, q is coprime to p, so $q + 1, 2q + 1, 3q + 1$… iterates over the whole set $\mathcal{S}$, so any k may be written as $nq + 1$. Now, proceed by induction on n. The base case $n = 1$ is trivial, for $\psi_{q+1} = \tau \in G$. For the inductive step, let $k = nq + 1$ and assume ψ_k exists. Consider $\psi_{k+q} \coloneqq \psi_k \circ \phi_k \circ \psi_k$:

$$\begin{cases} \psi_k(1) = (\psi_k \circ \phi_k \circ \psi_k)(1) = (\psi_k \circ \phi_k)(k) = \psi_k(k+q) = k + q \\ \psi_{k+1}(k+q) = (\psi_k \circ \phi_k \circ \psi_k)(k+q) = (\psi_k \circ \phi_k)(k+q) = \psi_k(k) = 1 \\ \psi_{k+1}(k) = (\psi_k \circ \phi_k \circ \psi_k)(k) = (\psi_k \circ \phi_k)(1) = \psi_k(1) = k \\ \psi_{k+1}(l) = (\psi_k \circ \phi_k \circ \psi_k)(l) = (\psi_k \circ \phi_k)(l) = \psi_k(l) = l \end{cases}$$

where $l \neq 1, k, k + q$. Hence $\psi_{k+q} = \psi_{(n+1)q+1}$ is a transposition swapping 1 and $k + q = (n + 1)q + 1$, hence the claim is proven. Next, pick any $p, q \in \mathcal{S}$. The desired transposition swapping them may be expressed as $\chi = \psi_p \circ \psi_q \circ \psi_p$, because:

[15] Wolfram|Alpha. (n.d.). Solve for x, x^5 - 4x + 2 = 0 [Computational result]. https://www.wolframalpha.com/input?i=solve+for+x%2C+x%5E5-4x%2B2%3D0

[16] Grinberg, D. (2022). Lecture 28: Permutations [Lecture notes]. *Drexel University*, p. 1. https://www.cip.ifi.lmu.de/~grinberg/t/22fco/lec28.pdf

$$\begin{cases} \chi(p) = (\psi_p \circ \psi_q \circ \psi_p)(p) = (\psi_p \circ \psi_q)(1) = \psi_p(q) = q \\ \chi(q) = (\psi_p \circ \psi_q \circ \psi_p)(q) = (\psi_p \circ \psi_q)(q) = \psi_p(1) = p \\ \chi(1) = (\psi_p \circ \psi_q \circ \psi_p)(1) = (\psi_p \circ \psi_q)(p) = \psi_p(p) = 1 \\ \chi(l) = (\psi_p \circ \psi_q \circ \psi_p)(l) = (\psi_p \circ \psi_q)(l) = \psi_p(l) = l \end{cases}$$

where $l \neq 1, p, q$. Hence, a transposition between any two arbitrary elements exists in G, and by closure, G contains every permutation for they are compositions of transpositions. So $G \cong S_p$. QED.

Since 5 is a prime, Proposition 18 applies; I only need to show that there are automorphisms in G that act as a transposition and a permutation of order 5 on the roots. The former is relatively easier to prove, since (9) shows that f has 2 complex roots, which are complex conjugates of each other by the complex conjugation theorem; now, notice that since $L \subset \mathbb{C}$, the complex conjugate $\phi : L \to L$ defined by

$$\phi(z) = z^*$$

for any $z \in L$ is necessarily an automorphism in L that fixes $\mathbb{Q} \subset \mathbb{R}$, since it satisfies the homomorphism property and is bijective, therefore $\phi \in G$. Because the complex roots of f are conjugates of each other, ϕ acts as a transposition between these two roots.

It remains to show that G contains an automorphism ψ of order 5. Observe that, as argued in the proof for Proposition 10, $\langle\psi\rangle \cong \mathbb{Z}_5$ would be a subgroup of G, which by Lemma 6, means that 5 divides $|G|$. Motivated by this, I also claim that the converse is true:

Proposition 19 (Cauchy's Theorem). Let p be a prime and G be a group. If p divides $|G|$, then G contains an element of order p.

Proof. Define

$$\mathcal{S} = \{(g_1, g_2, \cdots, g_p) | g_1, g_2, \cdots, g_p \in G, g_1 g_2 \cdots g_p = e\}$$

Consider n, the number of elements in $\mathcal{S}$. The first $p - 1$ elements can be chosen freely, and the last element is constrained by the relation that $g_1 g_2 \cdots g_p = e$; therefore, $n = |G|^{p-1}$ is divisible by p. For each $(g_1, g_2, \cdots, g_p) \in \mathcal{S}$, then,

$$\begin{aligned} &g_k g_{k+1} \cdots g_p g_1 g_2 \cdots g_{k-1} = (g_k g_{k+1} \cdots g_p)[(g_1 g_2 \cdots g_p)(g_p^{-1} g_{p-1}^{-1} \cdots g_k^{-1})] \\ &= (g_k g_{k+1} \cdots g_p)(g_p^{-1} g_{p-1}^{-1} \cdots g_k^{-1}) = e \end{aligned}$$

Hence $(g_k, g_{k+1}, \cdots g_p, g_1, g_2, \cdots g_{k-1}) \in \mathcal{S}$ where $1 \leq k \leq p$, which are not necessarily distinct. If they are distinct, then there are p such elements; if they are not, then there exists some k such that

$$(g_1, g_2, \cdots, g_p) = (g_k, g_{k+1}, \cdots g_p, g_1, g_2, \cdots g_{k-1})$$

then $g_i = g_{i+(k-1)} = g_{i+2(k-1)} = g_{i+3(k-1)} = \cdots$ (indices cycle back to 1 if larger than p). But because p is prime, the index iterates over all of $1, 2, \cdots, p$, which implies that all $g \coloneqq g_i$ are equal, and that $g^p = e$. Now suppose for contradiction that G does not contain any element of order p. This means that only $g = e$ satisfies $g^p = e$, so except for $(e, e, \cdots, e)$, every element in $\mathcal{S}$ implies the existence of $p - 1$ others in $\mathcal{S}$; hence

$$n - 1 \equiv 0 \pmod p$$
$$\therefore n \equiv 1 \pmod p$$

But as argued above, p divides n, hence contradiction. QED.

According to Proposition 19, then, I need only prove that 5 divides $|G|$. To do so, first let α be a root of f, and conjecture that f is the minimal polynomial of α over $\mathbb{Q}$. By Lemma 2, then, since

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq L$$

hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, which divides $[L : \mathbb{Q}] = |G|$ by Lemma 3 due to the multiplicativity of field extensions. This would prove that G contains an element of order 5 (in addition to a transposition as argued above), hence $G \cong S_5$, and f is not solvable by radicals.

To prove the conjecture, it suffices to prove that $f(x) = x^5 - 4x + 2$ is irreducible over $\mathbb{Q}$[17]. This may be done through Eisenstein's criterion, namely:

Lemma 20 (Eisenstein's Criterion). Let

$$f(x) = \sum_{k=0}^{n} c_k x^k \in \mathbb{Z}[x]$$

Then f is irreducible over $\mathbb{Q}$ if there exists prime p such that:
(1) p divides each c_k for $0 \leq k < n$;
(2) p does not divide c_n;
(3) p^2 does not divide c_0.

Here, choose $p = 2$. It divides all non-leading coefficients -4, 2, and 0, and it does not divide the leading coefficient 1. Also, $2^2 = 4$ does not divide the constant term 2, so Eisenstein's criterion applies to conclude that f is irreducible over $\mathbb{Q}$. Therefore, as argued above, $G \cong S_5$ is not solvable, and by Theorem 16, the roots of f do not have algebraic expressions. This implies that:

Theorem 21. There exists a quintic polynomial in $\mathbb{Q}[x]$ whose splitting field over $\mathbb{Q}$ is not contained in a radical extension of $\mathbb{Q}$.
Corollary. There exists a quintic polynomial in $\mathbb{Q}[x]$ not solvable by radicals.
Corollary. There does not exist a quintic formula[18].

[17] Otherwise, f is divisible by the true minimal polynomial of α. But f is irreducible, hence contradiction.

[18] Otherwise I may use this 'quintic formula' to express the roots of f algebraically.

Conclusion

In this essay, I have demonstrated how Galois theory may be used to discern the existence and properties of algebraic expressions for different numbers. In Section 1, I showed that all roots of unity have algebraic expressions, and provided a method to determine the various roots required to build them; and in Section 2, I have shown the solvability of a polynomial's Galois group as a necessary and sufficient condition for its solvability by radicals, and provided a counterexample to show that roots of quintic polynomials in general do not have algebraic expressions, hence concluding that a quintic formula cannot exist. Nevertheless, more Galois-theoretic machinery is needed to provide more satisfactory and specific results, for example, distinguishing composite roots between separate prime roots in the method outlined in Section 1.4 (e.g. a fourth root and two square roots), or explicitly proving that there exists a solution to the inverse Galois problem for S_n for every $n \geq 5$, so that it may be confirmed that no algebraic formula exists for polynomial equations higher than a quintic.

Appendix A: Definitions and Notations

The definitions of certain terminologies and notations used in my essay are listed below:

A.1: Groups

A **group** is a set G equipped with a binary operation[19] such that for $g, g', g'' \in G$,
(1) $gg' \in G$;
(2) $g(g'g'') = (gg')g''$;
(3) $e \in G$ where $ge = eg = g$;
(4) $g^{-1} \in G$ where $gg^{-1} = e$.

The **identity (group)**, denoted $\{e\}$, is the unique group up to isomorphism of order 1[20] that only consists of the identity.

The **order of a group** G, denoted $|G|$, is the number of elements in G.

Let $g \in G$. The smallest possible non-zero n for which $g^n = e$ is referred to as the **order of the element** g.

If G is a group and $g \in G$, then $g^n = \underbrace{gg \cdots g}_{n \text{ times}}$. Similarly, if ϕ is a function, then $\phi^n = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{n \text{ times}}$.

Two groups G and H are **homomorphic** if there exists a **homomorphism**, defined as a function $\phi : G \to H$ such that for $g, g' \in G$,

$$\phi(gg') = \phi(g)\phi(g')$$

This condition is dubbed the '**homomorphism property**'.

Two groups are **isomorphic**, denoted $G \cong H$, when there exists a bijective homomorphism $\phi : G \to H$.

$\mathbb{Z}_n \cong \langle a \rangle = \{a^k | 0 \leq k \leq n-1\}$ where $a^n = e$ is the **cyclic group** of order n, and it is said to be **generated** by a. Every subgroup of $\mathbb{Z}_n$ is cyclic of order dividing n[21].

$\mathbb{Z}_n^\times \cong \{\gcd(n,k) = 1 | 0 \leq k \leq n-1\}$ with multiplication modulo n as the operation is the **multiplicative group (of integers modulo n)**.

A group G is **abelian** if for $g, g' \in G$, $gg' = g'g$.

[19] The binary operation is usually omitted in algebraic expressions in a manner similar to products.
[20] Because any group G must consist of the identity e, which already makes $|G| = 1$.
[21] See Proposition 22 for a proof.

Let G be a group and $N \subseteq G$. If for every $n \in N$ and $g \in G$,

$$gng^{-1} \in N^{22}$$

then N is a **normal subgroup** of G, denoted $N \trianglelefteq G^{23}$.

A group G is **simple** if the only normal proper subgroup of G is the identity.

A **(left) coset** of a subgroup $H \subseteq G$ is defined as a set $gH \coloneqq \{gh | h \in H\}$ for any $g \in G$.

Let $N \trianglelefteq G$. G/N is a **quotient group**, defined to be the group of all left cosets of N with operation, for $g, g' \in G$, defined as:

$$(gN)(g'N) = (gg')N^{24}$$

A **(Jordan-Hölder) decomposition series** for a group G refers to a tower of groups

$$\{e\} \coloneqq H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n \coloneqq G$$

where each H_{i+1}/H_i is simple and also called the **(composition) factors** of G. They are unique up to permutation[25].

A group is **solvable** if all its factors are abelian, or equivalently, cyclic[26].

A.2: Fields and Extensions

A **field** is a set F equipped with the binary operations addition '$+$' and multiplication '$\times$' such that for $a, b \in F$,

(1) $a + b \in F$, $ab \coloneqq a \times b \in F$;

(2) $0, 1 \in F$ where $a + 0 = a$ and $a \times 1 = a$;

(3) $-a, a^{-1} \in F$ where $a + (-a) = 0$ and $aa^{-1} = 1$.

(4) $+$ and $\times$ are commutative and associative, and $\times$ distributes over $+$.[27]

Let $F \subseteq E$ be two fields. Then E/F is a **field extension**, and E is an **extension** of F.

Let E/F be a field extension. Then E is a vector space over F^{28}. $[E : F]$, denoting the **degree** of the field extension, is the dimension of this vector space. It is multiplicative[29].

[22] Alternatively, $g^{-1}ng \in N$, obtained by replacing $g \to g^{-1} \in G$.

[23] A normal *proper* subgroup is denoted $N \triangleleft G$.

[24] For verifying that the operation is well-defined, see Proposition 23.

[25] Baumslag, B. (2006). A Simple Way of Proving the Jordan-Hölder-Schreier Theorem. *The American Mathematical Monthly*, *113*(10), 933–935. https://doi.org/10.1080/00029890.2006.11920381

[26] By Proposition 10, any non-cyclic abelian group must have a cyclic (proper) subgroup, which as argued in Section 1.3, must be normal, meaning that such a group cannot be simple.

[27] Checking through all conditions reveals that $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.

[28] May be verified by checking that E satisfies all the eight vector space axioms with scalar field F.

[29] See Proposition 24 for details.

If F is a field, then $F(a)$, read 'F **adjoin** a', is a **simple** extension of F, and is the smallest field containing both F and a.

Let $F \subseteq E$ be two fields. If

$$F \coloneqq F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = E$$

for finite n where each $F_{i+1} = F_i\left(\sqrt[m_i]{a_i}\right)$[30] and $a_i \in F_i$, then E/F is a **radical extension**.

Let $\zeta_n \coloneqq \mathrm{e}^{2\pi i/n} \in F$. Then the simple radical extension $F\left(\sqrt[n]{a}\right)/F$ is **Kummer**.[31]

Let F be a field not containing ζ_n. Then $F(\zeta_n)/F$ is **cyclotomic**.

Two fields E and F are **homomorphic** if there exists a **homomorphism**, defined as a function $\phi : E \to F$ such that for $x, y \in E$,

$$\begin{cases} \phi(x+y) = \phi(x) + \phi(y) \\ \quad \phi(xy) = \phi(x)\phi(y) \end{cases}$$

This condition is dubbed the '**homomorphism property**'.

Two fields E and F are **isomorphic**, denoted $E \cong F$, when there exists a bijective homomorphism $\phi : E \to F$.

An **automorphism** of a field F is defined as an isomorphism $\phi : F \to F$.

The **Galois group** of a field extension E/F, denoted $\mathrm{Gal}(E/F)$, is defined as the group of automorphisms ϕ of E such that $\phi(x) = x$ for $x \in F$, with composition '$\circ$' as the operation.

If $\phi \in G$ where G is a Galois group of some field extension E/F, then ϕ **fixes** an element $x \in E$ if $\phi(x) = x$, or a field F if it fixes every element of F. If every $\phi \in G$ fixes F, then G is also said to fix F.

Let $F \subseteq K \subseteq E$, and $\phi \in \mathrm{Gal}(E/F)$. Then $\phi|_K$ is the function obtained by restricting the domain of ϕ to K.

Let E/F be a field extension, and $H \subseteq \mathrm{Gal}(E/F)$. Then E^H is the largest subfield of E fixed by H.[32]

E/F is a **Galois extension** if $F = E^{\mathrm{Gal}(E/F)}$.

[30] I deliberately do *not* define $F_{i+1} = F_i(\alpha)$ where $\alpha^{m_i} \in F_i$; otherwise $F(\zeta_n)$ for any n is a 'radical extension', and the framework in my essay would have assumed automatically that ζ_n has an algebraic expression.

[31] Every Kummer extension is also Galois since $F\left(\sqrt[n]{a}\right)$ contains all the roots of $x^n - a$, hence it is its splitting field over F.

[32] In other words, if $z \in E$ is fixed by H, then $z \in E^H$. Otherwise, if $z \notin E^H$ is fixed by H, then $E^H(z) \supset E^H$ is also fixed by H, since any $w \in E^H(z)$ may be written $w = f(z)$ for some $f \in E^H[x]$, and for any $\phi \in H$, $\phi(w) = \phi\big(f(z)\big) = f\big(\phi(z)\big) = f(z) = w$, hence contradiction.

A.3. Polynomials

A **ring** is a set R equipped with the binary operations addition '$+$' and multiplication '$\times$' such that for $a, b \in R$,
(1) $a + b \in R, ab \coloneqq a \times b \in R$;
(2) $0, 1 \in R$ where $a + 0 = a$ and $a \times 1 = a$;
(3) $-a \in F$ where $a + (-a) = 0$;
(4) $+$ and $\times$ are commutative and associative, and $\times$ distributes over $+$.[33]

If R is a ring, then $R[x_1, x_2, \cdots, x_m]$ is the ring of all multivariate polynomials in $x_1, x_2, \cdots, x_m$ with coefficients in R[34].

A polynomial is **(ir)reducible** over a ring R if it can(not) be expressed as the product of two non-constant polynomials in $R[x]$.

The **minimal polynomial** f of some z over a field F is defined as the unique[35] polynomial with leading coefficient 1 of smallest degree in $F[x]$ of which x is a root. It then divides any $g \in F[x]$ with x as a root[36]. f is also irreducible[37] and has distinct roots[38].

Let F be a field, and $f \in F[x]$. L is the **splitting field** of f over F if it is the smallest extension of F that contains all roots of f[39].

A polynomial **splits** over a field F if all its roots are in F.

Let F be a field. The **Galois group** of a polynomial $f \in F[x]$ refers to $\mathrm{Gal}(L/F)$, where L is the splitting field of f over F.

A polynomial in $R[x]$ is **solvable by radicals** if there exists an algebraic expression for its roots involving the algebraic operations and numbers in R.

A **permutation** on a finite set $\mathcal{S}$ is a bijective function $\phi : \mathcal{S} \to \mathcal{S}$.

[33] Every field is also a ring. Checking through all conditions reveals that $\mathbb{Z}$ is a ring.
[34] Thus $R[x]$ refers to the ring of all *univariate* polynomials in x with coefficients in R.
[35] See Proposition 25 for a proof.
[36] By the division algorithm, $g = fq + r$, where $q, r \in R[x]$ and $\deg r < \deg f$. Substituting α, $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) = 0$, thus $r(x) = 0$ by minimality and g is divisible by f.
[37] Otherwise x is a root of a polynomial in $R[x]$ of lower degree (a factor of f) and f will not be a minimal polynomial.
[38] See Proposition 26 for a proof.
[39] By definition, then, $L = F(r_1, r_2, \cdots, r_n)$ where the r_i's are the roots of f.

Appendix B: Supplementary Proofs

Below, I provide additional proofs for the lemmas stated in the essay, and verify the assumptions made in the definitions in Appendix A.

B.1: Proofs of Lemmas

Proof (Lemma 1). By construction, $f(x) = 0$, and by the homomorphism property,

$$\phi\big(f(x)\big) = f\big(\phi(x)\big) = 0$$

Thus $\phi(x)$ is also a root of f. QED.

Proof (Lemma 2, Statement 1). Let $n = \deg f$. I claim that any α^k for $k \geq n$ may be written as a polynomial of degree less than n in α with coefficients in F. For the base case $k = n$, since $f(\alpha) = \alpha^n + \sum_{i=0}^{n-1} c_i \alpha^i = 0$ where $c_i \in F$, I can write

$$\alpha^n = -\sum_{i=0}^{n-1} c_i \alpha^i = g(\alpha)$$

for some $g \in F[x]$ with $\deg g < n$. For the inductive step, assume $\alpha^k = \sum_{i=0}^{n-1} d_i \alpha^i$ where $d_i \in F$. Thus

$$\alpha^{k+1} = \alpha(\alpha^k) = \alpha \sum_{i=0}^{n-1} d_i \alpha^i = \sum_{i=0}^{n-1} d_i \alpha^{i+1} = \sum_{i=1}^{n} d_{i-1} \alpha^i$$
$$= \sum_{i=1}^{n-1} d_{i-1} \alpha^i + d_{n-1}\alpha^n = \sum_{i=1}^{n-1} d_{i-1}\alpha^i - d_{n-1} \sum_{i=0}^{n-1} c_i \alpha^i$$
$$= -c_0 d_{n-1} + \sum_{i=1}^{n-1} (d_{i-1} - c_i d_{n-1})\alpha^i = g(\alpha)$$

for some $g \in F[x]$ since $c_i, d_i \in F$ and F is closed under addition and multiplication. Clearly $\deg g < n$, thus proven.

Now, consider the form of $F(\alpha)$. Consider

$$E = \{f(\alpha) | f \in F[x], \deg f < n\}$$

First, I prove that E is a field. It is closed under addition, since the sum of any polynomial in α with degree less than n remain so, and is hence in E. For multiplication, the product of two polynomials in α is another polynomial in α, which, by the claim above, may be rewritten as a polynomial with degree less than n, and is hence in E. Additive inverses of polynomials of degree less than n remain so, hence in E; and for multiplicative inverses, let g be the minimal polynomial of any $\beta \in E$ over F. Without loss of generality, let $r_1 \coloneqq \beta, r_2, \cdots, r_j$ be the roots of g in E, and s the product of those not in E. Thus

$$g(x) = (x - r_1)(x - r_2) \cdots \big(x - r_j\big)h(x)$$

where $h \in E[x]$. Notice that by Vieta's formulae, $r_1 r_2 \cdots r_j s \in F$ and $s \in E$, since they are the constant terms of $g \in F[x]$ and $h \in E[x]$.

$$\therefore \frac{1}{\beta} = \frac{1}{r_1} = \left(\frac{1}{r_1 r_2 \cdots r_j s}\right) r_2 r_3 \cdots r_j s \in E$$

since F and E are closed under multiplication. Therefore E is a field, and $F(\alpha) \subseteq E$. But by closure, any field containing F and α must contain any polynomial in α with coefficients in F, whose degree by the claim above may be taken to be less than n. Thus $E \subseteq F(\alpha)$, which implies $E = F(\alpha)$.

Let $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ be the basis of the vector space of $F(\alpha)$ over F. Clearly they span $F(\alpha)$. They are linearly independent, otherwise α satisfies a non-zero polynomial of degree less than n and f will not be the minimal polynomial of α over F. Hence, the dimension of this vector space is $[F(\alpha) : F] = n$. QED.

Proof (Lemma 2, Statement 2). Proceed by induction on m. For the base case $m = 1$, by the proof above, for any $z \in F(\alpha_1)$, there exists $g \in F[x]$ where $z = g(\alpha_1)$. For the inductive step, define $K = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$ and consider any element $z \in K(\alpha_{m+1})$. By the proof above, I may write

$$z \coloneqq \sum_{i=0}^{n-1} c_i \alpha_{m+1}^i = \sum_{i=0}^{n-1} h_i(\alpha_1, \alpha_2, \cdots, \alpha_m) \alpha_{m+1}^i$$

by the inductive hypothesis, where $n = [K(\alpha_{m+1}) : K]$, $c_i \in K$, and $h_i \in F[x_1, x_2, \cdots, x_m]$. Each term in the sum is a sum of monomials of the form $a\alpha_1^{k_1}\alpha_2^{k_2} \cdots \alpha_m^{k_m}\alpha_{m+1}^{k_{m+1}}$ where $a \in F$, so this is a polynomial in all α_i's with coefficients in F. Thus, there exists $g \in F[x_1, x_2, \cdots, x_m, x_{m+1}]$ such that $z = g(\alpha_1, \alpha_2, \cdots, \alpha_m, \alpha_{m+1})$. QED.

Proof (Lemma 2, Statement 3). As proven above, any $z \in F(\alpha_1, \alpha_2, \cdots, \alpha_m)$ may be written

$$z = g(\alpha_1, \alpha_2, \cdots, \alpha_m)$$

where $g \in F[x_1, x_2, \cdots, x_m]$. Due to the homomorphism property,

$$\phi(z) = \phi\big(g(\alpha_1, \alpha_2, \cdots, \alpha_m)\big) = g\big(\phi(\alpha_1), \phi(\alpha_2), \cdots, \phi(\alpha_m)\big)$$

and thus is fully determined by $\phi(\alpha_i)$'s for all $1 \leq i \leq m$. Hence ϕ is completely and uniquely determined by all $\phi(\alpha_i)$'s. QED.

Proof (Lemma 3, Statement 1). Define $G = \mathrm{Gal}(M/F)$ and consider

$$g(x) \coloneqq \prod_{\phi \in G} \big(x - \phi(z)\big)$$

Since $\psi \in G$ is bijective, by closure and Lemma 1, it permutes the roots of g, which means $\psi\big(g(x)\big)$ only permutes the order of the products and is hence equal to $g(x)$. Thus, the coefficients of g are fixed by G, and since M/F is Galois, $g \in F[x]$. Also, by Lemma 1, every $\phi(z)$ within the product must be a root of f, which means that g divides f. But f is irreducible, implying that $f = g$, and its roots, which by construction are the various $\phi(z)$'s, are in M.

<u>Proof (Lemma 3, Statement 2).</u> By Lemma 1, M is a vector space of dimensionality $m \coloneqq [M : F]$ over F. Let $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ be a basis, so that every $z \in M$ may be written as $z = \sum_{i=1}^{m} c_i\alpha_i$ where $c_i \in F$, so is in $F(\alpha_1, \alpha_2, \cdots, \alpha_m)$. Hence $M \subseteq F(\alpha_1, \alpha_2, \cdots, \alpha_m)$. But since $F \subseteq M$ and $\alpha_i \in M$ for all $1 \leq i \leq m$, $F(\alpha_1, \alpha_2, \cdots, \alpha_m) \subseteq M$, implying that $M = F(\alpha_1, \alpha_2, \cdots, \alpha_m)$.

Now I prove that there exists β such that $M = F(\beta)$ by induction on m. The base case $m = 1$ is trivial, since $M = F(\alpha_1)$ and I can pick $\beta = \alpha_1$. For the inductive step, let $F(\alpha_1, \alpha_2, \cdots, \alpha_m) = F(\gamma)$ for some γ such that $F(\alpha_1, \alpha_2, \cdots, \alpha_m, \alpha_{m+1}) = F(\gamma, \alpha_{m+1})$. I claim that I can take $\beta = \gamma + c\alpha_{m+1}$ for some $c \in F$. Clearly, $F(\beta) \subseteq F(\gamma, \alpha_{m+1})$.

Suppose $\gamma \notin F(\beta)$. Then $\alpha_{m+1} \notin F(\beta)$, otherwise $\gamma = \beta - c\alpha_{m+1} \in F(\beta)$. Now, define f and g as the minimal polynomials of γ and α_{m+1} respectively over F, and let L be the splitting field of fg over F. For any $\phi \in \mathrm{Gal}(L/F(\beta)) \subseteq \mathrm{Gal}(L/F)$, then,

$$\gamma + c\alpha_{m+1} = \beta = \phi(\beta) = \phi(\gamma) + c\phi(\alpha_{m+1})$$
$$\therefore c = \frac{\gamma - \phi(\gamma)}{\phi(\alpha_{m+1}) - \alpha_{m+1}}$$

Hence, one can pick c that does not satisfy this equation to conclude that $\gamma \in F(\beta)$. This may be done so by ensuring that c is not equal to the expression for any $\phi \in \mathrm{Gal}(L/F) \supseteq \mathrm{Gal}(L/F(\beta))$. Hence, $\alpha_{m+1} = (\beta - \gamma)/c \in F(\beta)$ by closure, and $F(\gamma, \alpha_{m+1}) \subseteq F(\beta)$, which implies $F(\beta) = F(\gamma, \alpha_{m+1})$, hence proven.

I now let $M = F(\beta)$ and proceed with the proof. By Lemma 2, $n \coloneqq [M : F] = \deg f$ where f is the minimal polynomial of β over F, and without loss of generality let $r_1 \coloneqq \beta, r_2, \cdots, r_n$ be the roots of f (since f has distinct roots). By Lemma 1, any $\phi \in G \coloneqq \mathrm{Gal}(M/F)$ must send β to some r_i. By Lemma 2, the whole automorphism is uniquely determined by $\phi(\beta) = r_i$, so there are at most n automorphisms. But since f is irreducible, by Proposition 14[40], there exists $\phi \in G$ sending β to every r_i. Hence there are exactly n automorphisms, and $|\mathrm{Gal}(M/F)| = n = [M : F]$. QED.

<u>Proof (Lemma 3, Statement 3).</u> I first prove that if M/F is Galois, then it is the splitting field of some $f \in F[x]$ over F. As argued in the proof above, there exists $\alpha \in M$ such that $M = F(\alpha)$. Let f be the minimal polynomial of α over F, and L its splitting field over F. Since L contains α, $M \subseteq L$. But since f is irreducible, as proven, f must completely split over M, so

[40] This is not circular.

all the roots of f are in M. Hence $L \subseteq M$. This means that $M = L$, and is the splitting field of $f \in F[x]$ over F.

For the converse direction, pick any $z \in M$ that is not in F, and let g be the minimal polynomial of z over F and L the splitting field of g over M. Therefore L is the splitting field of $h \coloneqq fg$ over F, and without loss of generality let the roots of h be $z \coloneqq s_1, s_2, \cdots, s_m$. I construct an automorphism in $\mathrm{Gal}(L/F)$ as follows.

I claim that there exists an isomorphism $\sigma : F(s_1, s_2, \cdots, s_n) \to F\big(s_{\pi(1)}, s_{\pi(2)}, \cdots, s_{\pi(n)}\big)$ fixing F such that $\sigma(s_i) = s_{\pi(i)}$, where π is some permutation on the set $\{1, 2, \cdots, m\}$ that does not fix 1, and $1 \le n \le m$. Proceed by induction on n. For the base case, since $\deg g > 1$ (otherwise $g(x) = x - z \in F[x]$ implies $z \in F$), g has multiple roots, so let $s_i \neq s_1 = z$ be another root of g. Naturally g is the minimal polynomial of both s_1 and s_i over F. Let $\sigma : F(s_1) \to F(s_i)$ be a homomorphism fixing F such that $\sigma(s_1) = s_i$. Referring to the proof of Lemma 2, I can view $F(s_1)$ and $F(s_i)$ as vector spaces over F with the bases $\left\{1, s_1, s_1^2, \cdots, s_1^{\deg g - 1}\right\}$ and $\left\{1, s_i, s_i^2, \cdots, s_i^{\deg g - 1}\right\}$ respectively, every point in $F(s_1)$ is mapped to a distinct point in $F(s_i)$ with the same coordinates, so σ is an isomorphism.

For the inductive step, define $K = F(s_1, s_2, \cdots, s_n)$ and $K' = F\big(s_{\pi(1)}, s_{\pi(2)}, \cdots, s_{\pi(n)}\big)$. Let p be the minimal polynomial of s_{n+1} over K with degree d. By the inductive hypothesis there exists an isomorphism $\sigma : K \to K'$ fixing F such that $\sigma(s_i) = s_{\pi(i)}$ for $1 \le i \le n$. Let p be the minimal polynomial of s_{n+1} over K. Since s_{n+1} is a root of $h \in F[x] \subseteq K[x]$, it follows that p divides h (since it is a minimal polynomial), so the roots of p are the roots of h. Thus, I can write

$$\sum_{i=0}^{m} a_i x^i \coloneqq h(x) = p(x)q(x) \coloneqq \left(\sum_{i=0}^{d} b_i x^i\right)\left(\sum_{i=0}^{e} c_i x^i\right) \in F[x]$$

$$\therefore a_i = \sum_{j=0}^{i} b_j c_{i-j} \in F$$

Now, define $\tilde{p}(x) = \sum_{i=0}^{d} \sigma(b_i) x^i$ and $\tilde{q}(x) = \sum_{i=0}^{e} \sigma(c_i) x^i$, both of which are in $K'[x]$. Notice that

$$\tilde{p}(x)\tilde{q}(x) = \sum_{i=0}^{d} \sigma(b_i) x^i \sum_{i=0}^{e} \sigma(c_i) x^i = \sum_{i=0}^{m} \sum_{j=0}^{i} \sigma\big(b_j\big)\sigma\big(c_{i-j}\big)\, x^i = \sum_{i=0}^{m} \sigma\left(\sum_{j=0}^{i} b_j c_{i-j}\right) x^i$$

$$= \sum_{i=0}^{m} \sigma(a_i) x^i = \sum_{i=0}^{m} a_i x^i = h(x)$$

since $a_i \in F$ is fixed by σ. Hence $\tilde{p}$ divides h and its roots are those of h.

Now, choose s_k as a root of $\tilde{p}$ with $k \neq \pi(i)$ for any $1 \leq i \leq n$. This is possible, since

$$\tilde{p}\left(s_{\pi(i)}\right) = \sum_{j=0}^{d} \sigma\left(b_j\right) s_{\pi(i)}^{j} = \sigma\left(\sum_{j=0}^{d} b_j s_i^j\right) = \sigma\left(p(s_i)\right) = 0 \Rightarrow p(s_i) = 0$$

and if every root of $\tilde{p}$ is $s_{\pi(i)}$ for some $1 \leq i \leq n$, then every root of p is s_i (since both polynomials have the same number of roots for their degrees are the same), and s_{n+1} would not be a root, a contradiction. Henceforth, define $\pi(n+1) = k$, so π remains a permutation; and define $\sigma' : K(s_{n+1}) \to K'(s_k)$ as a homomorphism such that $\sigma'(x) = \sigma(x)$ for $x \in K$, and $\sigma(s_{n+1}) = s_k$. Viewing $K(s_{n+1})$ and $K'(s_k)$ as vector spaces over K with bases $\{1, s_{n+1}, s_{n+1}^2, \cdots, s_{n+1}^{d-1}\}$ and $\{1, s_k, s_k^2, \cdots, s_k^{d-1}\}$ respectively, every point in $K(s_{n+1})$ is mapped to a distinct point in $K'(s_k)$, for its coordinates are transformed under the isomorphism σ. So σ' is bijective and therefore an isomorphism, hence proven.

Now, apply the claim to $n = m$. Since $L = F(s_1, s_2, \cdots, s_m) = F\left(s_{\pi(1)}, s_{\pi(2)}, \cdots, s_{\pi(m)}\right)$ for any permutation π, I can conclude that there exists an automorphism of L fixing F that does not fix $z = s_1$, i.e. there exists $\phi \in \operatorname{Gal}(L/F)$ such that $\phi(z) \neq z$. Now let $r_1, r_2, \cdots, r_l$ be the roots of f, so that $M = F(r_1, r_2, \cdots, r_l)$. By Lemma 2, $z = t(r_1, r_2, \cdots, r_l)$ where $t \in F[x_1, x_2, \cdots, x_l]$, and

$$\phi(z) = \phi\left(t(r_1, r_2, \cdots, r_l)\right) = t\left(\phi(r_1), \phi(r_2), \cdots, \phi(r_l)\right)$$

By Lemma 1, every $\phi(r_i)$ is another root of f which is in M (since M is a splitting field), so by closure, $\phi(z) \in M$. Now, observe that $\phi|_M$ is an automorphism of M that fixes F, hence $\phi|_M \in \operatorname{Gal}(M/F)$ and since $\phi|_M$ does not fix $z \notin F$, $M^{\operatorname{Gal}(M/F)} = F$, therefore M/F is Galois. QED.

<u>Proof (Lemma 4).</u> I prove that the mapping $H \to M^H$ is bijective. For injectivity, if $H \neq H'$ are two distinct subgroups, suppose for contradiction that $M^H = M^{H'}$. Since every element of H fixes $M^{H'}$, $H \subseteq H'$. Apply the same argument and conclude that $H' \subseteq H$, which means $H = H'$, a contradiction. For surjectivity, since M/F is Galois, by Lemma 3, M must be the splitting field of some $f \in F[x] \subseteq K[x]$ over $F \subseteq K$ for some intermediate subfield K, so it is also the splitting field of f over K, meaning that M/K is Galois. Hence $K = M^{\operatorname{Gal}(M/K)}$ and is mapped from $\operatorname{Gal}(M/K) \subseteq \operatorname{Gal}(M/F)$. Therefore, the mapping is bijective and the correspondence holds. QED.

<u>Proof (Lemma 5, Statement 1).</u> I first prove that if K/F is Galois, then $N \trianglelefteq G$. Because K/F is Galois, every $z \in K$ is a root of its minimal polynomial $f \in F[x]$ which by Lemma 3 splits over K for it is irreducible. By Lemma 1, then, any $\phi \in G$ must send z to another root of f, which is in K, meaning that $\phi(z) \in K$. Thus, for any $\psi \in N$ and $\phi \in G$,

$$(\phi^{-1} \circ \psi \circ \phi)(z) = (\phi^{-1} \circ \phi)(z) = z$$

where the first equality results since ψ fixes $\phi(z) \in K$. Hence $\phi^{-1} \circ \psi \circ \phi$ fixes K and is in N, therefore $N \trianglelefteq G$.

For the converse direction, let $z \in K$. If $z \notin F$, pick $\phi \in G$ such that $\phi(z) \neq z$. This is possible since otherwise, $M^G \supseteq F(z) \supset F$ and M/F is not Galois. Since $N \trianglelefteq G$, for any $\psi \in N$,

$$(\phi^{-1} \circ \psi \circ \phi)(z) = z \rightarrow (\psi \circ \phi)(z) = \phi(z)$$

As argued before, if M/F is Galois, so is M/K, implying that $\phi(z) \in K$. Thus, $\phi|_K : K \rightarrow K$ is an automorphism of K that fixes F, hence $\phi|_K \in \mathrm{Gal}(K/F)$. But ϕ and hence $\phi|_K$ does not fix $z \notin F$, so $K^{\mathrm{Gal}(K/F)} = F$, and K/F is Galois. QED.

<u>Proof (Lemma 5, Statement 2).</u> Consider the mapping $\sigma : \mathrm{Gal}(K/F) \rightarrow G/N$ defined by

$$\sigma(\chi) = \phi N$$

for $\chi \in \mathrm{Gal}(K/F)$, where $\phi \in G$. Pick

$$\phi(z) = \begin{cases} \chi(z) & z \in K, \\ z & \text{otherwise} \end{cases}$$

so that $\chi = \phi|_K$. First check that it satisfies the homomorphism property; if $\chi, \chi' \in \mathrm{Gal}(K/F)$,

$$\sigma(\chi\chi') = (\chi\chi')N = (\chi N)(\chi' N) = \sigma(\chi)\sigma(\chi')$$

Next I prove that the mapping is bijective. For injectivity, if $\chi \neq \chi'$ is mapped to $\phi N = \phi' N$, then $\phi' = \phi \circ \psi$ for some $\psi \in N$, so $\psi = \phi^{-1} \circ \phi'$. If $z \notin K$,

$$\psi(z) = (\phi^{-1} \circ \phi')(z) = \phi^{-1}(z) = z$$

But ψ already fixes K, so $\psi(z) = z$ for every $z \in M$. This means that $\phi' = \phi \circ \psi = \phi$, which necessarily means $\chi = \phi|_K = \phi'|_K = \chi'$, a contradiction.

For surjectivity, for every $\phi \in G$, there exists $\phi' \in G$ such that

$$\phi'(z) = \begin{cases} \phi(z) & z \in K, \\ z & \text{otherwise} \end{cases}$$

since it is also an automorphism of M that fixes F. By closure, there exists $\psi \in G$ such that $\phi = \phi' \circ \psi$. If $z \in K$,

$$\psi(z) = \left(\phi'^{-1} \circ \phi\right)(z) = z$$

which means $\psi \in N$ for it fixes K. Hence, any coset $\phi N = (\phi' \circ \psi)N = \phi' N$, and is therefore mapped from $\chi = \phi'|_K \in \mathrm{Gal}(K/F)$, since it is an automorphism of K that fixes F. Thus, the map is bijective, and therefore the isomorphism holds. QED.

<u>Proof (Lemma 6, Statement 1).</u> Every $g \in G$ is in the coset gH, for $e \in H$ implies $g = ge \in gH$. Also, suppose for contradiction that there exist two distinct cosets $gH \neq g'H$ that are not disjoint. Then there exists $h, h' \in H$ such that

$$gh = g'h'$$
$$g^{-1}g' = hh'^{-1} := h'' \in H$$

by closure. Therefore, $g' = gh''$, which means $g'H = (gh'')H = gH$, hence contradiction. Thus, every element of G belongs to one and only one coset of H, and G can be partitioned into the cosets of H. The size of all cosets of H is $|H|$, meaning that $|G|$ is divisible by $|H|$. QED.

Proof (Lemma 6, Statement 2). By the proof above, G can be partitioned into the cosets of N, which all have sizes $|N|$. Therefore, there are exactly $|G|/|N|$ cosets. By definition, since $|G/N|$ is the group of all cosets of N, $|G/N| = |G|/|N|$. QED.

Proof (Lemma 17). Since G is solvable, write a full decomposition series

$$\{e\} \coloneqq G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_m \coloneqq G$$

Define $H_i \coloneqq H \cap G_i$. Notice that $H_i \lhd H_{i+1}$ since for any $h \in H_i \subseteq G_i$ and $g \in H_{i+1} \subseteq G_{i+1}$, because $G_i \lhd G_{i+1}$, $ghg^{-1} \in G_i$; and since $g, h \in H$, by closure, $ghg^{-1} \in H$, therefore $ghg^{-1} \in H \cap G_i$. Hence I can write

$$\{e\} \coloneqq H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m \coloneqq H$$

which may not be a full decomposition series. I need to prove that each H_{i+1}/H_i is abelian, so that after refining this series, each composition factor, as factors of H_{i+1}/H_i, are too abelian. To do so, let $x, y \in H_{i+1} \subseteq G_{i+1}$. Then

$$\begin{aligned}(xH_i)(yH_i) &= (xy)H_i = (xy)(H \cap G_i) = (xy)H \cap (xy)G_i = (xy)H \cap \big((xG_i)(yG_i)\big) \\ &= (yx)H \cap \big((yG_i)(xG_i)\big) = (yx)H \cap (yx)G_i = (yx)(H \cap G_i) = (yx)H_i = (yH_i)(xH_i)\end{aligned}$$

where the first equality in the second line results since G_{i+1}/G_i is abelian, and because $x, y \in H$, $(xy)H = (yx)H = H$. Therefore H_{i+1}/H_i is abelian, and H is a solvable group. QED.

Proof (Lemma 20). Suppose for contradiction that a polynomial

$$f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$$

satisfies Eisenstein's criterion yet is reducible in $\mathbb{Q}$. Without loss of generality suppose that f is primitive, i.e. the greatest common divisor of all a_k's is 1 (otherwise, divide f by that greatest common divisor to obtain primitive f', and if f' is reducible in $\mathbb{Q}$ then so is f). That means there exists non-constant polynomials

$$p(x) = \sum_{k=0}^{r} b_k x^k, \qquad q(x) = \sum_{k=0}^{s} c_k x^k$$

both of which are in $\mathbb{Q}[x]$, where $r = \deg p$, $s = \deg q$, and $n = r + s$, such that $f(x) = p(x)q(x)$. First, I show that p and q can be taken to be in $\mathbb{Z}[x]$ without loss of generality.

Let n_p and n_q be the least common multiples of the denominators of all b_k's and c_k's respectively, such that

$$\tilde{p}(x) \coloneqq n_p p(x) = \sum_{k=0}^{r} \tilde{b}_k x^k, \qquad \tilde{q}(x) = n_q q(x) = \sum_{k=0}^{s} \tilde{c}_k x^k$$

are both in $\mathbb{Z}[x]$ and primitive. This means that

$$\tilde{f}(x) \coloneqq n_p n_q f(x) = [n_p p(x)][n_q q(x)] = \tilde{p}(x)\tilde{q}(x)$$

Next, I show that $\tilde{f}$ is primitive too. Suppose for contradiction that there exists a prime p' dividing all coefficients in g, and let $\tilde{b}_i$ and $\tilde{c}_j$ be coefficients in $\tilde{p}$ and $\tilde{q}$ respectively so that p' divides $\tilde{b}_k$ for all $0 \leq k < i$ and $\tilde{c}_k$ for all $0 \leq k < j$, but not $\tilde{b}_i$ or $\tilde{c}_j$. Then the coefficient of x^{i+j} in $\tilde{f}$ is

$$\tilde{a}_{i+j} \coloneqq \sum_{k=0}^{i+j} \tilde{b}_k \tilde{c}_{i+j-k} = \tilde{b}_i \tilde{c}_j + \sum_{k=0}^{i-1} \tilde{b}_k \tilde{c}_{i+j-k} + \sum_{k=0}^{j-1} \tilde{b}_{i+j-k} \tilde{c}_k$$

which must be divisible by p' by the assumption. But both sums are divisible by p' since all $\tilde{b}_k$'s and $\tilde{c}_k$'s within the sums are, and $\tilde{b}_i \tilde{c}_j$ by construction is not, which means that p' does not divide $\tilde{a}_{i+j}$, hence contradiction. This means that $\tilde{f}$ is primitive too, but so is f, so $n_p n_q = \pm 1$, and $f(x) = \pm \tilde{p}(x)\tilde{q}(x)$ is therefore reducible over $\mathbb{Z}$.

I now proceed with the proof. Since p but not p^2 divides $a_0 = b_0 c_0$, without loss of generality, I may proceed by assuming that p divides b_0 but not c_0. Now, I claim that p divides b_k for all $0 \leq k \leq r < n$ and proceed by strong induction. The base case $k = 0$ is true for b_0 is assumed to be divisible by p. For the inductive step, since

$$a_k = \sum_{i=0}^{k} b_i c_{k-i} = b_k c_0 + \sum_{i=0}^{k-1} b_i c_{k-i}$$

$$\therefore b_k c_0 = a_k - \sum_{i=0}^{k-1} b_i c_{k-i}$$

which is divisible by p since p divides a_k as well as all b_i for $0 \leq i < k$ by the inductive hypothesis. Since p does not divide c_0, it must divide b_k, proving the claim. However, p does not divide $a_n = b_r c_s$, so it cannot divide b_r, hence contradiction. QED.

B.2. Proofs of Assumptions in Appendix A

Proposition 22. If $G = \langle a \rangle \cong \mathbb{Z}_n$, then every $H \subseteq G$ is cyclic of order m that divides n.

Proof. Let q be the smallest non-zero integer such that $a^q \in H$. If $a^k \in H$, then

$$a^k = a^{mq+r} = a^{mq} a^r$$

where $m, r \in \mathbb{Z}$ and $0 \leq r < q$ by the division algorithm. Since $a^q \in H$, so is any a^{-mq}, the inverse of $a^{mq} = (a^q)^m$. Then

$$a^{-mq} a^k = a^r \in H$$

by closure. But since $r < q$, $r = 0$, and $a^k = a^{mq} = (a^q)^m$. Since it is also a group, there must exist an integer p such that $(a^q)^p = a^{pq} = e = a^n$, which also implies $n = pq$. Thus, $H = \langle a^q \rangle$ is cyclic of order m that divides n. QED.

Proposition 23. If $N \trianglelefteq G$, then the operation on G/N is well-defined.

Proof. Suppose two cosets in G/N may be represented differently by $gN = g'N$. Thus, there exists $n \in N$ such that $g' = gn$. Now consider another coset $hN \in G/N$, and for the operation to be well-defined, I need $(gN)(hN) = (g'N)(hN)$. Since $N \trianglelefteq G$, $h^{-1}nh \coloneqq n' \in N$, which means $nh = hn'$. Thus,

$$(g'N)(hN) = (g'h)N = (gnh)N = (ghn')N = (gh)N = (gN)(hN)$$

QED.

Proposition 24. Let $F \subseteq K \subseteq E$. Then $[E : F] = [E : K][K : F]$.

Proof. Viewing E as a vector space over K and K a vector space over F, let $m \coloneqq [E : K]$ and $n \coloneqq [K : F]$, and $\{\alpha_1, \alpha_2, \cdots, \alpha_m\}$ and $\{\beta_1, \beta_2, \cdots, \beta_n\}$ be bases of E over K and K over F respectively. Hence, for any $x \in E$,

$$x = \sum_{i=1}^{m} a_i \alpha_i = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{i,j} \alpha_i \beta_j$$

where $a_i = \sum_{j=1}^{n} b_{i,j} \beta_j \in K$ and $b_{i,j} \in F$. Thus x is expressed as a linear combination of $\alpha_i \beta_j$ where $1 \le i \le m$ and $1 \le j \le n$, so the $\alpha_i \beta_j$'s span E. For linear independence, suppose that

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{i,j} \alpha_i \beta_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} b_{i,j} \beta_j \right) \alpha_i$$

But since the α_i's are linearly independent, $\sum_{j=1}^{n} b_{i,j} \beta_j = 0$ for every i; but the β_j's are linearly independent too, so $b_{i,j} = 0$ for all i, j. This means that the $\alpha_i \beta_j$'s (mn of them) are linearly independent, and form a basis of E over F, thus $[E : F] = mn = [E : K][K : F]$. QED.

Proposition 25. The minimal polynomial of any z over a field F is unique.

Proof. Let f and g be minimal polynomials of z over F. They have the same degree, otherwise they are not equal trivially. Define $h = f - g$, and notice that z is a root of h for $h(z) = f(z) - g(z) = 0$. But the leading coefficients of both f and g are 1, so the leading terms cancel out, leading to $\deg h < \deg f$ and therefore $h(x) = 0$ by minimality. This means that $f(x) = g(x)$, and the minimal polynomial is unique. QED.

Proposition 26. Let f be the minimal polynomial of z over a field F. Then f has distinct roots.

<u>Proof.</u> Suppose for contradiction that f has repeated roots. Let $r_1, r_2, \cdots, r_m$ be the roots of f listed without repeat, and n_i the multiplicity of the root r_i. Then

$$f(x) = (x - r_1)^{n_1}(x - r_2)^{n_2} \cdots (x - r_m)^{n_m}$$

Now suppose without loss of generality that $r \coloneqq r_1$ is a repeated root of f with multiplicity $n \coloneqq n_1 \geq 2$. Thus $f(x) = (x - r)^n g(x)$, where $g(x) = (x - r_2)^{n_2}(x - r_3)^{n_3} \cdots (x - r_m)^{n_m} \in L[x]$ with $\deg g < \deg f$. Thus

$$f'(x) = n(x - r)^{n-1}g(x) + (x - r)^n g'(x)$$
$$\therefore f'(r) = 0$$

for $n - 1 > 0$. Hence r is also a root of $f' \in F[x]$ by closure. But $\deg f' < \deg f$ since f is non-constant, so f is not the minimal polynomial of r over F. However, f is irreducible over F, so it is necessarily the minimal polynomial of r over F, hence contradiction. QED.

Appendix C: The Algebraic Expressions of ζ_n

C.1: List of p-th Roots

Below is a table compiling the list of the amounts of p-th roots present in the algebraic expressions for ζ_n, n ranging from 1 to 100, generated using the method of Section 1.4.

n	p-th roots								
	2	**3**	**5**	**7**	**11**	**13**	**23**	**29**	**41**
1									
2									
3	1								
4	1								
5	2								
6	1								
7	2	1							
8	2								
9	2	1							
10	2								
11	3		1						
12	2								
13	3	1							
14	2	1							
15	3								
16	3								
17	4								
18	2	1							
19	2	2							
20	3								
21	3	1							
22	3		1						
23	4		1		1				
24	3								
25	4		1						
26	3	1							
27	2	2							
28	3	1							
29	4	1		1					
30	3								
31	4	1	1						
32	4								
33	4		1						
34	4								
35	4	1							

36	3	1							
37	3	2							
38	2	2							
39	4	1							
40	4								
41	5		1						
42	3	1							
43	3	2		1					
44	4		1						
45	4	1							
46	4		1		1				
47	5		1		1		1		
48	4								
49	3	2		1					
50	4		1						
51	5								
52	4	1							
53	5	1							
54	2	2							
55	5		1						
56	4	1							
57	3	2							
58	4	1		1					
59	5	1		1				1	
60	4								
61	5	1	1						
62	4	1	1						
63	3	2							
64	5								
65	5	1							
66	4		1						
67	5	1	1		1				
68	5								
69	5		1		1				
70	4	1							
71	5	1	1	1					
72	4	1							
73	4	2							
74	3	2							
75	5		1						
76	3	2							
77	5	1	1						
78	4	1							
79	4	2				1			

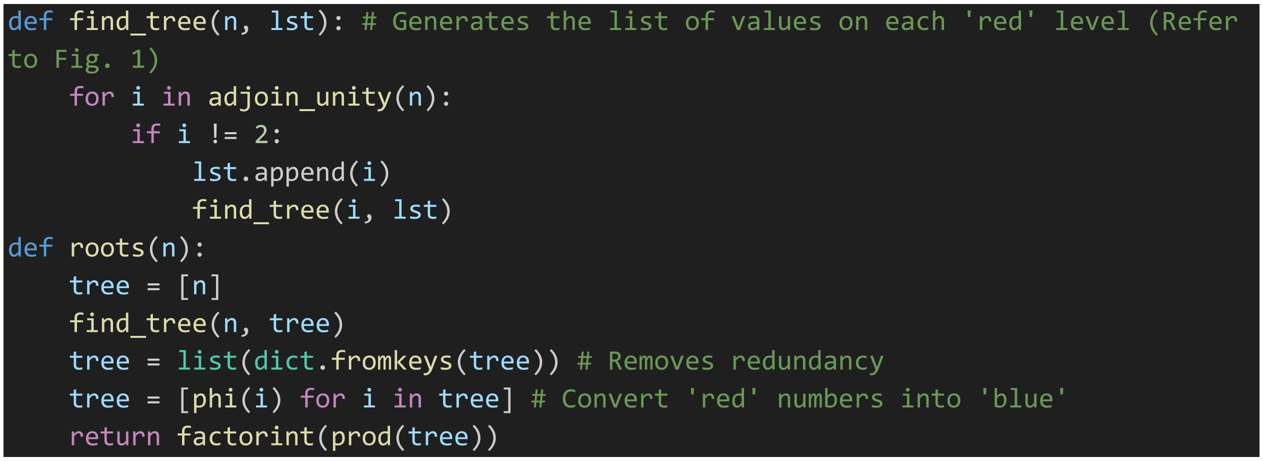
80	5								
81	2	3							
82	5		1						
83	6		1						1
84	4	1							
85	6								
86	3	2		1					
87	5	1		1					
88	5		1						
89	6		1		1				
90	4	1							
91	4	2							
92	5		1		1				
93	5	1	1						
94	5		1		1		1		
95	4	2							
96	5								
97	6	1							
98	3	2		1					
99	5	1	1						
100	5		1						

Table 2: List of Roots Present in the Algebraic Expressions for ζ_n

C.2: Python Algorithm

Below is a block of code written in Python that I used to determine the various entries in Table 2 (of course, this also applies to $n > 100$); the last function `roots(n)` returns the roots present in the algebraic expression for ζ_n.

```
from sympy.ntheory import primefactors
from sympy import factorint
from math import gcd, prod
def phi(n): # Euler totient function
    num = 0
    for i in range(1, n+1):
        if gcd(n, i) == 1:
            num += 1
    return num
def adjoin_unity(n): # Finds the roots of unity required in the base field before
adjunction of zeta_n
    req = []
    for i in primefactors(phi(n)):
        if i != 2:
            req.append(i)
    return req
```



```python
def find_tree(n, lst): # Generates the list of values on each 'red' level (Refer
to Fig. 1)
    for i in adjoin_unity(n):
        if i != 2:
            lst.append(i)
            find_tree(i, lst)
def roots(n):
    tree = [n]
    find_tree(n, tree)
    tree = list(dict.fromkeys(tree)) # Removes redundancy
    tree = [phi(i) for i in tree] # Convert 'red' numbers into 'blue'
    return factorint(prod(tree))
```