Impossibilities Proved by Galois Theory

Oklahoma State University

Chapman Howard

13 May, 2019

Introduction

I'll give a brief personal introduction, then move to introducing the material.

I began studying Galois theory, probably as many do, because of my interest in two thing: one, his untimely and yet very dramatic death, and two, the initial nebulousness of something called insolvability. It never struck me before my first course in abstract algebra that it might be possible to prove something was genuinely impossible to do. It was this spark that probably changed the course of my academic career. You see originally I had planned on graduating with my BS in Mechanical Engineering (which I will still do, just with a Mathematics degree as well) and entering the wild world of industry to see if someone would pay for me to continue my education. I never dreamed of getting a Ph.D and believed that psuedo private-sector research institutions, like the numerous national laboratories, would be my home. This project has changed that for me. Studying such fundamental concepts in abstract Mathematics has sparked in interest in me I can't hide. I try to discuss the results with my friends and predictably it is over their hide and I fall flat trying to explain it. But that doesn't stop me! It simply feels so exciting that I must move forward. I've truly found a passion in this subject and I am so thankful for those who have helped me along the way. My thesis advisor, Dr. Anand Patel has pushed me very hard, and continues to, to gain a working understanding of the material as well as succeed in my pursuit of a graduate education. Thank you Dr. Patel. Truly. Now for the material.

Studying this material I used two sources. *Galois Theory* by **Ian Stewart** was a huge boone for me. This is where I gleaned almost all my proofs and information about what field extensions were, what a Galois group was, and on and on. Also the interesting application the final chapter discussing the Rational Distance Problem, was educated by **Roy Barbara's** paper *Points at Rational Distance from the Vertices of a Unit Polygon.* So I say thank you to these two authors and mathematicians as well. I have learned much from their work and certainly wouldn't be in the position I am now without their work.

To introduce the material I have covered, it is necessary to begin with the necessity of types of numbers, as many subjects are motivated by the advancement of our definition of a number. The path from only considering a number as an element of $\mathbb{N}$ then $\mathbb{Z}$ then $\mathbb{Q}$ then $\mathbb{R}$ and finally $\mathbb{C}$ follows mathematicians pursuit of solutions to problems, usually problems like polynomials, but sometimes other problems. This pursuit of solutions to polynomials motivated mathematicians for thousands of years. The solution to the general quadratic polynomial was found maybe as long ago as 1600 BC. It took mathematicians another two thousand years to find the solution to the general cubic, wherein they found that any quartic could be reduced to a cubic form and solved in that manner. The quintic, though it did not take another two thousand years, required much more abstract ideas, and the solution was

not a general equation. It was a stop sign. This, and anything bigger than this, is impossible to solve with radicals. These aren't the only problems that motivated mathematicians, however, some Ancient Greek math games were also used to define numbers like π. I'll cover these problems too. I'll go through these proofs starting with basic ideas, as I was learning from the ground up. We'll see first the impossibilities of Ruler and Compass Construction, then the insolvability of the general quintic, and finally an open problem whose arguments are highly related to this material.

Contents

Chapter 1

Geometric Impossibilities

1.1 Introduction

We first turn to understanding the impossibilities of the geometric problems from antiquity. What is needed to solve these problems, though it was motivated by Galois' study of the quintic polynomial, does not need the full machinery of Galois theory. We will turn to the next chapter on the insolvability of the general quintic equation for that level of abstraction. For the three geometric impossibilities, all that is required is a knowledge of basic Field theory: what an extension of a field is, how to measure how far away two fields are from each other, and how we can use this knowledge and apply it to the game of Ruler and Compass Construction.

1.2 Basic Field Theory

To begin, we define a field extension. Before turning to a formal definition we give the following conceptual understanding. To extend a field means to adjoin to it an element it does not yet contain, and then let the Field axioms generate all possible elements that this new field has access to. Here is our definition:

Definition 1:
Let K be a field. Then we say that L/K, read "L over K" is a field extension if $K \subset L$ and $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$. We say that L is a finite extension of K is n is finite, and an infinite extension if n is infinite.

For example, $\mathbb{Q}(\sqrt{2})/\mathbb{Q} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. So we now have a way to manipulate fields by adjoining a certain element. It turns out that this notion of extension has an implicit relation to polynomials. When we wish to start thinking about the length of the extension, or how far away an extended field is from its base field, we must first analyze their relation to polynomials. We will start by proving that every irreducible monic polynomial must map coefficients of the base field of an extension to a number in the extended field.

Theorem 1:
If K is any subfield of $\mathbb{C}$ and m is any irreducible monic polynomial over K, then there exists $\alpha \in \mathbb{C}$, algebraic over K, such that α is a root of minimal polynomial m over K.

Proof:
Let $\alpha \in \mathbb{C}$ have minimal polynomial f over K, and be any zero of $m \in \mathbb{C}$. Then f must divide m. But m is irreducible and both polynomials are monic, so $f = m$ □

Now that we can associate an irreducible polynomial to every $\alpha \in \mathbb{C}$, we must understanding how to use this notion to measure how much bigger one field is than another. Naturally in mathematics when we discuss the notion of measuring distance between two things we turn to creating a vector space. So we use our knowledge of field extensions to create a vector space that we might use to measure the degree of an extension.

Theorem 2:
If L/K is a field extension, then the operations

$$(\lambda, u) \mapsto \lambda u \qquad (\lambda \in K, u \in L)$$

$$(u, v) \mapsto u + v \qquad (u, v \in L)$$

define on L the structure of a vector space over K.

Proof:
We must verify the following axioms to verify this is a vector space.

1. $u + v = v + u$ for all $u, v \in L$.
2. $(u + v) + w = u + (v + w)$for all $u, v, w \in L$
3. There exists an additive identity in L.
4. There exist additive inverses in L.
5. The multiplicative identity of K, 1, satisfies $1 * u = u$ for all $u \in L$.
6. If λ,$\mu \in K$, then $(\lambda)\mu u = \lambda(\mu u)$ for all $\mu \in L$.

It is clear that each of these follows directly from the assumption that we are working with subfields of $\mathbb{C}$ and that $K \subset L$.

So we now have defined a vector space, and vector spaces are good for measuring distances and having degrees. So what can we do with this information? We make the following definition:

Definition 3:
The degree $[L : K]$ of an extension L/K is the dimension of the vector space V of L over K.

So now we know how to measure the distance covered by field extensions, or equivalently how much bigger one field is than another. But what if our extension is by more than one element? We know that for an extension L/K, if $L = K(\alpha_1, \alpha_2)$ then we can define $M = K(\alpha_1)$ and $L = M(\alpha_2)$. So we can take our extensions step by step. Does this work

work degrees? We will prove the answer with a theorem.

Theorem 4: Short Tower Law
If K,L,M are subfields of $\mathbb{C}$ *and* $K \subseteq L \subseteq M$ *then*

$$[M : K] = [M : L][L : K]$$

Proof:

Let $(x_i)_{i \in I}$ be a basis for L as a vector space over K and let $(y_j)_{j \in J}$ be a basis for M over L. For all $i \in I$ and $j \in J$ we have $x_i \in L$ and $y_j \in M$. We will show that $(x_i y_j)$ is a basis for M over K (where $x_i y_j$ is the product in the subfield M). Since dimensions of vector spaces are the cardinality of their bases the theorem will follow.

First we prove that they are linearly independent. Suppose that some finite combination of the basis elements is zero:

$$\sum_{i,j} k_{ij} x_i y_j \qquad (k_{ij} \in K)$$

We can rearrange this as two sums:

$$\sum_j \left(\sum_i k_{ij} x_i \right) y_j = 0$$

Now since the $k_{ij} x_i$ lie in L and we know they are linearly independent over L we see that

$$\sum_i k_{ij} x_i = 0$$

We can repeat this argument inside L and find that the k_{ij} must be zero. So the elements $x_i y_j$ must be linearly independent over K. Next we show that the $x_i y_j$ span M over K. We know any element in M can be written as

$$x = \sum_i \lambda_{ij} x_i$$

for some $\lambda_{ij} \in K$. Finally, putting it all together we see that

$$x = \sum_{i,j} \lambda_{ij} x_i y_j$$

as we wanted to show. □

Now we can generalize and use induction to use the deduce the following corrollary:

Corrollary 5: Tower Law

If K_j/K_0 is a field extension then $[K_j : K_0] = [K_j : K_{j-1}][K_{j-1} : K_{j-2}]...[K_1 : K_0]$.

So now we can fully discuss the degree of an extension as a product of its intermediate simple extensions. However, we still have no way to discuss what an easy way to find the number of elements needed for a basis of the vector space defined by our field extension really is. For this, we will finally return to polynomials. We need the notion of transcendental extension and algebraic extensions first:

Definition 6:

Let $L = K(\alpha)$. If α is the root of some polynomial whose coefficients lie in K, then we say L/K is an algebraic extension. Otherwise it is transcendental.

Now we use this definition to formally understand how to find the degree of a field extension.

Proposition 6:

Let $K(\alpha) : K$ be a simple extension. If it is transcendental then $[K(\alpha) : K] = \infty$. If it is algebraic, then $[K(\alpha) : K] = \partial m$, where m is the minimal polynomial of α over K.

Proof:

We consider only simple extension by use of the tower law. So let $K(\alpha)$ be a field extension and let f be the minimal polynomial of α over K, with $\partial f = n$. Then we see that as proved earlier $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ are linearly independent and constitute a basis for $K(\alpha)$ over K. So $[K(\alpha) : K] = n$. □

So now we finally have a working understanding of field extensions, how they work, how to measure them, and how they relate to polynomials. It turns out that this relation to polynomials is precisely what makes field extensions useful for proving the geometric impossibilities. Let us investigate.

1.3 Ruler and Compass Constructions

So we turn to Ruler and Compass construction. The game from antiquity where Greeks challenged themselves to construct certain geometric figures using only an unmarked ruler and a pair of compasses. As stated before, the legal moves in the game were to draw a start line between to given or constructed points, or to draw a circle centered at one point

with another point at radius from the center using the compasses. We wish to find a way to relate each construction to a polynomial, and therefore a field extension, so we may get a feeling for what types of constructions, and thus field extensions, are not possible in the given constraints of the game.

First we make some useful notation. We will say that in each construction we will start with a set of points P_0. Typically $P_0 = \{(0,0),(0,1)\}$ or $P_0 = \{(0,0),(1,0)\}$ because the problems have to do with addressing constructions of unit length. However in full generality P_0 could be any set of points. We will also say that K_0, our base field in these constructions is the field generated by thinking of each element x_i, y_i that are coordinates of our points r_i as generating a subfield of $\mathbb{R}$. For example, if $P_0 = \{(0,0),(0,1)\}$ then our base field $K_0 = \mathbb{Q}$.

Now that we have this general feeling for how this relation between field theory and construction will work, we only need two proofs to give us the machinery to discuss the problems fully. First, we make a formal tie between polynomials, field extensions, and the geometric constructions.

Lemma 7:
Let x_j and y_j be the coordinates of the point r_j and K_j be the subfield attained by adjoining a smaller field $K_{j-1} \subset K_j$ with the set $\{x_j, y_j\}$ so that $K_{j-1}(x_j, y_j) = K_j$. With this definition, x_j and y_j are zeros in K_j of quadratic polynomials over K_{j-1}.

Proof:
The important part to understand here is that they are all zeros of *quadratic* polynomials. So all constructions constitute a minimal polynomial of degree 2.

So we must show for each case, line meets line, line meets circle, and circle meets circle, that the generated points are successively found as roots of quadratic polynomials. We will , as Stewart does, take the case line meets circle and show hwo the simple coordinate geometry produces a quadratic polynomial, and leave the other two cases to practice:

Let $A = (p,q)$,$B = (r,s)$,$C = (t,u)$ be points whose coordinates lie in K_{j-1}. Then draw the line AB and circle whose center is at C with radius w with $w^2 \in K_{j-1}$, we know that $w^2 \in K_{j-1}$ since w is the distance between two points C and either intersection of line AB with the circle. So the equation of the line AB is $AB : \dfrac{x-p}{r-p} = \dfrac{y-q}{s-q}$, and the equation of the circle becomes $(x-t)^2 + (y-u)^2 = w^2$. Finally we combine both equations to find our quadratic $(x-t)^2 + (\dfrac{s-q}{r-p}(x-p) + q - u)^2 = w^2$ for the x coordinates. The same holds true for the y coordinates. □

This is a big step! Now we can relate each construction of new points to a quadratic polynomial, and earlier we related polynomials to field extensions. We're nearly ready to use our full machinery to prove the impossibilities. Lastly we need a way to make the transitive leap from constructibility to field theory. We prove the following theorem to do so:

Theorem 8:
If $r = (x, y)$ is constructible from a subset of points P_0 of $\mathbb{R}^2$, and K_0 is the subfield of $\mathbb{R}$ generated by the coordinates of the points of P_0 then the degrees

$$[K_0(x) : K_0] \quad \textit{and} \quad [K_0(y) : K_0]$$

are powers of 2.

Proof:

We use our notation as above. Using the previous results we see that

$$K_{j-1}(x_j) : K_{j-1}] = 1 \text{ or } 2$$

And similarly

$$K_{j-1}(y_j) : K_{j-1}] = 1 \text{ or } 2$$

For both we see that if the corresponding polynomial is reducible then we have an extension of degree one, otherwise it is two. Now, by the tower law we have

$$K_{j-1}(x_j, y_j) : K_{j-1}] = [K_{j-1}(x_j, y_j) : K_{j-1}(x_j)][K_{j-1}(x_j) : K_{j-1}] = 1 \text{ or } 2 \text{ or } 4$$

Upon inspection we find the value of 4 never arises, and further we observe that since

$$[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0]$$

is a power of 2, then we see that so also must $[K_0(x) : K_0]$ be a power of 2. □

1.4 Proofs of Impossibility

At last we have all the machinery we need to skewer the three problems of antiquity. We proceed in level of difficulty.

Theorem: Impossibility of Doubling the Cube:
Given the side length of any cube, it is impossible to construct the side of a cube of double the volume.

Proof:

Say $P_0 = \{(0,0)(1,0)\}$ is our cube's side of unit length. Then our base field $K_0 = \mathbb{Q}$. So, constructing a cube of double the volume would be equivalent to constructing the point $(\alpha, 0)$ where $\alpha^3 = 2$. So by the previous theorem, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ should equal 2^n for some $n \in \mathbb{N}$. But α has minimal polynomial $t^3 - 2 = 0$. So $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. And 3 is not a power of two. □

Next we show that in general, it is impossible to trisect an angle. That's not to say there are no angles that can be trisected. Given the angle π it is simple to construct the angle $\pi/3$. For this proof we will exhibit one angle that cannot be trisected, showing that it is not possible in general. First, the theorem:

Theorem: Impossibility of Trisecting a General Angle
It is impossible to trisect the angle $\pi/3$, and there for impossible to trisect the general angle.

Proof:

Take $P_0 = \{(0,0), (0,1)\}$ where again $K_0 = \mathbb{Q}$. We first note that constructing the angle $\pi/3$ is relatively easy. Simply bisect the line between the two starting points, and draw the unit circle. Then the line from the origin to the intersection constitutes and angle of $\pi/3$. This is because we constructed the point $(\cos\theta, 0)$ and used it to intersect the unit circle, making an angle of *theta* with the x axis. So trisecting the angle $\pi/3$ is equivalent to starting with P_0 and constructing the point $(\alpha, 0)$ where $\alpha = \cos\dfrac{\pi}{9}$. From this we could construct $(\beta, 0)$ where $\beta = 2\alpha$. Now we turn to trigonometric identities to find the minimal polynomial of the construction.

Remember the $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Substitute $\theta = \pi/9$ and we get $\cos 3\theta = 1/2 = (\beta^3/2) - (3/2)\beta$. Multiply by two and subtract to get the polynomial $\beta^3 - 3\beta - 1 = 0$. We show that this polynomial is irreducible by using Eisensteins criterion on $f(\beta + 1)$.

Finally, once we know the polynomial is monic and irreducible, we deduce that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. So β and thus α are not constructible, so it is impossible to trisect the angle $\pi/3$. □

Now finally we turn to the final and most idiomatically famous problem, squaring the circle. For this proof we will need to take the transcendence of π over $\mathbb{Q}$ as a given, since its proof is lengthy and unrelated. Again, first we see the theorem:

Theorem: Impossibility of Quadrature:
Given a circle in the plane, it is impossible to construct a square of equal area using only ruler and compass constructions.

Proof:

Begin with $P_0 = \{(0,0), (1,0)$ to draw the unit circle. Then we claim that squaring the

circle would be equivalent to constructing the point $(0, \sqrt{\pi})$ from P_0. However we note that if $(0, \sqrt{\pi})$ is constructible then so is $(0, \pi)$. We will then prove the contrapositive to show that $\neg(0, \pi)_{constructible} \implies \neg(0, \sqrt{\pi})_{constructible}$.

From here it is simple. If $(0, \pi)$ was constructible then $[\mathbb{Q}(\pi) : \mathbb{Q}]$ would be a power of 2. However we know than π is transcendental over $\mathbb{Q}$ so $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. □

So we have proven the basic three geometric impossiblities! A great accomplishment. This level of abstraction will set us up nicely to work our way into the full machinery of Galois theory and be able to prove distinctly that the general quintic polynomial is not solvable by radicals.

Chapter 2

Insolvability of the Quintic

2.1 Introduction

So we have proved using basic field theory that the three geometric problems of antiquity are in fact impossible using only ruler and compass constructions. A very natural question to ask is what motivated these tactics to solve these problems? The answer lies directly in the hundreds of years that mathematicians spent devoted to studying the solutions of the quintic polynomial. It was proved in the late 1500's that the third and fourth degree (which can be tactly transformed into a resolvent cubic eqauation) are indeed solvable by radicals. What remained was to prove that the quintic polynomial did or did not have a solution by radicals. Many mathematicians including the famous Ruffini, Lagrange and Abel studied radicals in the hopes that they would glean some new insight about the type of equation needed to solve the general quintic. They nearly succeeded. What truly cracked the code so to speak was young Galois' invention of a new mathematical structure. He created the first understanding of symmetric groups and field extensions, and it was his work in combining the two notions that truly progressed the work.

2.2 Galois Theory Proper

To begin, we will advance our knowledge of field theory and field extensions, and then finally broach the area of Galois theory proper. First we see a definition of a special kind of map within a field extension:

Definition 1:
Let $L : K$ be a field extension. A K-automorphism of L is a map $\rho : L \to L$ such that ρ is homomorphism from L to L (and therefor an isomorphism as well), and for all $k \in K$, $\rho(k) = k$. Further, when this definition holds, we say that K is the fixed field of ρ.

This definition is incredibly important to understand, because it is the center of Galois theory. More conceptually, we can think of a K-automorphism of L as any map that fixes all of K but permutes some elements of L. This will be especially important when we start

to relate this notion of permuting just certain elements to the roots of polynomials, as one might predict. Next, we see what properties these special maps of field extensions have when composed.

Theorem 2:
If L/K is a field extension, then the set of all K-automorphisms of L is a group under composition of maps.

Proof:
For proof, we must simply verify the group axioms.

1. First we show closure. Suppose α and β are automorphisms of L. Then clearly their composition is an automorphism. Similarly $\alpha \circ \beta(k) = \alpha(\beta(k)) = \alpha(k) = k$. So the group is closed.

2. All α and β in the group are automorphisms and therefor invertible. See that $k = \alpha^{-1}\alpha(k) = \alpha^{-1}(k)$ so it is a K-automorphism.

3. The identity map is clearly a K-automorphism.
4. The maps are clearly associative. □

So we know that we can construct a group of all the K-automorphisms, and indeed we make a central, formal definition of this group.

Definiton 3:
The Galois group of a field extension L/K, denoted in this paper as $\Gamma(L/K)$, is the group of all K-automorphisms of L under the group law of composition of maps.

This is one of the central takeaways. Though we have already explored the three geometric impossiblities, we never defined anything that had Galois' name on it or his work explicity tied to it. Now we have made this step. It was this merging of polynomials, field extensions, and group theory that made Galois such a savant, and solidified his place in history.

To work with this group, we would like to identify each step of the extension and what its group structure looks like. To do so we need to have a correspondence between the intermediate fields of L/K and the subgroups of $\Gamma(L/K)$. Clearly we need to define functions to transport us both from the world of Field extensions and K-automorphisms into the world of group structure, and likewise from the world of groups to fields. So we define these maps as follows:

Definiton 4:
Let L/K be a field extension. Then $\mathcal{F}$ is the set of all intermediate fields, $\mathcal{G}$ be the set of all subgroups H of the Galois group $\Gamma(L/K)$. Then we define two maps

$$^* : \mathcal{F} \to \mathcal{G}$$

$$^{\dagger} : \mathcal{G} \to \mathcal{F}$$

So for example if $M \in \mathcal{F}$ then M^* is the group of all M-automorphisms of L, and if $H \in \mathcal{G}$ then $H^{\dagger}$ is the fixed field of H. We observe that the maps reverse inclusion so the largest field will produce the smallest group and vice versa. This is because the smallest fixed field we can produce from the map is K, and no group of automorphisms fixes a smaller field than the automorphisms of L. If $K \subset M \subset L$ then M^* is a larger field than K. That is $L^* \subset M^* \subset K^*$.

We need one more definition before we jump into the fundamental theorem of Galois theory, and it is a relative simple one. It contains two new concepts mashed together.

Definition 5:

The splitting field of a polynomial f with rational coefficients, denoted Σ_f is the smallest field such that f splits into linear factors. Also, if $M \subset \Sigma_f$ and f splits in M then $M = \Sigma_f$. Also, we say that a field extension L/K is normal if and only if every polynomial with coefficients in K that has at least one root in L splits in L.

So we have an inclusion reversing map between groups and fields and we have a definition for what to call a field when it is just big enough to contain all zeros of the polynomial. This will allow us to fully discuss the results of the fundamental theorem of Galois theory and prove them in full force.

Fundamental Theorem of Galois Theory
If L/K is a normal extension inside $\mathbb{C}$, with Galois group G, and if $\mathcal{F}$, $\mathcal{G}$, †, * are defined as above, then:

1. *The Galois group has order $[L : K]$*
2. *The maps *, and † are mutual inverses, and setup an order-reversing one-to-one correspondence between $\mathcal{F}$ and $\mathcal{G}$.*
3. *If M is an intermediate field, then*

$$[L : M] = |M^*| \qquad [M : K] = |G|/|M^*|$$

4. *An intermediate field M is a normal extension of K if and only if M^* is a normal subgroup of G.*
5. *If an intermediate field M is a normal extension of K, then the Galois group $\Gamma(M : K)$ is isomorphic to the quotient group G/M^*.*

Proof:

We will make our way from one to five.

First, we show that the Galois group (for a normal extension inside $\mathbb{C}$ has order $[L : K]$. We proceed by induction on $[L : K]$. If $[L : K] = 1$ then the result is trivial. Now suppose $[L : K] = k > 1$. Let $\alpha \in L/K$ with minimal polynomal m over K. Then $\partial m = [K(\alpha) : K] = r > 1$. So now m is an irreducible polynomial over some subfield of $\mathbb{C}$ with one zero in the normal closure N o K, and so it must split in N. By induction we see there are exactly $s = [L : K(\alpha)] = k/r$ $K(\alpha)$ monomorphisms of from L to N. We now there are r distinct K automorphisms of N, and the composition of these maps shows we have $rs = k$ distinct K automorphisms of L, and that these exhaust the K monomorphisms from L to N. So the number of K automorphisms of L is exactly the degree of the field extension, and **1.** is proved. □

Next, we show that the maps $^*and^\dagger$ are mutual inverses that set up an order reversing bijection between $\mathcal{F}$ and $\mathcal{G}$. This is simple. Since L/K is normal, then we have shown the intermediate fields are normal as well, so $M^{*\dagger} = M$. The other direction is a bit more tricky. Consider $H \in \mathcal{G}$. We know that at least $H \subseteq H^{\dagger *}$. So $H^{\dagger *\dagger} = H^\dagger$ and that $|H| = [L : H^\dagger] = [L : H^{\dagger *\dagger}]$ and finally that $[L : H^{\dagger *\dagger}] = |H^{\dagger *}|$ so $H \subseteq H^{\dagger *}$ and $|H| = |H^{\dagger *}$ so $H = H^{\dagger *}$. So **2.** is proved □

The third is almost immediate. It lies in our assumption that L/K is normal and that we know for an intermediate field M that $[L : M] = |M^*|$. The fact that $[M : K] = |G|/|M^*$ follows immediately from our definition of the maps. So **3.** is proved □

The last two proofs require a short lemma. The proof is short and unrelated so we omit it.

Lemma 6:
Suppose L/K is a field extension with M as an intermediate field and τ is a K-automorphism of L. Then $\tau(M^*) = \tau M^* \tau^{-1}$.

Now we use the lemma to show that if τ is a K-monomorphism from M to L then $\tau(M) = M$ and $\tau M^* \tau^{-1} = M^*$. So M^* is unchanged under conjugation and therefor a normal subgroup of G. The other direction of implication follows a similar argument except that we must notice for any K automorphism of L τ we can find a corresponding M automorphism of L σthat satisfies $\tau_M = \sigma$. So **4.** is proved. □

Finally we show **5.**: Let $G = \Gamma(L/K)$ and $G' = \Gamma(M/K)$. Then we can define $\varphi : G \to G'$ such that $\varphi(\tau) = \tau_M$. As we have proved before φ is a K automorphism of L and it is surjective. So the kernel of φ, $ker(\varphi) = M^*$. Then we use standard notation to derive $G' = im(\varphi) = G/ker(\varphi) = G/M^*$, and the final piece is proved. □

So finally we have proved every piece of the fundamental theorem of Galois theory and we can use each piece more as a tool than as an impressive result. This is the natural vein of Galois theory in general, the constructions are not beautiful results themselves, but their power in handling abstract field extensions is great and will allow us to discuss the quintic

polynomial in full generality.

2.3 Solvability

To begin talking of the quintic polynomial we need to draw a connection between the Galois group and its related tools, and the light it sheds on the field extensions related to certain polynomials. This thread of logic should feel very familiar. It's what we've been doing through the whole paper, taking one idea and another seemingly unrelated structure that has great proof power and connecting them in a way that is crucially beneficial. We begin this relation with a definition that will allow us to test Galois groups for an important property: solvability.

Definiton 7:
We say a group is solvable if it has a finite series of subgroups:

$$1 = G_0 \subseteq G_1 \subseteq ... \subseteq G_n = G$$

such that

1. $G_i \triangleleft G_{i+1}$, *where* $i = 0, .., n$.
2. G_{i+1}/G_i *is abelian, where* $i = 0, .., n$.

This seems hard to articulate and even harder to calculate. How can one find a series of normal subgroups that spans the distance from the group in totality all the way to the identity? Well the answer is indeed unclear. However, it would be more clear if there were an easy way to find groups where this bridge was either relatively short or nonexistent and that is where we turn to next.

Defintion 8:
We say a group G is simple if its only normal subgroups are 1 and G.

So a simple group has a connect of normal subgroups from the whole group to the identity, namely $1 \triangleleft G$. The shortest bridge possible. So we find any easy was to test for solvability of a group is to find a simple, abelian group. If the group is simple then it satisfies **1.** of solvability, and if it is abelian then it clearly satisfies **2.** as well. We also notice that if a group is both simple and solvable, that is must be isomorphic to some $\mathbb{Z}_p$ where p is prime. Clearly $\mathbb{Z}_p$ is abelian and because it is of prime order, its only subgroups are 1 and G. It is abelian so every subgroup is normal, and that ties it up.

We also wish to take a brief tangent (ba dum tss....) to solvability as it relates to radical extensions, because this is the concrete idea behind solvability of a polynomial. So we give

a definition for what a radical extension is and then how it relates to solvability.

Definition 9:
An extension $L : K$, $L = K(\alpha_0, ..., \alpha_n)$ is radical if for all α_n there exists an integer m such that $\alpha_n^m \in K$.

Conceptually speaking, an extension is radical if every root can find its way back to the base field in a cyclic order. Now let us make the connection.

Theorem 10:
If K is a subfield of $\mathbb{C}$ and $K \subseteq L \subseteq M \subseteq \mathbb{C}$, and finally M/K is radical, then $\Gamma(L : K)$ is solvable.

Proof:

This one is a biggie. We will need several preliminary lemmas.

Lemma 10.1:
If L/K is a radical extension in $\mathbb{C}$ and M is the normal closure of L/K then M/K is radical.

Proof:

Let $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$ and let f_i be the minimal polynomial of α_i over K. Then M where $L \subseteq M$ is clearly the splitting field for all the f_i multiplied. So for every zero β_{ij} for each f_i we can construct an isomorphism $\sigma : K(\alpha_i) \to K(\beta_{ij}$. As proved earlier we know that σ must be a K automorphism of M, and since σ is radical over K so is β_{ij} and thus so is M. □

Lemma 10.2
Let K be a subfield of $\mathbb{C}$ and let L be the splitting field for $t^p - 1$ over K, where p is prime. Then $\Gamma(L/K)$ is abelian with cyclic order $p - 1$.
Proof:

The proof is relatively straightforward, and we will summarize. Find a generator and show that two general roots of the polynomial map this generator to their own power so the roots $\alpha_i\alpha_j$ will map to the same generator no matter their order of multiplication. □

Lemma 10.3
Let K be a subfield of $\mathbb{C}$ in which $t^n - 1$ splits, and let $a \in K$, and L be a splitting field for $t^n - 1$ over K. Then $\Gamma(L/K)$ is abelian.

Proof:

Again the proof is straightforward and will be summarized. Set two K automorphisms of L then show that no matter what order you compose them you get the same element of L sicne the maps are defined by their effect of the the adjoined element. So the group is

abelian because the compositions create an equivalent element.

Finally we have the most important lemma to show us that normal extensions are solvable.

Lemma 10.4
If K is a subfield of $\mathbb{C}$ and L/K is normal and radical, then $\Gamma(L/K)$ is solvable.

The proof is not straightforward, but we will summarize. The proof is by induction on the degree of the extension. If the degree is 1 the proof is trivial, and further we must show that since L/K is normal, the polynomial $t^p - 1$ splits in L we may apply our previous lemmas to find that $\Gamma(M(\alpha_1))$ is isomorphic to $\Gamma(L/M)/\Gamma(L/M(\alpha_1)$ and finally that $\Gamma(M/K)$ is isomorphic to $\Gamma(L/K)/\Gamma(L/M)$.

Now we use the lemmas to tie up Theorem 10.

Proof:

Let K_0 be the fixed field of $\Gamma(L/K)$ and Let N/M be the normal closure of M/K_0. Then

$$K \subseteq K_0 \subseteq L \subseteq M \subseteq N$$

Since M/K_0 is radical, N/K_0 is normal and radical and thus its Galois group is solvable. Finally we note that Since $\Gamma(L/K_0)$ must also be solvable and $\Gamma(L/K_0) = \Gamma(L/K)$ that $\Gamma(L/K)$ must be solvable as well. □

The idea behind this tower of lemmas is simple. Each extension we look at in a radical extension is an addition of *nth* roots. Such extensions will always have abelian Glaois groups and the sequence of Galois groups that fit together in a tower of radical extensions will make a sequence of abelian groups. Then finally we can use the tools from the Galois correspondence to show that the Galois groups must then be solvable.

2.4 The General Quintic Polynomial

Now we pivot back to Galois' orignial viewpoint: the quintic polynomial. Here we will encounter yet more new machinery and structure in order to finally put a nail in the coffin of the general quintic. This is the final piece of legwork (really brainwork) we need to do to be able to understand what is truly going on when the degree of the polynomial goes from 4 to 5, and why the jump is significant enough to rob the world of mathematics of a beautiful general formula. First, we yet again tie together previously defined terms, taking the notion of polynomials and splitting field and making them work in the notation of Galois groups.

Definition 11:
The Galois group of a polynomial f over a field K is $\Gamma(\Sigma_f : K)$ where, as expected, Σ_f is the splitting field of f.

Once we have this definition we can rephrase Theorem 10 to the following:

Theorem 10, restated:
Let f be a polynomial over a subfield K of $\mathbb{C}$. If f is solvable by radicals then the Galois group of f over K, $\Gamma(\Sigma_f/K)$ is solvable.

This is actually an if and only if case because the converse holds as well, but the proof requires knowledge of the characteristic of fields, and we will stick to subfields of $\mathbb{C}$ as Galois did. Our primary goal is to prove that the general quintic with coefficients in $\mathbb{Q}$ or some finite extension of $\mathbb{Q}$ is not solvable by radicals. For this we will need to define something called the elementary symmetric polynomial. Before we do this though we will add a bit of motivation.

So we have proved all the types of Galois groups we see and which are solvable and which are insolvable. The central relation behind them all is the structure of the group. Since the groups are made of K-automorphisms of L, we can understand the structure of these groups to be how they permute the roots of the minimal polynomials for the adjoined elements. Let's focus specifically on the permutation aspect. So if we are testing the permutation of the roots of these polynomials to find if the Galois group is solvable, and thus if the equation is solvable with radicals, we need to construct a polynomial that is as general as possible when it comes to permutation of roots. We call this the general polynomial of degree n, and for it we will need to define, as said before, something called an elementary symmetric polynomial.

Definition 12: *The elementary symmetric polynomial is a sum of products of the roots of a polynomial of some degree n. We define them as follows:*

$$s_0 = (-1)^n \alpha_1 \alpha_2 ... \alpha_n$$

$$...$$

$$s_{n-1} = \alpha_1 + \alpha_2 + ... + \alpha_n$$

$$s_n = 1$$

These are called symmetric because their value is unchanged by permutation of the roots. Because each polynomial has only one type of grouping, e.g. all groups of two distinct roots, all groups of three distinct roots, permuting those roots will just switch the order of the groupings. This will leave the value unchanged.

Now our goal is to show that for $n \geq 5$ when you adjoin $s_0, ..., s_n$ to $\mathbb{Q}$, any extension of this field will be isomorphic to the symmetric group of order $n4 =$, and it will be this

key observation that leads us all the way back down the cookie trail to an insolvable Galois group. First we define the general polynomial of degree n.

Definition 13: General Polynomial of Degree n
The general polynomial of degree n over $\mathbb{Q}$, g, is defined as follows:

$$g = s_0 + s_1 t + ... + s_{n-1} t^{n-1} + t^n.$$

Now we only need to do two more things: show when the Galois group is actually the symmetric group of n letters, and further to show when the S_n is not solvable.

Theorem 14:
For any field K, let g be the general polynomial of degree n over K, and let Σ be the splitting field for g over $K(s_1, ..., s_n)$ where the s_n are the elementary symmetric polynomials. Then the zeros $t_1, .., t_n$ of g in Σ are independent transcendental elements over K, and the Galois group $\Gamma(\Sigma : K(s_1, ..., s_n))$ is the symmetric group $\mathbb{S}_n$.

Proof:
For proof we will use $K = \mathbb{Q}$ since that is where we are concerned.

The extension $\Sigma/\mathbb{Q}(s_1, s_2, ..., s_n)$ is finite. Since the t_i are independent transcendental elements the s_i are now the elementary symmetric polynomials in $\mathbb{Q}(t_1, ..., t_n)$. We now make two important observations: that S_n acts as a group of automorphisms on Σ, and that the fixed field of this extension is $\mathbb{Q}(s_1, ..., s_n)$. We know the extension is normal by definition of Σ, so we can use the tools from the fundamental theorem of Galois theory. We know that $\Gamma(\Sigma/\mathbb{Q}(s_1, ..., s_n)$ contains S_n and by **1.** the group has order $n! = |S_n$, so it equals S_n.

We are nearly there. Now recognize that the alternating group A_n is a normal subgroup of S_n and that only in certain cases A_n will be simple. This fixes a very strict criteria for solvability, and so makes it easier to weed out insolvable Galois groups.

Theorem 15:
If $n \geq 5$ then the alternating group A_n of degree n is simple.

Proof:

We know that A_n is generated by all three cycles. First we will assume that $1 \neq N \triangleleft A_n$. We will proceed by observing that if N contains a 3 cycle it contains all three cycles and thus $N = A_n$. Then we must prove that for $n \geq 5$ that N must contain a 3 cycle.

Suppose that N contains a 3-cycle, and WLOG we will assume that $(123) \in N$. For any $k > 3$ the cycle $(32k)$ is an even permutation, and is in A_n and thus

$$(32k)^{-1}(123)(32k) = (1k2)$$

is in N. So N contains $(1k2)^2 = (12k)$ for all $k \geq 3$. So we claim that A_n is generated by all 3-cycles of the from $(12k)$. If $n = 3$ then we're finished. If $n > 3$ then for all $a, b > 2$ the permutation $(1a)(1b)$ is even and thus in A_n and then A_n contains

$$((1a)(1b))^{-1}(12k)(1a)(1b) = (abk)$$

as long as $k =\neq a, b$. Again, since A_n is generated by all 3 cycles then we must have $N = A_n$.

So it remains to show that N must contain at least one 3-cycle. To do this we split into cases.

Case 1. Suppose that N contains an element $x = abc...$, where $a, b, c...$ are disjoing cycles and

$$a = (a_1...a_m) \qquad (m \geq 4)$$

Now let $t = (a_1a_2a_3)$. Then N contains $t^{-1}xt$. Since t commutes with $b, c, ...$ because the cycles are all disjoint, it follows that

$$t^{-1}xt = (t^{-1}at)bc... = z$$

so that N contains

$$zx^{-1} = (a_1a_2a_m)$$

which is clearly a 3 cycle.

Case 2. Suppose that N contains an element involving at least two 3-cycles. WLOG we can say that N contains

$$x = (123)(456)y$$

where y is some permutation fixing $1, 2, 3, 4, 5, 6$. Let $t = (234)$. Then N contains

$$(t^{-1}xt) = (123456)$$

Then by argument of case 1, N contains a 3-cycle.

Case 3. Now suppose that N contains an element x of the form $(ijk)p$, where p is a product of disjoint 2-cycles that are also disjoint from (ijk). Then N contains $x^2 = (ikj)$ which is a 3 cycle.

Case 4. This is the case where every element of N is a product of disjoint 2 cycles. We assume that $n \geq 5$ so we say that N contains

$$(12)(34)p$$

where p fixes $1, 2, 3, 4$. Let $t = (234)$ then N contains

$$(t^{-1}xt)x^{-1} = (14)(23)$$

now say $u = (145)$ so N contains

$$u^{-1}(t^{-1}xtx^{-1})u = (45)(23)$$

so that finally N contains

$$(45)(23)(14)(23) = (145)$$

a 3-cycle, contradicting the intial assumption.

So finally we conclude that A_n is simple if $n \geq 5$. □

We now have all the machinery we need to tackle the general quintic, and so we do. Here is the culmination of the whole chapter:

Final Theorem: Insovability of The Quintic Polynomial:
If $n \geq 5$ then the general polynomial of degree n is not solvable by radicals.

Proof:

We know that the general polynomial as an extension of $\mathbb{Q}$ is isomorphic to S_n, and that if the polynomial is solvable so is the Galois group. So if S_n is solvable then so must A_n be solvable since it is a subgroup of S_n. Then A_n must also be simple by Theorem 15, and so it must be cyclic of prime order. But $|A_n| = (1/2)n!$ is not prime if $n \geq 5$. □

So the general polynomial is killed. This took more machinery but less effort to prove than would be providing an example of a polynomial of degree 5 that is not solvable by radicals. However, the theorem still allows for a curious case: though the general polynomial is insolvable, it is still possible that each individual polynomial has a trick that allows it to be solvable by radicals, so it remains to provide a proof of an insolvable 5th degree polynomial. Next we turn our attention to a related geometric problem that uses Galois theory to show that equivalent values must lead to equivalent field extensions.

Chapter 3

Rational Distance Problem

3.1 Introduction

The Rational Distance Problem can be summarized as follows: if we are given a unit n-gon, the polygon of n vertices with side length of 1, denoted P_n, can we find a point in the plane of $\mathbb{R}^2$ that is a rational distance from all vertices of P_n? The answer to the questions is rather complicated. In our answer we draw almost totally from *Points at Rational Distance from a Unit Polygon* by **Roy Barbara**, published Dec. 15th, 2009. We make several key observations, and offer explanations, evaluating cases by value of n.

For $n \leq 2$, the question is trivial, as P_n is a point or line.

For $n = 3$, the answer is yes, and the points turn out to be dense in the plane of $\mathbb{R}^2$. As cited in Barbara's paper.

For $n = 4$, the answer is not yet known.

For $n \geq 5$ the answer is no unless $n = 6$, in which case the answer is yes, or if $n \in \{8, 12, 24\}$, in which case the answer is unknown.

To answer these cases we will proceed by making a key observation about the geometry of the problem, and then relate this observations to field extensions and their corresponding Galois groups to show that only the certain n listed above are candidates for solutions to the problem.

Here is our formal definition of the problem: the theorem we will keep in the back of our mind and return to prove once we have built up sufficient machinery.

Central Theorem:
If for $n \geq 3$, P_n stands for the unit n-gon, then let $P1$ be the proposition, "Is there a point at rational distance from the vertices of P_n?"

For $n = 5$ the answer to $P1$ is false.
For $n = 6$ the answer to $P1$ is true.
For $n \geq 7$ the answer to $P1$ is false, except possibly when $n = 8, 12, 24$.

For proving our central theorem we must also make a central observation. We will start by analyzing the geometry of the problem, making a slightly rigorous treatment of the ad hoc method for solving the problem that most would take. This observation will allow us to make the jump between Geometry and Galois theory and derive a proof to the central

theorem.

Central Observation:
For the statement $P1$ to be true, the following relation must holds. For a unit n-gon P_n:

$$\frac{n}{4}\cot\frac{\pi}{n} = \sqrt{a_1} \pm \sqrt{a_2} \pm ... \pm \sqrt{a_n}$$

where the a_i are positive rational numbers.

3.2 Deriving The Relation

At first glance the relation is rather odd. It seems to be making a trigonometric equality to a sum of quadratic roots. However, once we inspect the problem a little closer, the relation is clear, and its power toward narrowing down possible cases for the solution of the problem is great. So let us dive in.

First notice that for any point in a supposed solution, there will be a number of triangles, whose sides are lines drawn from the point to two adjacent vertices of P_n, equal to n. For example, for any point in the plane of $\mathbb{R}^2$, we can draw 5 unique triangles from adjacent vertices for a pentagon, 6 for a hexagon, etc. We will always have n triangles.

Next notice that we can split the points into two cases, inside P_n and outside P_n. We claim that no matter the case, the area of P_n can be constructed from the area of the triangles.

For the first case, where the point is inside P_n, it is clear that the sum of the areas of the n triangles will add to the area of P_n. So we find that Area(P_n)=Area(Triangles).

For the next case, where the point is outside P_n, the answer is just a bit more complicated. For these points we see that some of triangles areas will intersect the area of P_n, and some will be completely outside the area of P_n or deprecated completely if the point lies on the line extending through a side of P_n. For this case we define a *negative triangle* to be one whose area lies completely outside of P_n and a *positive triangle* to be one whose area in any way overlaps the area of P_n. We claim that by subtracting the area of the negative triangles from the area of the positive triangles then we will obtain exactly the area of P_n. So we have that no matter the case of the point in the plane, Area(P_n) = Area(Triangles).

Let us now dissect both sides of this equation. For the area of P_n we utilize simple geometry. Note that we can calculate the area of any P_n by assuming the chosen point is the center point of P_n. Then all triangles are congruent. We also note that the sum of the angles adjacent to the center point will be 2π. So the value of one angle

is $\frac{2\pi}{2}$. To calculate the area of this triangle we bisect this angle to make a right triangle. Then the base of the triangle is 1/2 and the height is $(1/2) * \cot\frac{2\pi}{2n}$. So the area is $(1/2)(b)(h) = (1/2)(1/2)(1/2)(\cot\frac{2\pi}{2n} = (1/8)\cot\frac{\pi}{n}$. Recall this is the area of an inner triangle divided in two, so we have $2n$ triangles, giving a total area of $\frac{n}{4}\cot\frac{\pi}{n}$, as we stated in the beginning of the section.

Now for the area of the triangles we remember that for the answer to $P1$ to be true, we must have all distances rational, and therefore all sides of the triangle rational. So we use Heron's formula to calculate Area(Triangle) $= \sqrt{s(s-a)(s-b)(s-c)}$, where a,b,c, are the side lengths of the triangle, and s the semiperimeter, to show the area of all triangles is a sum of positive and negative areas, all square roots of rational numbers.

Finally, we have derived our central relation:

$$\frac{n}{4}\cot\frac{\pi}{n} = \sqrt{a_1} \pm \sqrt{a_2} \pm ... \pm \sqrt{a_n}$$

.

3.3 Group Theory With Flat Fields

Now let us understand that since our relation poses an inequality, if we extend $\mathbb{Q}$ by adjoining either the left-hand side or the right-hand side of the relation, we will achieve the same extension of $\mathbb{Q}$. Notice the right-hand side will always constitute an extension of degree 2^n, and the Galois group will always be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 ... \times \mathbb{Z}_2$ an n amount of times. So, if we can show that the Galois group of $\mathbb{Q}(\frac{n}{4}\cot\frac{\pi}{n})$ is not such a group, then we will have reached a contradiction.

First we define such a group:
Definition 1:
We say that a field is L flat if every subfield K satfies the following:

$$\Gamma(K/\mathbb{Q}) = 2^n$$

and $\Gamma(K/\mathbb{Q})$ *is a product of* $\mathbb{Z}_2$*s.*

Then clearly every subfield of a flat field is flat, and we leave it as a quick exercise to prove that $\mathbb{Q}(\sqrt{a_1} \pm \sqrt{a_2} \pm ... \pm \sqrt{a_n})/\mathbb{Q}$ is flat. Now we begin to make our arguments about

for what n make a $\mathbb{Q}(\frac{n}{4}\cot\frac{\pi}{n})$ is not flat.

To begin, we will make a useful proposition:

Proposition 1:
Let d,m,n be positive integers with $d > 1$ and $n = dm$. Then $\mathbb{Q}(cot\frac{\pi}{d})$ and $\mathbb{Q}(cos\frac{2\pi}{d})$ are subfield of $\mathbb{Q}(cot\frac{\pi}{n})$.

Proof:

Let $x = \frac{\pi}{n}$ and $y = \frac{\pi}{d}$. Then as defined above $y = mx$. We will use induction on m to see that $y \in \mathbb{Q}(\cot x)$. See that $\cot(m+1) = \frac{\cot mx * \cot x - 1}{\cot mx + \cot x}$. Now let $t = \cot x$. Use the identity $\cos\frac{2\pi}{d} = \frac{t^2-1}{t^2+1}$ and the fact that $t \in \mathbb{Q}(\cot\frac{\pi}{n})$ to see that $y \in \mathbb{Q}(\cot x)$ as claimed. □

This will prove useful in the final proof. Now we need to understand for what kinds of prime numbers of n will we achieve a flat field extension of $\mathbb{Q}$. We will prove a lemma:

Lemma 1:
Let p be a prime number. Suppose the relation $a^2 = p(b^2 + c^2)$ holds for some a, b, c. Then we see that $\mathbb{Q}(\sqrt{a + b\sqrt{p}}) : \mathbb{Q}$ is a cyclic extension of degree 4.

Proof:

Recognize that $a + b\sqrt{p}$ is not a square in $\mathbb{Q}(\sqrt{p})$. So set $x = \sqrt{a + b\sqrt{p}}$. We know that $x \notin \mathbb{Q}(\sqrt{p})$. But recognize that x^2 *is* in $\mathbb{Q}(\sqrt{p})$. So x^2 has degree two over $\mathbb{Q}$ and hence x has degree 4 over $\mathbb{Q}$

Now we must show that the extension is cyclic. See that the irreducible polynomial of x over $\mathbb{Q}$ is

$$f = X^4 - 2aX^2 + (a - pb^2)$$

, and that the Galois group $G = \Gamma(\mathbb{Q}(x)/\mathbb{Q})$ has order four and is a transitive group. So the elements of G permute the roots of f in a four cycle. So the extension is both cyclic and degree 4. □

Now using Proposition 1 and Lemma 1 we can show that the kinds of extensions of $\mathbb{Q}$ that interest of are cyclic of degree 4, and therefore there Galois group is not a product of $\mathbb{Z}_2$s. We will begin with n equal to 5 and 16.

Proposition 2:
Both $\mathbb{Q}(\cot\frac{\pi}{5})$ and $\mathbb{Q}(\cot\frac{\pi}{16})$ are cyclic extensions of degree 4, and therefore not flat.

Proof:
For 5, use the identity $5\cot\frac{\pi}{5} = \sqrt{25+10\sqrt{5}}$ and apply Lemma 1 with $p = 5$, and $(a, b, c) = (25, 10, 5)$.
For 16, use the identity $\cot\frac{\pi}{16} = 1 + \sqrt{2} + \sqrt{4+2\sqrt{2}}$ and see that $\mathbb{Q}(\sqrt{4+2\sqrt{2}} = \mathbb{Q}(1+\sqrt{2}+\sqrt{4+2\sqrt{2}}$. Then apply Lemma 1 with $p = 2$ and $(a, b, c) = (4, 2, 2)$. □

Now we extract one more case that breaks our relation. We will use another proposition to show that both primes 7 or greater and the number 9 break the extension relation.

Proposition 3:

Let $p \geq 7$ be a prime number. Then $\mathbb{Q}(\cos\frac{2\pi}{p})/\mathbb{Q}$ is a cyclic extension of degree greater than or equal to 3. Similarly,$\mathbb{Q}(\cos\frac{2\pi}{p})/\mathbb{Q}$ is a cyclic extension of degree 3.

Proof: Let $\Omega = \mathbb{Q}(e^{i\frac{2\pi}{p}})$. We know that $\Omega/\mathbb{Q}$ is a cyclic extension of degree $p-1$. We know $\mathbb{Q}(\cos\frac{2\pi}{p})$ is a sub extension of Ω and it has degree $\frac{p-1}{2} \geq 3$.
For Ω with $p = 9$ we know that $\Omega_9/\mathbb{Q}$ is abelian since we just have roots of unity. Then we see that $\mathbb{Q}(\cos\frac{2\pi}{9})$ is a Galois extension and its degree is $(1/2)\phi(9) = 3$. Any group of order 3 is cyclic, so the proof is completed. □

Finally we move to amalgamating our proofs to explicitly state which extensions are flat and which are not.

3.4 Final Proofs

Proposition:
Let $n \geq 5, n \neq 6$. Then if $\Omega = \mathbb{Q}(\cot\frac{\pi}{n})$ is a flat field, we must have $n = 8, 12, 24$.

Proof:

Suppose that n is divisible by 5. Then we see that Proposition 1 shows that $\mathbb{Q}(\cot\frac{pi}{5}$ is a subfield of Ω and Proposition 2 shows that the Galois group of $\mathbb{Q}(\cot\frac{pi}{5}/\mathbb{Q}$ is a cyclic group of order 4, and not flat.

Now suppose that n is divisible by 16. Like above by Proposition 1 $\mathbb{Q}(\cot\frac{pi}{16}$ is a subfield of Ω and proposition 2 shows that the Galois group of $\mathbb{Q}(\cot\frac{pi}{16}/\mathbb{Q}$ is a cyclic group of order 4, and not flat.

Now suppose that n is divisible by 9. Again, by proposition 1, $\mathbb{Q}(\cot\frac{pi}{16}$ is a subfield of Ω and proposition 3 shows that the Galois group of $\mathbb{Q}(\cot\frac{pi}{9}/\mathbb{Q}$ is a cyclic group of order 3, and not flat. □

Now finally notice that since $\frac{n}{4}$ would always be a rational number, $\mathbb{Q}(\frac{n}{4}\cot\frac{\pi}{n}) = \mathbb{Q}(\cot\frac{\pi}{n})$.

Final Proof of Original Theorem:

Proof:

For $n = 5$ we see that the extension is not flat, so our primary relation is contradicted.

For $n = 6$ the answer is yes. See that the center point of a unit hexagon is at unit distance from all vertices.

For n $geq7$ we note that there are few conditions that must be satisfied. For the answer to $P1$ to be yes, n must be of the form $n = 2^{(1,2,3)}3^(0,1)$ since we have proved that if 16 divides n, the extension will not be flat, and if 9 divides n, the extension will not be flat. So finally for $n \geq 7$ the answer is no except when $n \in \{8, 12, 24\}$. □

So we have tied it all together. What we find especially interesting about this problem is that the basic premise leaves it open to those only old enough to know basic geometry. However, the complexity of the proposed partial solutions is at the level of late undergraduate or early graduate level mathematical understanding. Finally, we note that of the open cases (where $n = 4, 8, 12, 24$), the hardest case seems to be the square, $n = 4$.

References:

[1] Galois Theory by Ian Stewart (2003) 3rd Edition, Chapman and Hall/CRC, A CRC Press Company, Boca Raton.

[2] R. Barbara, Points at rational distance from the vertices of a unit polygon, Bulletin of the Iranian Mathematical Society, vol. 35, pp. 209215, 2009.