# Lecture 1-8: Classical construction problems and splitting fields

January 8, 2025

There are three classical construction problems, dating back to the ancient Greeks, which ask whether if it possible to carry out certain geometric constructions using only a compass and an *unmarked* straightedge. More precisely, they ask whether it is possible with these tools to duplicate the cube, that is, to construct a cube whose volume is exactly twice that of a given cube; to trisect the angle, that is, to construct an angle of $\theta$ radians given one of $3\theta$ radians; and to square the circle, that is, to construct a square whose area is the same as that of a given circle.

The answer to all of these questions is no, but one must be careful to understand what this answer means in each case. In the first case, we choose a unit of length and are given two points this distance apart; in the second case, parametrizing angles by their cosines, we are given two points exactly $\cos 3\theta$ apart, and in the third case we are again given two points at unit distance. In the first case, we must construct two other points at distance $2^{1/3}$; in the second, we must construct two points at distance $\cos\theta$; and in the third we must construct tow points at distance $\sqrt{\pi}$. In the second case, I need to specify more precisely what $\theta$ is. There are many angles $\theta$ that can be constructed directly, without the use of any auxiliary angles (for example $\theta = \pi/2$); there are other angles $\theta$ such that one cannot construct an angle of $\theta$ radians from scratch, but one can construct such an angle if one of $3\theta$ radians is given. I will show however that one can construct an angle of $\pi/3$ radians (this is easy) but not one of $\pi/9$ radians.

In each case the tools allow me only to construct the line through two given points, or the circle with a given center passing through a given point, or the intersection(s) of two such lines or circles. The well-known equations of lines and circles in the Cartesian plane show that the only possible distances between pairs of points constructed in this way are those lying in fields constructed from the rational field $\mathbb{Q}$ by a sequence of iterated quadratic extensions, that is, lying in a field $\mathbb{Q}_n \subset \mathbb{R}$ such that there are fields $\mathbb{Q}_0 = \mathbb{Q}, \mathbb{Q}_1, \ldots, \mathbb{Q}_n$ such that each $\mathbb{Q}_i$ is a quadratic extension of $\mathbb{Q}_{i-1}$. Conversely, there are elementary constructions showing that one can construct two points at distance $\alpha$ if $\alpha$ is real, nonnegative, and lies in such a field $\mathbb{Q}_n$. See pp. 532-3 in the text.

In particular, since it was observed last time that since the degree 3 of $2^{1/3}$ is not a power of 2, this number cannot lie in any such field $\mathbb{Q}_n$, so that the cube cannot be duplicated. For $\alpha = \cos \pi/9$, the triple-angle formula from trigonometry shows that $8\alpha^3 - 6\alpha - 1 = 0$, since $\cos \pi/3 = 1/2$; writing $\beta = 2\alpha$, we get that $\beta^3 - 3\beta - 1 = 0$. The polynomial $x^3 - 3x - 1$ is easily seen to have no rational roots (such roots would have to be algebraic integers and the only candidates are $\pm 1$, neither of which is a root). Thus this polynomial has no linear factors in $\mathbb{Q}[x]$, whence it is irreducible and the degrees of $\alpha$ and $\beta$ over $\mathbb{Q}$ are both 3. Thus an angle of $\pi/3$ radians cannot be trisected. Finally, it is well known that both $\pi$ and $\sqrt{\pi}$ are transcendental over $\mathbb{Q}$ (though I will not stop to prove this here), so the degree of $\sqrt{\pi}$ is infinite and the circle cannot be squared (Theorem 24, p. 533).

This is not the end of the story for geometric constructions, as another classical Greek problem asks for which $n$ a regular $n$-gon can be constructed with straightedge and compass. I am not quite ready to present the full solution to this problem; suffice it to say for now that the answer is yes for $n$ if and only if the primitive $n$th root $e^{2\pi/n}$ can be constructed (that is, its real and imaginary parts can be constructed). The degree of this element turns out to be $\phi(n)$, the Euler phi function evaluated at $n$, which counts the number of positive integers less than $n$ and relatively prime to it. If the prime factorization of $n$ is $p_1^{a_1} \dots p_m^{a_m}$, then any such integer is completely determined by its remainder modulo the prime powers $p_i^{a_i}$ for every $i$, which must be a non-multiple of $p_i$. Hence $\phi(n) = (p_1^{a^1} - p_1^{a_1-1}) \dots (p_m^{a_m} - p_m^{a_m-1})$; it is easy to check that this product is a power of 2 if and only if $n$ is a product of a power of 2 and distinct primes $p_i$, each one more than a power of 2.

In turn a number $2^m + 1$ has a chance of being prime only if $m$ is a power of 2 (since otherwise $2^m + 1$ is a sum of odd powers, which admits a standard factorization). Numbers of the form $2^{2^i} + 1$ are called *Fermat numbers*; it turns out that the first five of these (for $0 \leq i \leq 4$) are prime but there are no other known primes of this form. Eventually I will show conversely that if $n$ is the product of a power of 2 and distinct Fermat primes then the regular $n$-gon can indeed be constructed. For now I will digress a bit to give the general definition of the cyclotomic polynomial $\Phi_n$, which you will need for the first HW. This is the unique monic polynomial in $\mathbb{C}[x]$ whose roots are the exactly the primitive $n$th roots of 1 in $\mathbb{C}$. Since every $n$th root of 1 in $\mathbb{C}$ is a primitive $d$th root of 1 for some divisor $d$ of $n$, we have the factorization $x^n - 1 = \prod_{d|n} \Phi_d(x)$; assuming inductively that $\Phi_d(x)$ actually lies in $\mathbb{Z}[x]$ for all $d < n$, it follows that $\Phi_n(x) \in \mathbb{Z}[x]$. Thus the coefficients of $\Phi_n$ are actually integers.

For now I want to iterate the construction that starts with an irreducible polynomial $q$ of degree $n$ over a field $K$ and passes to the larger field $K_1 = K[x]/(q)$, in which this polynomial has a root; this is sometimes called *adjoining a root of $q$ to $K$*. Letting $\alpha$ be the root of $q$ in $K_1$, write $q(x) = (x - \alpha)q_2$ for some $q_2 \in K_1[x]$ and let $p_2$ be an irreducible factor of $q_2$. Then adjoin a root of $p_2$ to $K_1$, obtaining a larger field $K_2$ in which $q$ has at least two roots. Iterating this process, we find after finitely many steps that there is a field $K_m$ which is generated by roots of $q$ over $K$ and over which $q$ factors into linear factors. Such a field is called a splitting field for $q$ over $K$ (Definition, p. 536). The construction shows that the degree $[K_m : K] \leq n!$ (using the multiplicativity of field degrees). More generally, by further iterating the construction, one sees that any finite collection of nonconstant (but possibly reducible) polynomials $q_1, \ldots, q_m$ over a field $K$ admits a splitting field.

As an example, the splitting field of the polynomial $x^n - 1$ over $\mathbb{Q}$ is easily seen to be the subfield $\mathbb{Q}[\zeta_n]$ of $\mathbb{C}$ generated by $\mathbb{Q}$ and $\zeta_n = e^{2\pi i/n}$, since all roots of this polynomial are powers of this fixed one. This extension is called the *n*th cyclotomic extension or the *n*th cyclotomic field (p. 540).

The central goal of Galois theory is to understand roots of polynomials over fields by studying automorphisms of their splitting fields. To that end I first determine when an isomorphism from one field $F$ to another one $F'$ extends to an isomorphism from a simple finite extension of $F$ into an extension of $F'$.

## Lemma

Let $\phi : F \to F'$ be an isomorphism from the field $F$ into $F'$. Let $F(\alpha)$ be a simple algebraic extension of $F$ such that $\alpha$ has minimal polynomial $p$ in $F[x]$ and let $E'$ be an extension of $F'$. Then $\phi$ extends to an isomorphism from $F(\alpha)$ into $E'$ if and only if the polynomial $\phi(p)$ has a root in $E'$.

## Proof.

We have $F(\alpha) \cong F[x]/(p)$. Given any homomorphism $\pi$ from $F$ into a ring $R$ and an element $r \in R$ there is a unique homomorphism from the polynomial ring $F[x]$ into $R$ extending $\pi$ and sending $x$ to $r$. Replacing $F[x]$ by the quotient $F[x]/(p)$ we see that $\phi$ extends to $F(\alpha)$ if and only if $\phi(p)$ has a root in $E'$, as claimed. □

## Uniqueness of splitting fields: Theorem 27, p. 541

Leet $\phi : F \to F'$ be an isomorphism of fields and let $f$ be a nonconstant polynomial over $F$. Let $E, E'$ be splitting fields of $f$ and $\phi(f)$ over $F$ and $F'$, respectively. Then $\phi$ extends to an isomorphism from $E$ into $E'$.

**Proof.**

This follows by repeated applications of the lemma, at each step defining $\phi$ on a new root of an irreducible factor $p$ and locating a root of $\phi(p)$ in $E'$ among the roots of $\phi(f)$ there. □

As a corollary, any two splitting fields of a single polynomial $p$ or a finite collection of such over a field $F$ are isomorphic and in particular have the same degree over $F$ (Corollary 28, p. 542), since any nonzero homomorphism from one field to another necessarily has kernel 0, so that the isomorphisms from one splitting field to another are necessarily isomorphisms onto.

By iterating the splitting field construction and using Zorn's Lemma, one can show that every field $F$ admits an algebraic closure, that is, an algebraic extension $\overline{F}$ such that every nonconstant polynomial in $F[x]$ is the product of linear factors in $\overline{F}[x]$. See Proposition 30 on p. 544; the technique used in the proof will never appear again in the course, so I will omit the proof in class. I note, however, that $\overline{F}$ is algebraically closed, since given any nonconstant polynomial in $\overline{F}[x]$, the field generated by $F$ and its coefficients is a finite extension $F'$ of $F$. The minimal polynomials of the elements in a basis of $F'$ are products of linear factors in $\overline{F}[x]$, so there are no proper finite extensions of $\overline{F}$.

I close by returning to finite fields. I have already shown that the order $q$ of any such field $F_q$ must be a prime power $p^n$ and that all elements of $F_q$ are roots of the polynomial $x^q - x$, so that we can identify $F$ with the splitting field of $x^q - x$ over the prime subfield $F_p = \mathbb{Z}_p$, so that any two fields of order $q$ are isomorphic, as mentioned previously. What is not yet clear, however, is that there is a field of order $q$ for every prime power $q$; it is conceivable that the splitting field of $x^q - x$ over $F_p$ has order less than $q$. I will rule this out next time. Note finally that if $m$ divides $n$, then all roots of $x^{p^m} - x$ are also roots of $x^{p^n} - x$, so $F_{p^m}$ is a subfield of $F_{p^n}$, as mentioned last time.