Euler Circle Chapter 7: Constructability + Galois Fields

Albert Ye

May 12, 2020

Notes

§0.0.1 Construction

The ancient Greeks wondered what shapes they could/couldn't construct with just a straightedge.

Could construct segments of length $a+b$, $|a-b|$, ab, a/b, $\sqrt{a}$.

Three things they couldn't do:

- **Trisect angle.** Given *any* angle, trisect.
- **Duplicate cube.** Given some cube, find the cube with twice the area.
- **Square circle.** Given some circle, find the square that bisects it.

Ground rules: We have a segment of length 1 with endpoints $(0,0)$ and $(1,0)$. We can

- Draw a line between two constructed points
- Find the point of intersection of two non-parallel lines.
- Construct a circle with center P and radius a
- Find points of indersection between line/circle and circle/circle. (if they exist)

Here's how to multiply lengths with compass/straightedge: Take lines of length a, b. Find the point where they intersect, and take the point on one line that's one unit away from intersection. Then Just similar-triangles away.

Divide follows trivially.

Definition 0.1. We call the collection of lengths of constructible segments, as well as their negatives, the **constructable** numbers.

The constructable numbers form a field as the sum, product, quotient, and difference of constructable numbers is constructable. This field contains $\mathbb{Q}$, but also some irrationals. Note that the field of constructible numbers is contained in R. It contains, for instance, $\sqrt{2}$. Call the field of constructible numbers $\mathbb{F}$.

What does $\mathbb{F}$ contain? Note that we can consider a point $(x, y) \in \mathbb{R}^2$ to be constructible if $x, y \in \mathbb{F}$. Suppose P, Q are constructible points. The line through them has the equation $ax + by + c = 0$, where $a, b, c \in \mathbb{F}$.

Similarly, if P has a constructible point and $r \in \mathbb{F}$, then the circle centered at P with radius r can be written in the form $(x-h)^2 + (y-k)^2 = r^2$, where $h, k, r \in \mathbb{F}$. The only way to generate *new* points is by intersecting lines and circles.

- **Intersection of lines.** If $a, b, c, d, e, f \in \mathbb{F}$, then any intsersection of the lines $ax + by + c = 0$ and $dx + ey + f = 0$ also has coordinates in $\mathbb{F}$.

- **Intersection of line and circle.** If $a, b, c, h, k, r \in \mathbb{F}$, then any intersection of the line and the circle lies in a quadratic extension of $\mathbb{F}$, or an extension of the form $\mathbb{F}(\sqrt{x})$ for some positive $x \in \mathbb{F}$.

- Intersection twocircles: If $h_1, k_1, r_1, h_2, k_2, r_2 \in \mathbb{F}$, then any intersection of the circles $(x - h_1)^2 + (y - k_1)^2 = r_1^2$ and $(x - h_2)^2 + (y - k_2)^2 = r_2^2$ lies in a quadratic extension of $\mathbb{F}$.

Thus we see that any individual step in the construction at most increases the degree of the field of numbers thus far constructed by a factor of 2. Thus any field of constructible numbers must have degree 2^n for some n. On the other hand, an subfield of $\mathbb{R}$ that can be obtained by successively adjoining sqrts of positive elements is a field of constructible numbers, because we know how to take square roots. Thus, we have

Theorem 0.2

A number $\alpha \in \mathbb{R}$ is constructible iff there is a sequence of fields $F_0 = \mathbb{Q} \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$.

§0.0.2 Solving the Greek Problems

Problem 0.3 (Trisecting the angle)**.** Prove that most angles can't be trisected.

Solution 0.4. We claim we *cannot* trisect a $\frac{\pi}{3}$ angle. Suppose we can construct $\theta = \pi/9$ using a compass and straightedge, which we assume is measured wrt the positive x-axis. We can find a point of distance 1 from the origin and angle θ, i.e. $(\cos\theta, \sin\theta)$. Thus $\cos\theta$ must be constructible. Apply the triple-angle identity for cos:

$$\cos 3\theta = 1 - \cos^3\theta - 3\cos\theta.$$

Letting $\theta = \frac{\pi}{9}$, we have $\cos 3\theta = \frac{1}{2}$. Hence $\cos\theta$ is a root of the cubic polynomial $4x^3 - 3x - \frac{1}{2}$ or $8x^3 - 6x - 1$. Let $y = 2x$, so we have $y^3 - 3y - 1 = 0$. This polynomial is irreducible. Therefore, $[\mathbb{Q}(2\cos\frac{\pi}{9} : Q] = 3$, and so $[\mathbb{Q}(\cos\frac{\pi}{9} : \mathbb{Q}] = 3$. Thus, by the Tower Law, $\cos\frac{\pi}{9}$ cannot lie in any constructible field, for its degree is not a power of 2. Thus, we can't construct a $\frac{\pi}{9}$ angle.

Problem 0.5 (Doubling the cube)**.** Prove that we cannot construct a cube with side length $\sqrt[3]{2}$.

Solution 0.6. We wish to construct of segment of length $a = \sqrt[3]{2}$. a is a root of $x^3 - 2 = 0$, which is irreducible by Eisenstein. Hence, $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, so a can't be constructed.

Problem 0.7 (Squaring the circle)**.** Prove that we can't construct a square with the same area as a given circle.

Solution 0.8. We take it as given that π is transcendental, so $\sqrt{\pi}$ is also transcendental. A circle with radius 1 has area π, so if we have a square of the same area, it must have sidelength $\sqrt{\pi}$. Since $\sqrt{\pi}$ is transcendental, it can't be constructed.

§0.0.3 Splitting Fields

Let F be a field and $f(x)$ an irreducible polynomial with coefficients in F. Adjoining one or all roots my yield different fields.

Definition 0.9. Let F be a field and f a nonzero polynomial with coefficients in F. We say that an extension L/F is a **splitting field** for f if all the roots of f lie in L, but not in any smaller extension of F.

Equivalently, the splitting field of f is the field obtained by adjoining all roots of f to F.

Example 0.10
- If $a \in Q$ is not a perfect square, then the splitting field of $x^2 - a$ is $\mathbb{Q}(\sqrt{a})$, since the other root $-\sqrt{a}$ is already in this field. Its degree is 2.
- The splitting field of the polynomials x^2+1 and x^2-2 is $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$. It has degree 4 over $\mathbb{Q}$, and it contains three quadratic subfields: $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$. This is an example of a biquadratic field. This is also the splitting field of $(x^2+1)(x^2-2)$.
- The splitting field of the polynomial $x^3 - 2$ over $\mathbb{Q}$ is the field $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}$.

Let p be a prime, and consider the splitting field L of $f(x) = x^p - 2$. f is irreducibleby Eisenstein with $p = 2$. Its roots are $\sqrt[p]{2}\zeta_p^k$ for $0 \le k \le p-1$ and $\zeta_p = e^{2\pi i/p}$. Thus $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_p)$. We have

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[p]{2})] \cdots [(\mathbb{Q}(\sqrt[p]{2} : \mathbb{Q}],$$

which is a multiple of p. On the other hand,

$$[L : Q] = [L : \mathbb{Q}(\zeta_p)] \cdot [\mathbb{Q}(\zeta_p) : \mathbb{Q}].$$

Now we have to compute $[\mathbb{Q}(\zeta_p : \mathbb{Q}]$. Note that ζ_p is a root of $x^p - 1$ but isn't 1, so it's a root of $x^{p-1} + x^{p-2} + \cdots + x + 1 = \Phi_p(x)$. Exercise: check that $\Phi_p(x)$ is irreducible. Thus $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Thus $[L : \mathbb{Q}]$ is a multiple of $p-1$, and so $[L : \mathbb{Q}]$ is a multiple of $p(p-1)$.

Suppose K/F is a field extension and α is algebraic over F. How do we compare $F(\alpha) : F]$ to $[K(\alpha) : K]$? Since $[F(\alpha) : F]$ is the degree of the minimal polynomial of α over F and $[K(\alpha) : K]$ is the degree of the minimal polynomial over K, we must have $[K(\alpha) : K] \le [F(\alpha) : F]$.

Now, we have $[L : \mathbb{Q}(\zeta_p)] \le [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}]$. Thus we have $[L : \mathbb{Q} \le p(p-1)$, so it's equal.

§0.0.4 Algebraic Closures

Definition 0.11. A field F is said to be **algebraically closed** if all irreducible polynomials over F have degree 1.

For example, $\mathbb{C}$ is algebraically closed, and $\overline{\mathbb{Q}}$ (Q-bar) is too. Q-bar is equivalent to the set of algebraic numbers.

§0.0.5 Field Automorphisms and fixed fields

(K) is the set of automorphisms of K. In fact, it's a group. Suppose K is a field and $\sigma \in (K)$. Then there are some $x \in K$ s.t. $\sigma(x) = x$. These elements are said to be **fixed** by σ.

Proposition 0.12

If $\sigma \in (K)$, then the set of elements of K fixed by σ forms a field.

Proof. Since σ is a homomorphism, $\sigma(0) = 0$ and $\sigma(1) = 1$, so $0, 1$ are fixed. Suppose a, b are fixed. Then

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$$
$$\sigma(ab) = \sigma(a)\sigma(b) = ab$$
$$\sigma(-a) = -\sigma(a) = -a$$
$$\sigma(a^{-1} = \sigma(a)^{-1} = a^{-1}.$$

Thus, the set of fixed is closed, so it is a field. □

Proposition 0.13

- If $L/K/F$ is a tower of field extensions, then $(L/K) \leq (L/f)$.
- If $H_1 \leq H_2 \leq (K)$, then $K^{H_1} \subset K^{H_2}$.

Proposition 0.14

Let K/F be a field extension. Let $\sigma \in (K/F)$, let $\alpha \in K$ be algebraic over F, and let $f(x)$ be the minimal polynomial for α over F. Then $\sigma(\alpha)$ is a root of $f(x)$.

Proof. Suppose $f(x) = x^n - a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then, we have

$$\begin{aligned}
0 &= \sigma(f(\alpha)) \\
&= \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \\
&= \sigma(\alpha)^n + \cdots + \sigma(a_1\alpha) + \sigma(a_0) \\
&= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 \\
&= f(\sigma(\alpha)).
\end{aligned}$$

Thus, $\sigma(\alpha)$ is a root of f. □

Note also that an automorphism is entirely specified by its behavior on a generating set of the field. If $K = F(\alpha)$, for instance, then $\sigma \in (K/F)$ is entirely determined by the value of $\sigma(\alpha)$.

Proposition 0.15

Let α be algebraic over F, and let $K = F(\alpha)$. Then $|(K/F)| \leq [K : F]$.

In general, Proposition 5.4 is supposed to be equality in good cases. It isn't in the case of $\mathbb{Q}(\sqrt[3]{2})$ because the other things aren't automorphisms, but only isomorphisms between different fields. This is because $\mathbb{Q}(\sqrt[3]{2})$ isn't a splitting field. If K is the splitting field of $f(x)$ over F, then $(K/F) = [K : F]$.

There's one more thing that can go wrong, which is that the minimal polynomial f of α could have a double root, i.e there is some $\alpha \in K$ s.t. $(x-a)^2 | f(x)$. In this case, if $f(x)$ is irreducible, $[F(\alpha) : F] = \deg(f)$, but there aren't enough roots of f to have $\deg(f)$ automorphisms.

This doesn't happen in fields we're familiar with like finite extensions of $\mathbb{Q}$. To see this, look at $f'(x)$, the derivative of f. If $(x-a)^2$ is a factor of $f(x)$, then $x-a$ is a factor of $f'(x)$, and $\deg(f') = \deg(f) - 1$. Also, if the coefficients of f lie in F, then so do the coefficients of f'. Thus, a polynomial with multiple roots cannot be a minimal polynomial.

However, this can happen in other fields in $\mathbb{F}_p(t)$. We can still take derivatives here, and the derivative has pretty much the same properties as it does over $\mathbb{Q}$ or $\mathbb{R}$, but with one subtle point: the derivative could be 0. For example, the polynomial $x^p - i$ over $\mathbb{F}_p(t)$ is the minimal polynomial of $\sqrt[p]{t}$, and it has only one root because $x^p - t = (x - \sqrt[p]{t})^p$ in $\mathbb{F}_p(t)$. Note that the derivative of $x^p - t$ is 0.

Definition 0.16. An algebraic field extension K/F is said to be **separable** if, for any $\alpha \in K$, the minimal polynomial of α has all distinct roots.

§0.0.6 Galois extensions/groups

Galois extensions: nicest extensions, right number of automorphisms.

Definition 0.17. An algebraic extension K/F is said to be **Galois** if $K^{(K/F)} = F$.

Theorem 0.18

The following are equivalent for an algebraic extension K/F:

1. K/F Galois
2. K/F is normal and separable.
3. $|(K/F)| = [K : F]$

Definition 0.19. If K/F is Galois, we write (K/F) instead of (K/F). We call (K/F) the **Galois group** of K/F.