GALOIS THEORY : LECTURE 12

LEO GOLDMAKHER

Last lecture, we asserted that the following four constructions are impossible given only a straightedge and a compass:

(1) *Doubling the cube*, i.e. constructing a cube with twice the volume of a given cube
(2) *Trisecting the angle*
(3) *Squaring the circle*, i.e. constructing a square of area equal to the area of a given circle
(4) *Constructing a regular heptagon*

In this lecture, we will prove the impossibility of constructions 1, 2, and 4 and discuss the impossibility of 3. These proofs are all due to a 23-year-old Frenchman named Pierre Wantzel (all proofs appeared in an 1837 paper).

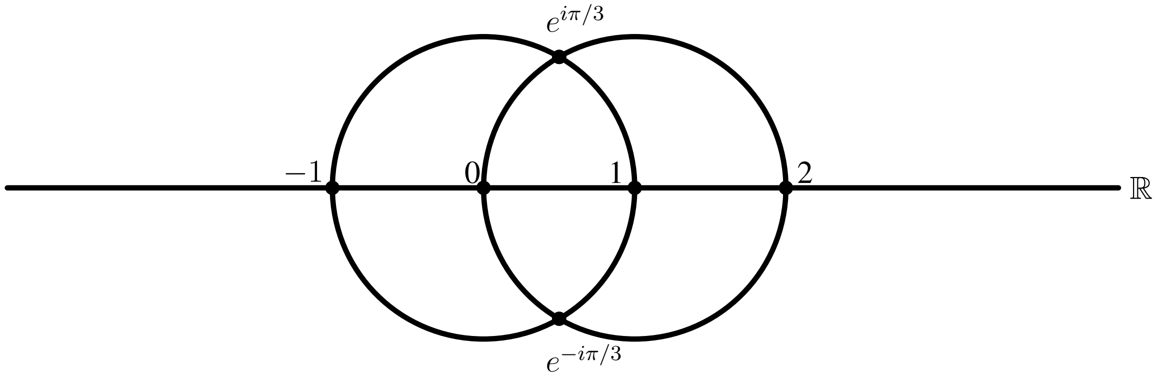
1. Formalizing constructibility

In order to understand Wantzel's proofs, we need to connect field theory to the notions of constructibility from last lecture. First, we consider what it means for a point to be constructible given our geometric tools. We'll focus on constructing points in $\mathbb{C}$ starting with just two given points in $\mathbb{C}$: 0 and 1.

Given just the two points 0 and 1, we can

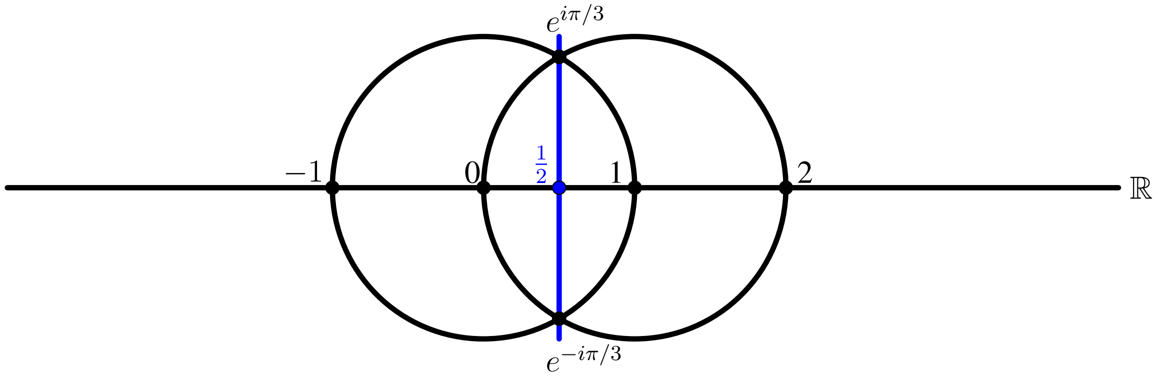
- use our straightedge to draw the horizontal axis (i.e. $\mathbb{R}$)
- use our compass to draw a circle centered at 0 and passing through 1
- use our compass to draw a circle centered at 1 and passing through 0

Examining the points of intersection, we see that we've constructed four new points: 2, -1, and $\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$. (Recall that $\frac{1}{2} \pm \frac{\sqrt{-3}}{2} = e^{\pm i\pi/3}$.)



Now we have six points and can continue the process, drawing all possible lines and circles defined by these six points and then forming new intersection points. For example we can construct $\frac{1}{2}$ by drawing a line connecting $e^{i\pi/3}$ and $e^{-i\pi/3}$:

Date: March 12, 2018.
Based on notes by Franny Dean.



This led us to give a rigorous definition of what it means to construct points from a given set of points:

Definition 1.1. Given a set $S \subseteq \mathbb{C}$, we say an element $z \in \mathbb{C}$ is ***constructible in one step*** from S if and only if there exist points $x, y, a, b \in S$ such that

(1) $z \in \overline{xy} \cap \overline{ab}$,
(2) $z \in \overline{xy} \cap C_a(b)$, or
(3) $z \in C_x(y) \cap C_a(b)$.

Here $C_a(b)$ denotes the circle centered at a through point b.

With this formal definition in hand, we start with the set of points $\{0, 1\}$ and construct new points iteratively:

Definition 1.2. We say $z \in \mathbb{C}$ is ***constructible*** if and only if there exists a finite sequence of points $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n$ with $\alpha_n = z$ such that

α_1 is constructible in one step from $\{0, 1\}$
α_2 is constructible in one step from $\{0, 1, \alpha_1\}$
α_3 is constructible in one step from $\{0, 1, \alpha_1, \alpha_2\}$
$\vdots$
$\alpha_n = z$ is constructible in one step from $\{0, 1, \alpha_1, \ldots, \alpha_{n-1}\}$

Daishiro pointed out that we constructed $1/2$ at the second step of our iteration, whereas according to the above definition it would take three steps to do so. Thus, one might wish to instead use the following definition:

Definition 1.3. Let $S_0 := \{0, 1\}$, $S_1 := \{z \in \mathbb{C}$ constructible in one step from $S_0\}$, and

$$S_k := \{z \in \mathbb{C} \text{ constructible in one step from } S_0 \cup S_1 \cup \cdots \cup S_{k-1}\}.$$

(Colloquially, S_k is the set of all points constructible in at most k steps from $\{0, 1\}$.) We say $z \in \mathbb{C}$ is ***constructible*** if and only if there exists $k \in \mathbb{N}$ such that $z \in S_k$.

In practice it doesn't matter which of these definitions we follow, since we are only interested in whether the number of steps to construct an element is finite, not the minimum number of steps it would take. In this document, we'll use the latter.

2. Connection to Field Theory

Having formalized constructibility, we now connect constructible numbers to field theory.

Proposition 2.1. *If α, β are constructible, then so are $\alpha \pm \beta, \alpha\beta$, and $\frac{\alpha}{\beta}$ (assuming $\beta \neq 0$).*

Thus, the set of all constructible numbers is a field! We will not prove this proposition, but we encountered all the necessary ingredients for the proof last time: from 0 and 1 we constructed $2 = 1 + 1$ and $-1 = 0 - 1$, and we also used similar triangles to construct $1/3$ from 1 and 3. We can also use similar triangles to construct $\alpha\beta$ given α and β.

Note that the set of all constructible numbers is an intermediate field between $\mathbb{Q}$ and $\mathbb{C}$. How does it relate to the two fields? Wantzel's key insight was the following:

Theorem 2.2. *If β is constructible, then $[\mathbb{Q}(\beta):\mathbb{Q}] = 2^k$ for some $k \in \mathbb{Z}$.*

Remark. The converse turns out to be false; for example, there exists β of degree 4 over $\mathbb{Q}$ which isn't constructible. (You will prove this later this semester.)

Before proving this theorem, we demonstrate its power by using it to prove the impossibility of the four challenging constructions listed at the start of this lecture.

3. Impossibility proofs

Corollary 3.1. *We cannot double the cube.*

Proof. We will show we cannot double a unit cube. To do so would require us to construct $\sqrt[3]{2}$. But the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is x^3-2, whence $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$. Theorem 2.2 implies that $\sqrt[3]{2}$ is not constructible, from which we conclude that we cannot double the cube. □

Corollary 3.2. *We cannot construct a regular heptagon.*

Proof. Observe that constructing a regular heptagon is equivalent (by Proposition 2.1) to constructing the seventh roots of unity. In particular, if we can construct the regular heptagon then we can construct $\zeta_7 := e^{2\pi i/7}$.

Note that ζ_7 satisfies $x^7 - 1 = 0$. This polynomial is reducible, since it has 1 as a root:

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Thus ζ_7 is a root of $x^6 + x^5 + \cdots + x + 1$. By problem **5.1**(e) we know that this is irreducible over $\mathbb{Q}$, whence it must be the minimal polynomial of ζ_7 over $\mathbb{Q}$. This yields $[\mathbb{Q}(\zeta_7):\mathbb{Q}] = 6$, and Theorem 2.2 implies that we cannot construct ζ_7. Thus, the regular heptagon is not constructible. □

Andrew observed that one can adapt the proof to show the impossibility of constructing the regular p-gon for any prime p of the form $p \neq 2^k + 1$. It turns out that more is true. To describe this, we first label such primes:

Definition 3.3. Primes which are one more than a power of two are called ***Fermat Primes***.

Gauss proved that for any distinct Fermat primes $p_1, \ldots, p_n$ and any $k \in \mathbb{N}$ it is *possible* to construct a regular $2^k p_1 p_2 \cdots p_n$-gon. Wantzel completed the story by proving the converse: it is impossible to construct a regular n-gon for any n which isn't a product of a power of two and distinct Fermat primes.

This result naturally leads to some questions about Fermat primes. Are there infinitely many of them? Does their definition force them to satisfy any other interesting properties? A result you will prove on your next assignment is:

Proposition 3.4. *A prime p is a Fermat prime if and only if $p = 2^{2^k} + 1$ for some $k \in \mathbb{Z}$.*

Example 3.5. Thus, plugging in $k = 0, 1, \ldots, 4$ we see that the first few Fermat primes are $3, 5, 17, 257, 65537$. It turns out that these are also the *only* known Fermat primes! In particular, it is a major open question whether or not there exist infinitely many Fermat primes.

The last impossibility proof hinged on proving the impossibility of constructing a certain angle, or equivalently, of constructing a certain root of unity. The same idea is also at the heart of the next result.

Corollary 3.6. *There is no construction which trisects a given angle.*

Proof. Let ℓ denote line segment in $\mathbb{C}$ connecting 0 to 1. We will prove the impossibility of constructing the $20°$ angle whose base is ℓ. Since a $60°$ angle whose base is ℓ *is* constructible, this proves that no construction exists which trisects an arbitrary given angle. Note that there do exist angles we *can* trisect, e.g. a right angle.

We proceed by contradiction. If we could construct the $20°$ angle with base ℓ, then we would be able to construct the 18th-root of unity $\zeta_{18} := e^{i\pi/9}$. Since the constructible numbers form a field, we would also be able to construct its complex conjugate $\overline{\zeta_{18}}$. All this would imply that the real number $\zeta_{18} + \overline{\zeta_{18}}$ is also constructible. We now prove that this is not the case by showing that $\zeta_{18} + \overline{\zeta_{18}}$ has degree 3 over $\mathbb{Q}$.

Observe that

$$\begin{aligned}(\zeta_{18}+\overline{\zeta_{18}})^3 &= \zeta_{18}^3 + 3\zeta_{18}\overline{\zeta_{18}}(\zeta_{18}+\overline{\zeta_{18}}) + \overline{\zeta_{18}}^3 \\ &= e^{i\pi/3} + e^{-i\pi/3} + 3(\zeta_{18}+\overline{\zeta_{18}}) \\ &= 1 + 3(\zeta_{18}+\overline{\zeta_{18}}).\end{aligned}$$

This implies that $\zeta_{18}+\overline{\zeta_{18}}$ is a root of the polynomial x^3-3x-1, which (by the rational root test) is irreducible over $\mathbb{Q}$ and therefore is the minimal polynomial of $\zeta_{18}+\overline{\zeta_{18}}$ over $\mathbb{Q}$. It follows that $[\mathbb{Q}(\zeta_{18}+\overline{\zeta_{18}}):\mathbb{Q}]=3$. Theorem 2.2 immediately implies that $\zeta_{18}+\overline{\zeta_{18}}$ isn't constructible. □

Remark. Grace observed the following nice corollary: one cannot construct a 4° angle, since then one would be able to construct a 20° angle. (More generally, this shows that one cannot construct a $d°$ angle for any $d \mid 20$.) It turns out that it is possible to construct a 3° angle, however.

Corollary 3.7. *We cannot square the circle.*

We didn't prove this in lecture, because the proof relies on knowing the transcendence of π over $\mathbb{Q}$ (a fact whose proof appears in the book but that we won't cover in class). Assuming this fact, however, the proof isn't terribly hard.

Proof. The area of a unit circle is π, so to construct a square of the same area amounts to constructing a side of length $\sqrt{\pi}$. If this were constructible, then π would be as well. But since π is transcendental over $\mathbb{Q}$, we have $[\mathbb{Q}(\pi):\mathbb{Q}]=\infty$, and we conclude by Theorem 2.2. □

4. Proof of Theorem 2.2

We prove Theorem 2.2 in three stages.

Claim 1: Given $S \subseteq \mathbb{C}$. If z is constructible in one step from S, then $[\mathbb{Q}(S,z):\mathbb{Q}(S)] \le 2$.

Claim 2: Let S_k denote the set of all numbers which are constructible from $\{0,1\}$ in at most k steps (see Definition 1.3). Then $[\mathbb{Q}(S_k):\mathbb{Q}]=2^m$ for some $m \in \mathbb{Z}$.

Claim 3: If $\beta \in \mathbb{C}$ is constructible, then $[\mathbb{Q}(\beta):\mathbb{Q}]=2^n$ for some $n \in \mathbb{Z}$.

Proof of Claim 1. We first recall what it means for a point z to be constructible in one step from a set S. Let's say that a line is constructible from S iff it passes through two points of S, and that a circle is definable from S iff it's centered at one point of S and passes through another. In this language, z is constructible in one step from S iff it lies in the intersection of two lines, two circles, or a circle and a line which are constructible from S. We now prove a statement which is somewhat stronger than the claim in the claim: that any z constructible in one step from $\mathbb{Q}(S)$ has degree 1 or 2 over $\mathbb{Q}(S)$.

- If z is the intersection of 2 lines constructible from $\mathbb{Q}(S)$, then z is the solution to a system of two linear equations whose coefficients lie in $\mathbb{Q}(S)$. This implies that $z \in \mathbb{Q}(S)$, whence $[\mathbb{Q}(S,z):\mathbb{Q}(S)]=1$.
- If z is the intersection of a line and a circle constructible from $\mathbb{Q}(S)$ then it is the solution to a system consisting of a linear equation and a quadratic equation, both with coefficients in $\mathbb{Q}(S)$. In particular, the linear equation shows that $x := \operatorname{Re} z$ and $y := \operatorname{Im} z$ are related to each other by a factor from $\mathbb{Q}(S)$. Using the linear equation to express y in terms of x and substituting this into the quadratic yields a quadratic equation in the single variable x with coefficients in $\mathbb{Q}(S)$. It follows that minimal polynomial of x over $\mathbb{Q}(S)$ has degree at most 2, whence $[\mathbb{Q}(S,z):\mathbb{Q}(S)] \le 2$ in this case.
- If z is the intersection of two circles constructible from $\mathbb{Q}(S)$, we obtain two quadratic equations of the form $(x-a)^2+(y-b)^2=r^2$ (with $a,b,r^2 \in \mathbb{Q}(S)$ and $x=\operatorname{Re} z$, $y=\operatorname{Im} z$). Subtracting one of these from the other produces a linear relation between x and y with coefficients in $\mathbb{Q}(S)$. Now we proceed as in the previous case to conclude that $[\mathbb{Q}(S,z):\mathbb{Q}(S)] \le 2$. (Note that we're pretty lucky here: usually the intersection of two quadratics yields the solution to a quartic equation, not just a quadratic one!)

(The proof of this is carried out more explicitly in the textbook.) □

Proof of Claim 2. We prove this by induction. Given any $\alpha \in S_k$, it must be constructible in one step from S_{k-1}. Thus Claim 1 implies that $[\mathbb{Q}(S_{k-1}, \alpha) : \mathbb{Q}(S_{k-1})] = 1$ or 2. Since any element $\beta \in S_k$ is constructible in one step from S_{k-1}, we see that β is constructible in at most one step from $S_{k-1} \cup \{\alpha\}$, whence Claim 1 gives $[\mathbb{Q}(S_{k-1}, \alpha, \beta) : \mathbb{Q}(S_{k-1}, \alpha)] = 1$ or 2. Adjoining all the elements of S_k one at a time in this way, we obtain a tower of field extensions:

$$\begin{tikzcd}
\vdots \\
\mathbb{Q}(S_{k-1}, \alpha, \beta) \arrow[u, dash, "1 \text{ or } 2"] \\
\mathbb{Q}(S_{k-1}, \alpha) \arrow[u, dash, "1 \text{ or } 2"] \\
\mathbb{Q}(S_{k-1}) \arrow[u, dash, "1 \text{ or } 2"]
\end{tikzcd}$$

Since S_k is a finite set, this tower terminates. The Tower Law then implies $[\mathbb{Q}(S_k) : \mathbb{Q}(S_{k-1})] = 2^j$ for some $j \in \mathbb{N}$. By induction we may assume that $[\mathbb{Q}(S_{k-1}) : \mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$, whence (employing the Tower Law once again) we see that

$$[\mathbb{Q}(S_k) : \mathbb{Q}] = [\mathbb{Q}(S_k) : \mathbb{Q}(S_{k-1})][\mathbb{Q}(S_{k-1}) : \mathbb{Q}] = 2^{j+m}.$$

This concludes the proof. □

Proof of Claim 3. Given any constructible $\beta \in \mathbb{C}$, there exists k such that $\beta \in S_k$. In particular we have a tower of extensions

$$\begin{tikzcd}
\mathbb{Q}(S_k) \\
\mathbb{Q}(\beta) \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash, "d"]
\end{tikzcd}$$

with $d := [\mathbb{Q}(\beta) : \mathbb{Q}]$. By Claim 2 we know that $[\mathbb{Q}(S_k) : \mathbb{Q}] = 2^m$ for some $m \in \mathbb{N}$. Tower Law then implies that $d \mid 2^m$, whence d must be a power of 2. □