Lecture 13: Constructible Numbers

Rules: 
A) Given two points, can draw the line joining them and the circle centered at one pt and passing through the other.

B) Can find pts of intersection between drawn lines and circles.

[Given midpts of segments, perpendicular bisectors, parallel lines.]

\[ C = \{ z \in \mathbb{C} \mid z \text{ can be constructed from } 0, 1 \text{ by the above operations} \} \]

\( C \) is a field, closed under \(|z|, \Re(z), \Im(z), \overline{z}\).

ThmA: If \( z \in C \), then \([\mathbb{Q}(z) : \mathbb{Q}] = 2^n\). In particular, \( C/\mathbb{Q} \) is algebraic.

Cor: Can't construct a reg. 7-gon.

Cor: Can't trisect angles

Cor: Can't square a circle.

[Today, will prove above theorem, as well as]

ThmB: \( C \) is the smallest subfield of \( \mathbb{C} \) which is closed under taking square roots.
Theorem 1: \( z \in \mathbb{C} \) is constructible iff there exist fields 
\[ Q = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \subseteq \mathbb{C} \] 
with \( z \in K_n \) and each 
\[ [K_{k+1} : K_k] = 2. \]

Note this gives Theorem 1 as 
\[ 2^n = [K_n : Q] = [K_n : Q(z)][Q(z) : Q]. \]

Lemma 1: \( \mathbb{C} \) is closed under \( z \mapsto \sqrt{z} \)

Proof: First, any \( r \geq 1 \) in \( \mathbb{C} \cap \mathbb{R} \) has a square root as follows.

Set \( s = \frac{r+1}{2} \) and consider 
\[ z = (s-1) + yi \]
and note \( x^2 + y^2 = s^2 \)
gives 
\[ y = \sqrt{s^2 - (s-1)^2} = \sqrt{2s-1} = \sqrt{r}. \]
As \( z \in \mathbb{C} \), have 
\( \text{Im}(z) = \sqrt{r} \in \mathbb{C} \) as well. Next, any \( 0 < r < 1 \) has \( \sqrt{r} \in \mathbb{C} \) as \( \frac{1}{\sqrt{r}} \in \mathbb{C} \). For the general \( z = re^{i\theta} \in \mathbb{C} \), have 
\( r = |z| \in \mathbb{C} \Rightarrow e^{i\theta} \in \mathbb{C} \). Since \( \sqrt{z} = \sqrt{r}e^{i\theta/2} \), it remains to prove \( e^{i\theta/2} \in \mathbb{C} \).

Lemma 2: Suppose \( F \subseteq K \subseteq \mathbb{C} \). If \( [K : F] = 2 \), then 
\[ K = F(\sqrt{z}) \] 
for some \( z \in F \).

Proof: Pick \( \alpha \in K \setminus F \). Then \( K = F(\alpha) \) and 
\[ M_{\alpha, F}(x) = x^2 + bx + c \] 
for \( b, c \in F \). By quadratic formula, have 
\[ K = F(\sqrt{b^2 - 4c}) \] 
since \( \alpha = (1 \pm \sqrt{b^2 - 4c})/2 \).
Explain why these lemmas give half of Thms B and C.

Outline the moral.

Set $P_i = \{0, 1, i, -i\}$ and $P_n = \{\text{all } z \in \mathbb{C} \text{ constructible in one step from pts in } P_{n-1}\}$

Define $F_n = \mathbb{Q}(P_n) \subseteq \mathbb{C}$. finite set

Note $UF_n = \mathbb{C}$. By symmetry of $P_i$, have $F_n$ closed under $z \mapsto \overline{z}$.

Lemma 3: For all $z \in P_n$, have $[F_n(z) : F_n] = 1$ or 2.

Proof of Thm C: ($\Leftarrow$) Clear from Lemmas 1 and 2

($\Rightarrow$) Since $UF_n = \mathbb{C}$, it suffices to show $[F_n : \mathbb{Q}]$ has such a tower of subfields.

Fix $k$, and number $z_1, z_2, ..., z_m$ in $P_{k+1}$. Consider

$$F_k \subseteq F_k(z_1) \subseteq F_k(z_1, z_2) \subseteq ... \subseteq F_k(z_1, ..., z_m) = F_{k+1}$$

Since each $z_i$ sat a poly of deg $\leq 2$ in $F_k[x]$ by

Lemma 3, have $[F_k(z_1, ..., z_i) : F_k(z_1, ..., z_{i-1})] = 1$ or 2

Removing duplicates gives the desired tower of subfields. □
**Proof of Thm B:** Let $K =$ smallest subfield of $\mathbb{C}$ that is closed under $\sqrt{}$. By Lemma 1, $K \subseteq \mathbb{C}$.

Conversely, any $z \in \mathbb{C}$ lives in a tower of subfields as given by Thm C. By Lemma 2, these are obtained by adding $\sqrt{}$'s, so $\mathbb{C} \subseteq K$. So $K = \mathbb{C}$. \qed

**Proof of Lemma 3:**

**Case 1:** $z \in \mathbb{P}_n$ is the intersection of two lines defined by $a, b, c, d$ in $\mathbb{P}_{n-1}$, as shown.

Set $K = F_n(z)$. Note that $K$ is unchanged if we translate the whole picture by some $u \in F_n$.

The same is true if we multiply the whole picture by $v \in F_n$.

Thus can assume that $c = 0$ and $d = 1$. 

\[ a = x_a + iy_a \]
\[ b = x_b + iy_b \]
As $F_n$ is closed under $w \mapsto \overline{w}$, it is also closed under $w \mapsto \text{Re}(w) = \frac{1}{2}(w + \overline{w})$ and $w \mapsto \text{Im}(w) = \frac{1}{2i}(w - \overline{w})$.

So $F_n = x_a, y_a, x_b, y_b$. The line $L$ has eqn

$$(y_b - y_a)(x - x_a) = (x_b - x_a)(y - y_a)$$

and hence setting $y = 0$ and solving for $x$ shows that $z \in F_n$. So $K = F_n$.

**Case 2:** $z \in P_n$ is the intersection of a line and a circle.

As before, assume $c = 0$ and $d = 1$. We seek the common solutions to $x^2 + y^2 = 1$ and $y = mx + b$ for $m, b \in F_n$. Let $(x, y)$ be the solution corresponding to $z$.

Note $(1 + m^2)x^2 + 2mbx + b^2 - 1 = 0$, so $[F_n(x) : F_n] \leq 2$.

As $i \in F_n$, have $F_n(z) \subseteq F_n(x) = F_n(x, y)$ and so $[F_n(z) : F_n] \leq 2$. 
Case 2 is the intersection of two circles

Can assume \( a = 0 \) and \( c = 1 \).

So consider

\[
X^2 + Y^2 = 161^2 = \overline{b \overline{b}} = R_1
\]

\[
(X - 1)^2 + Y^2 = 16 - 11^2 = R_2
\]

both in \( F_n \)

Subtract to get \( 2x - 1 = R_1 - R_2 \implies x \in F_n \)

and \( F_n(z) = F_n(Y) = F_n(\sqrt{R_1 - ((R_1 - R_2) + 1)/2}) \)

So \( [F_n(z) : F_n] \leq 2 \).

[Causs-Wantzel 1830s] A regular \( n \)-gon is constructible

if and only if \( n = 2^k p_1 \ldots p_t \) where \( k \geq 0 \) and the

\( p_i \) are distinct primes of the form \( 2^2 + 1 \).

Only 5 such Fermat primes are known: 3, 5, 17, 257, 65537.