Lecture 8: Ruler-Compass Constructions

Aim Lecture: Recall how intermediate fields arise in constructibility.

Radical Ext$^{\underline{n}}$s

Def$^{\underline{n}}$ 1: Consider a tower of field ext$^{\underline{n}}$s

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n = K \dots \text{ⓧ}$$

The tower is

ⓐ radical if each $F_{i+1} = F_i(\sqrt[m_i]{\alpha_i})$ for some $\alpha_i \in F_i$ in which case we say K/F is radical

ⓑ quadratic if $[F_{i+1} : F_i] = 2$.

E.g. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{5 - \sqrt{3}})$ is quadratic & radical.

Rem.: ⓐ If $m_i = r\,s$ above then can refine $F_i \subset F_{i+1}$ to

$$F_i \subset F_i(\underbrace{\sqrt[s]{\alpha_i}}_{\beta}) \subset (F_i(\beta))(\sqrt[r]{\beta})$$

By induction can refine ⓧ so all m_i are prime.

ⓑ If char $F \neq 2$ & there is a quadratic tower from F to K, then K/F is radical with $[K:F] = 2^n$, $n \in \mathbb{N}$.

Proof:

Consider tower ⊗ with $[F_{i+1}:F_i]=2$. Let $\alpha \in F_{i+1}-F_i$ so its min. poly $p(x)$ $/F_i$ is quadratic with discriminant $\delta \in F_i$. Quadratic formula $\Rightarrow$

$$F_{i+1} = F_i(\sqrt{\delta}).$$ $\square$

Constructibility

Recall

Def^n 2: $z \in \mathbb{C}$ is constructible if it lies in some set $P_i \subset \mathbb{C}$ which can be constructed recursively below (together with a set LC_i of lines & circles in $\mathbb{C}$).

$\boxed{\text{Step 0}}$ $P_0 = \{0, 1\}$, $LC_0 = \emptyset$

$\boxed{\text{Step 1}}$ $LC_{i+1} = LC_i \cup$ either

(a) a line L through 2 pts of P_i

OR (b) a circle C centre in P_i & radius equal to dist. between 2pts of P_i.

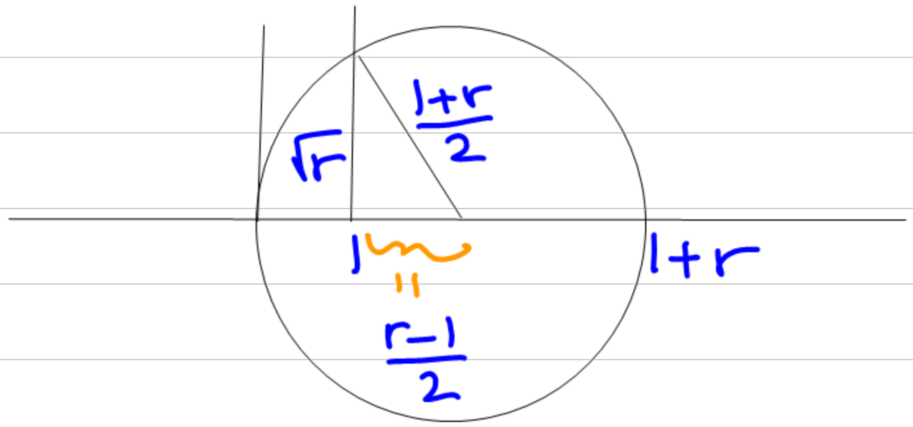
$\boxed{\text{Step 2}}$ $P_{i+1} = P_i \cup$ intersection pts of L or C above with all other lines & circles in LC_i

$\boxed{\text{Step 3}}$ Repeat.

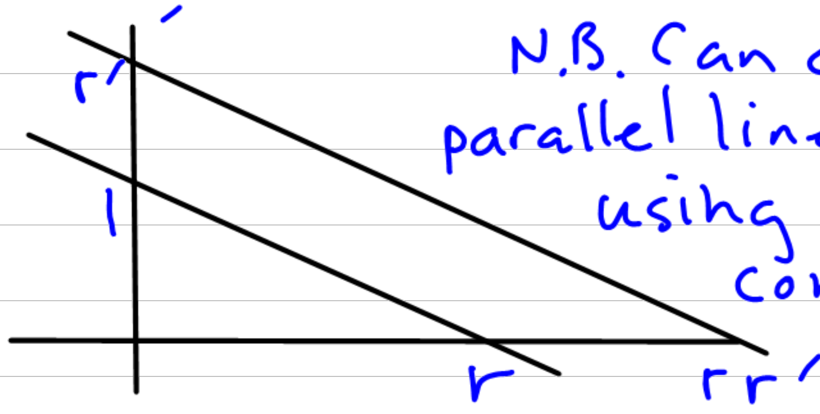
<u>Thm</u>: $z \in \mathbb{C}$ is constructible iff there's a quadratic tower from $\mathbb{Q}$ to a field K containing z.

Sketch Proof ($\Leftarrow$) only: Suffice show set P of constructible numbers is closed under $+, -, \times, \div$ & $\sqrt{\ }$.

e.g. closure under $\sqrt{\ }$: let $z = re^{i\theta} \in P$. We can halve θ $\because$ you can bisect angles using ruler & compass.
Also $\sqrt{r} \in P$ $\because$



To see $r, r' \in P \cap \mathbb{R} \Rightarrow rr' \in P$ use



N.B. Can construct parallel lines using ruler & compass.

Corollary: The regular n-gon is constructible iff $e^{2\pi i/n}$ is constructible.

$\boxed{\text{Basic Number Theory Facts}}$

To construct regular n-gons need to understand units in ring $\mathbb{Z}/m\mathbb{Z}$.

Def^n 3: The Euler phi-function

$\varphi(m)$ = no. positive integers $< m$ that are rel. prime to m

where m = integer > 1.

e.g. $\varphi(12) = \#\{1, 5, 7, 11\} = 4$

Facts: (a) $j + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ is invertible iff j is rel. prime to m.

Hence $|\underbrace{(\mathbb{Z}/m\mathbb{Z})^*}_{\text{group of units}}| = \varphi(m)$

(b) $e^{2\pi i j/m}$ is a primitive m-th root of unity iff j is rel. prime to m

Proof: (b) clear. For (a) $j + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^*$ iff $\langle j + m\mathbb{Z}\rangle = \mathbb{Z} \iff \mathbb{Z} = j\mathbb{Z} + m\mathbb{Z} = \gcd(m, j)\mathbb{Z} \iff \text{g.c.d.}(m, j) = 1$.

Thm: Let F = finite field. Then F^* is cyclic. In particular p prime $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Proof: Let $|F| = p^n$ so F^* is an abelian group order $p^n - 1$, rel. prime to p. Structure thm of finite abelian groups $\Rightarrow$

$$F^* \simeq \mathbb{Z}/h_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/h_r\mathbb{Z}$$

with $1 \neq h_1 | h_2 | \dots | h_r$.

If $r > 1$ then $h_r < p^n - 1$ & elts of F^* give $p^n - 1$ roots to the eq$^{\underline{n}}$ $x^{h_r} = 1$, a contradiction.