Ruler and compass constructions.

1. Definition. Suppose $S \subset \mathbf{C}$. We let

$$l(S)$$

be the set of lines in $\mathbf{C}$ at least two points of which are in S. We let

$$c(S)$$

be the set of circles in $\mathbf{C}$ whose centers are in S and at least one point of which is in S. We let $\gamma(S)$ be the set of points $z \in \mathbf{C}$ such that $z \in S$ or

$$z \in L_1 \cap L_2 \qquad \text{for two nonparallel lines } L_1 \text{ and } L_2 \text{ in } l(S)$$

or

$$z \in L \cap C \qquad \text{for some line } L \in l(S) \text{ and some circle } C \in c(S)$$

or

$$z \in C_1 \cap C_2 \qquad \text{for two distinct circles } C_1 \text{ and } C_2 \text{ in } c(S).$$

2. Definition. We set

$$K = \bigcup_{n=0}^{\infty} \gamma^n(\{0,1\});$$

A point of K is said to be **constructible**.

Our goal is to prove the

3. Main Theorem. K is a subfield of C each member of which is algebraic over $\mathbf{Q}$ with degree a power of 2.

4. Theorem. Suppose $S \subset \mathbf{C}$ and $z \in \gamma(S)$. Then either $z \in \mathbf{Q}(S \cup \overline{S})$ or z is algebraic of degree 2 over $\mathbf{Q}(S \cup \overline{S})$.

Proof. Suppose for $i = 1, 2$ that $w_i,\ z_i$ are distinct points of S

Part One. Suppose $w_1 z_2 - w_2 z_1 \neq 0$. Let

$$L_i = \{z \in \mathbf{C} : (\overline{z_i - w_i})z + (z_i - w_i)\overline{z} = (\overline{z_i - w_i})w_i + (z_i - w_i)\overline{w_i}\}$$

for $i = 1, 2$ and let z be the unique point of $L_1 \cap L_2$. By Cramer's Rule, $z \in \mathbf{Q}(S \cup \overline{S})$.

Part Two. Let

$$L = \{z \in \mathbf{C} : (\overline{z_1 - w_1})z + (z_1 - w_1)\overline{z} = (\overline{z_1 - w_1})w_1 + (z_1 - w_1)\overline{w_1}\},$$

let

$$C = \{z \in \mathbf{C} : |z - w_2| = |z_2 - w_2|\}$$

and suppose $z \in L \cap C$. Note that the defining equation for C can be written

$$(*) \qquad z\overline{z} - z\overline{w_2} - \overline{z}w_2 - w_2\overline{w_2} = z_2\overline{z} - z_2\overline{w_2} - \overline{z_2}w_2 - w_2\overline{w_2}.$$

Solve the defining equation of L for $\overline{z}$:

$$\overline{z} = ((\overline{z_1 - w_1})w_1 + (z_1 - w_1)\overline{w_1} - (\overline{z_1 - w_1})z)/(z_1 - w_1)$$

and substitute this in $(*)$, thereby concluding that either $z \in \mathbf{Q}(S \cup \overline{S})$ or z is algebraic of degree 2 over $\mathbf{Q}(S \cup \overline{S})$.

Part Three. For each $i = 1, 2$ let

$$C_i = \{z \in \mathbf{C} : |z - w_i| = |z_i - w_i|\},$$

suppose $C_1 \neq C_2$ and suppose $z \in C_1 \cap C_2$. Note that the defining equation for C_i can be written

$$(i) \qquad z\overline{z} - z\overline{w_i} - \overline{z}w_i - w_i\overline{w_i} = z_i\overline{z_i} - z_i\overline{w_i} - \overline{z_i}w_i - w_i\overline{w_i}$$

for each $i = 1, 2$. Subtract (2) from (1) and solve the resulting linear equation for $\overline{z}$ for $\overline{z}$. Then substitute this value back in (1), thereby concluding that either $z \in \mathbf{Q}(S \cup \overline{S})$ or z is algebraic of degree 2 over $\mathbf{Q}(S \cup \overline{S})$. □

5. Theorem. Suppose $S \subset \mathbf{C}$. Then

a. Suppose $z_i,\ i = 1, 2$ are distinct points of S and L is the perpendicular bisector of the line segment joining z_1 to z_2. Then $L \in l(\gamma(S))$.

b. Suppose $L_1 \in l(S)$, $z \in S \sim L_1$ and L_2 is the line passing through z which is perpendicular to L_1. Then $L_2 \in l(\gamma^2(S))$.

c. Suppose $L_1 \in l(S)$, $z \in S \sim L_1$ and L_2 is the line passing through z which is parallel to L_1. Then Then $L_2 \in l(\gamma^3(S))$.

Proof. Look at the pictures I'm going to draw. □

6. Theorem. We have

a. $i \in K$;

b. $x, y \in \mathbf{R}$ and $z = x + iy \in K \ \Rightarrow\ x \in K$ and $y \in K$;

c. $z \in K \ \Rightarrow\ \overline{z} \in K$;

d. $z \in K \ \Rightarrow\ -z \in K$;

e. $z, w \in K \ \Rightarrow\ z + w \in K$;

f. $z \in K \ \Rightarrow\ |z| \in K$;

g. $z, w \in K \ \Rightarrow\ zw \in K$;

h. $z \in K \sim \{0\} \ \Rightarrow\ 1/z \in K$.

Proof. Look at the pictures I'm going to draw. □

7. Theorem. Suppose $z \in K$. Then z is algebraic over K of degree a power of 2.

Proof. We have already shown that each member of $\gamma^{n+1}(\{0, 1\})$ is algebraic over $\mathbf{Q}(\gamma^n(\{0, 1\} \cup \overline{\gamma^n(\{0, 1\})})$ of degree 1 or 2 whenever $n = 0, 1, 2, \ldots$. Since $\gamma^{n+1}(\{0, 1\})$ is finite, it follows that

$$[\mathbf{Q}(\gamma^{n+1}(\{0, 1\} \cup \overline{\gamma^{n+1}(\{0, 1\})}), \mathbf{Q}(\gamma^n(\{0, 1\} \cup \overline{\gamma^n(\{0, 1\})})] \qquad \text{is a power of 2 for } n = 0, 1, 2, \ldots.$$

But this implies that

$$[\mathbf{Q}(\gamma^{n+1}(\{0,1\} \cup \overline{\gamma^{n+1}(\{0,1\})}), \mathbf{Q}] \qquad \text{is a power of 2 for } n = 0, 1, 2, \ldots.$$

□