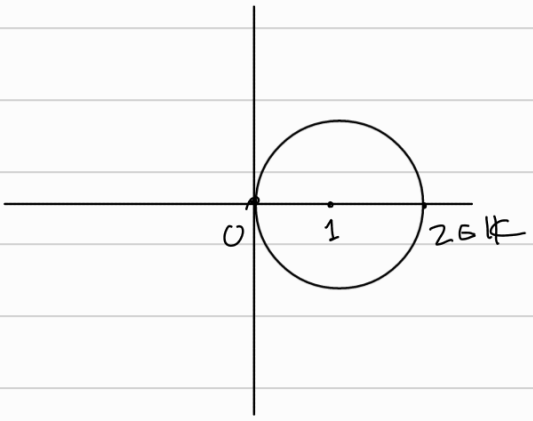
17. Constructions with ruler and compass (Chapter 18.5)

Let $P \neq Q$ be two points in $\mathbb{C}$. Then
$L(P,Q)$ denotes the line through P and Q,
$C(P,Q)$ denotes the circle with center P through Q.
So $L(P,Q)$ models the action of using a raler, while $C(P,Q)$ models the action of using a compass.

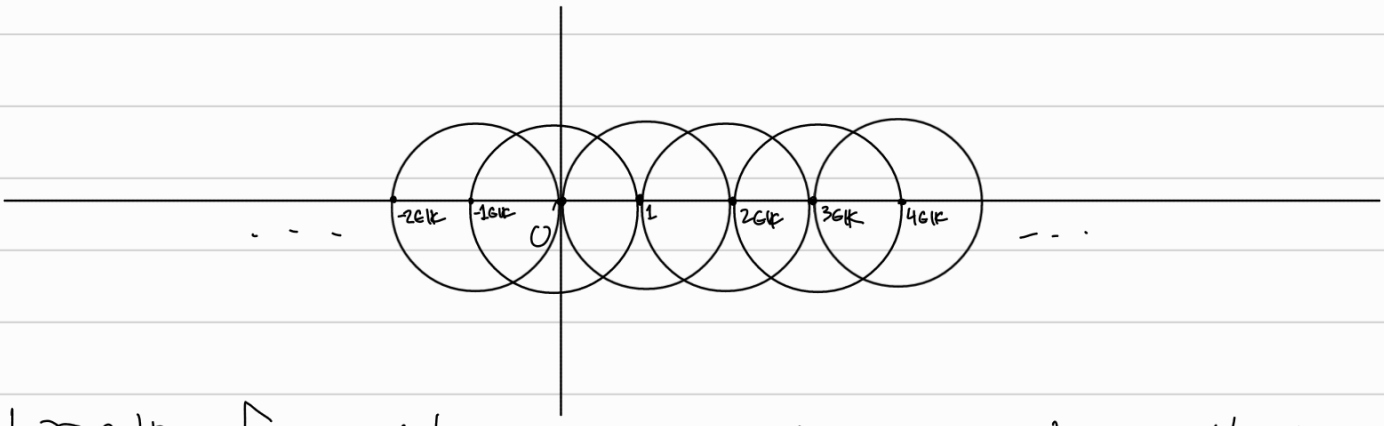
Definition 17.1. A point $Z \in \mathbb{C}$ is called constructible from given points $E,F,G,H \in \mathbb{C}$ if one of the following holds:
(1) $Z \in L(E,F) \cap L(G,H)$, where $L(E,F) \neq L(G,H)$, or
(2) $Z \in L(E,F) \cap C(G,H)$, or
(3) $Z \in C(E,F) \cap C(G,H)$, where $C(E,F) \neq C(G,H)$.

Definition 17.2. The subset $\mathbb{K} \subseteq \mathbb{C}$ of all constructible numbers is defined inductively by
(1) $0,1 \in \mathbb{K}$, and
(2) if $E,F,G,H \in \mathbb{K}$ and Z is constructible from E,F,G,H, then $Z \in \mathbb{K}$.

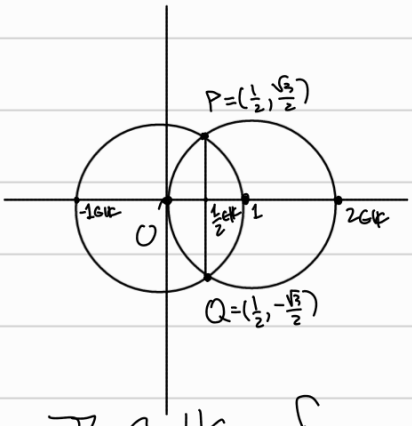
Example 17.3. (1) $2 \in \mathbb{K}$. Indeed, we can draw the line through $0,1 \in \mathbb{K}$ and the circle with center 1 passing through 0 to get $2 \in \mathbb{K}$:



and inductively:



(2) $\frac{1}{2}\mathbb{Z} \subseteq K$. From the above picture, we have all the circle intersections in K. Then For example



$$\frac{1}{2} = (\tfrac{1}{2}, 0) = L(P, Q) \cap L(0, (1,0))$$

(3) $2i\mathbb{Z} \subseteq K$. For example $C((1,0),(-1,0)) \cap C((-1,0),(1,0)) = \{2i, -2i\}$.
(4) $\{(1,1)\} = L((2,0),(0,2)) \cap C((1,0),(0,0))$ so $(1,1) \in K$. Similarly, $(1,-1) \in K$.

Notice that the allowed operations of constructibility coincide with those of Euclidean geometry. Hence we may also perform some standard actions of Euclidean geometry, for example drawing a line parallel to a given line and going through a given point (exercise).

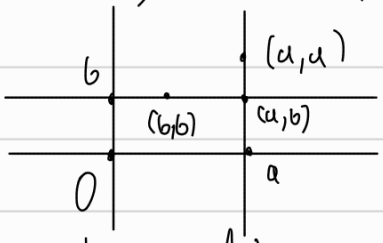
Lemma 17.4 Let $a \in \mathbb{R}$. The following are equivalent.
(1) $a \in K$.
(2) $a + ai \in K$.
(3) $ai \in K$.

Proof. (1) $\Rightarrow$ (2): $a+ai$ is the intersection of $C((a,0),(0,0))$ and $L((0,0),(1,1))$.
(2) $\Rightarrow$ (3): draw the line parallel to y-axis through (a,a) and intersect with x-axis.

(3) $\Rightarrow$ (2): Symmetric to (1) $\Rightarrow$ (2).
(2) $\Rightarrow$ (1): Symmetric to (2) $\Rightarrow$ (3). $\square$

Lemma 17.5 Let $a, b \in \mathbb{R}$. The following are equivalent.
(1) $a, bi \in \mathbb{K}$.
(2) $a+bi \in \mathbb{K}$.

Proof. (1) $\Rightarrow$ (2) $\{a+bi\} = L((a,0),(a,a)) \cap L((0,b)\cap(b,b))$.
Picture:



(2) $\Rightarrow$ (1): Draw a line through (a,b) and parallel to $L(0,i)$. It intersects $(0,1)$ at $(a,0)$ so $a \in \mathbb{K}$. Similarly $bi \in \mathbb{K}$. $\square$

Lemma 17.6 Let $z = a+bi$, $w = c+di \in \mathbb{K}$. Then the following hold.
(1) $z \pm w \in \mathbb{K}$.
(2) $z \cdot w \in \mathbb{K}$.
(3) If $w \neq 0$, then $\frac{z}{w} \in \mathbb{K}$.

Proof By Lemma 17.5 we have $a, c \in \mathbb{K}$ and $bi, di \in \mathbb{K}$.
(1) $a \pm c$ is the intersection of $L((0,0),(1,0))$ and $C((a,0),(a,c))$. Similarly we obtain $(b \pm d)i$. Then $z \pm w = (a \pm c) + (b \pm d)i \in \mathbb{K}$ by Lemma 17.5.
(2) From what we have already shown it suffices to show that $ac \in \mathbb{K}$. Since $\mathbb{Z} \subseteq \mathbb{K}$, we have by (1) that $c-1 \in \mathbb{K}$. Then ac is the intersection of $L((0,c),(a,c-1))$ and $L(0,(1,0))$.
(3) Again it is enough to show that if $a', b' \in \mathbb{R} \cap \mathbb{K}$, and $b' \neq 0$, then $\frac{a'}{b'} \in \mathbb{K}$. If $a' = 0$ there is nothing to show. If $a' \neq 0$, then $\frac{a'}{b'}$ is the intersection of $L((0,a'),(a',a'(1-b')))$ and $L(0,(1,0))$. $\square$

Corollary 17.7. There are Field extension $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$.

Proof. Since $0, 1 \in K$ and by Lemma 17.6 it follows that K is a field. Since $\mathbb{Z} \subseteq K$, it follows that $\mathbb{Q} \subseteq K$. □

Lemma 17.8. Let $z \in K$. Then $\sqrt{z} \in K$.

Proof. If $z = a+bi$ and $(c+di)^2 = a+bi$, then

$$c^2 - d^2 + 2cdi = a+bi$$

implies $c^2 - d^2 = a$ and $2cd = b$. Since this is a quadratic system, we have $c, d \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$. Hence it is enough to show that $a \in K \cap \mathbb{R}$ implies $\sqrt{a} \in K$. Notice that $(1, \sqrt{a})$ lies in the intersection of $C((\frac{1+a}{2}, 0), (0,0))$ with $L((1,0),(1,1))$. Then $(0, 2\sqrt{a})$ is in the intersection of $C((1, \sqrt{a}), (0,0))$ and $L((0,0),(0,1))$. Hence $(0, \sqrt{a}) \in K$ and so $\sqrt{a} \in K$ by Lemma 17.4. □

Theorem 17.9. The following are equivalent.

(1) $z \in K$ is constructible.

(2) There exists a sequence of field extensions $\mathbb{Q} = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n$ such that $z \in k_n$ and for every $1 \leq i \leq n$ we have $[k_i : k_{i-1}] = 2$. In particular it follows that $k_i = k_{i-1}(z_i)$ for some z_i with $z_i^2 \in k_{i-1}$.

If moreover any of (1) or (2) holds, then the following also holds

(3) There exists $t \in \mathbb{Z}$, $t \geq 0$ such that $[\mathbb{Q}(z) : \mathbb{Q}] = 2^t$.

Note: the book says (3) ⇒ (1) too, which is wrong, see problem 15 in Problem Set 6

Proof. We first show the extra claim in (2). For that it is enough to show that if $\mathbb{Q} \subseteq F \subseteq E$ are Field exte-

nsions with $[E:F]=2$, then there exists $\alpha \in E$ with $E=F(\alpha)$ and $\alpha^2 \in F$. Since $F \subsetneq E$, we have that there exists $\beta \in E \setminus F$. Then $F \subsetneq F(\beta) \subseteq E$ and so $[E:F] = [E:F(\beta)][F(\beta):F]$ implies $2=[E:F(\beta)][F(\beta):F]$. Since $[F(\beta):F]>1$, we conclude that $E=F(\beta)$. Then $\beta^2 \in E=F(\beta)$ and $[F(\beta):F]=2$ implies that there exist $a,b \in F$ such that $\beta^2 = a+b\beta$. Hence $\beta = \frac{a \pm \sqrt{a^2+4b}}{2}$. Set $\alpha = \frac{\sqrt{a^2+4b}}{2}$. Then $\beta = \frac{a}{2} \pm \alpha$ and so $\alpha \in E \setminus F$. As for b, we conclude that $E=F(\alpha)$. Since $\alpha^2 = \frac{a+4b}{4} \in F$, the claim is proved.

(1) $\Rightarrow$ (2). If $z \in \mathbb{Q}$, then there is nothing to show. Assume that z is constructed from $\mathbb{Q}$ after k iterations of the allowed operations in Definition 17.1. Notice that if $E,F,G,H \in K$, K a field, then the intersection of $L(E,F)$ and $L(G,H)$ is also in K, since the equations of a line are linear. On the other hand, the intersections of $L(E,F)$ and $C(G,H)$ or $C(E,F)$ and $C(G,H)$ are not necessarily in K since a quadratic equation is involved. Hence the obtained point, say α, From each such intersection belongs to $K(\alpha)$ and $[K(\alpha):K]=2$ if $\alpha \notin K$. Since z is reached after k iterations, we have a sequence of fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_k$$

where $[K_i : K_{i-1}] \in \{1,2\}$ and $z \in K_k \setminus K_{k-1}$. By removing the trivial field extensions from this sequence, (2) follows.

(2) $\Rightarrow$ (1) We claim that $K_i \subseteq \mathbb{K}$ for all $0 \le i \le n$. For $i=0$ this follows from Corollary 17.7. Assume that $K_{i-1} \subseteq \mathbb{K}$ and we show that $K_i \subseteq \mathbb{K}$. We have $K_i = K_{i-1}(z_i)$ and $z_i^2 \in K_{i-1} \subseteq \mathbb{K}$. Since $z_i^2 \in \mathbb{K}$, we have that $\sqrt{z_i^2} = z_i \in \mathbb{K}$ by Lemma 17.8. Since $K_{i-1} \subseteq \mathbb{K}$ and $z_i \in \mathbb{K}$ and $\mathbb{K}$ is a field, we obtain that $K_i = K_{i-1}(z_i) \subseteq \mathbb{K}$, as claimed. In particular $z \in K_k \subseteq \mathbb{K}$.

(3) follows immediately by (2) since $\mathbb{Q}(z) \subseteq K_k$. $\square$

Corollary 17.10. It is not possible to construct a square with the same area as a circle of radius 1 (using ruler and compass).

Proof. The area of the circle of radius 1 is π. Assume to a contradiction that there exists a square of side a with area $a^2 = \pi$. Then a is constructible. By Theorem 17.9 we have $[\mathbb{Q}(a) : \mathbb{Q}] = 2^t$. In particular, $\mathbb{Q} \subseteq \mathbb{Q}(a)$ is an algebraic extension. But $\pi = a^2 \in \mathbb{Q}(a)$ is transcedental over $\mathbb{Q}$, and we reach a contradiction. □