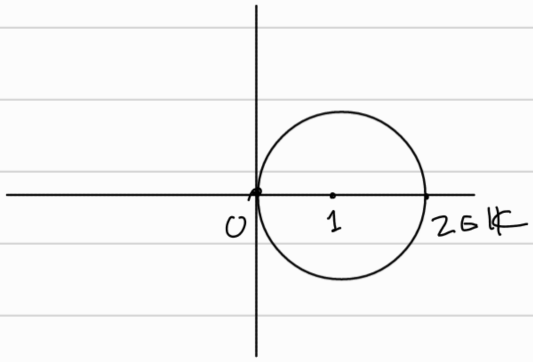
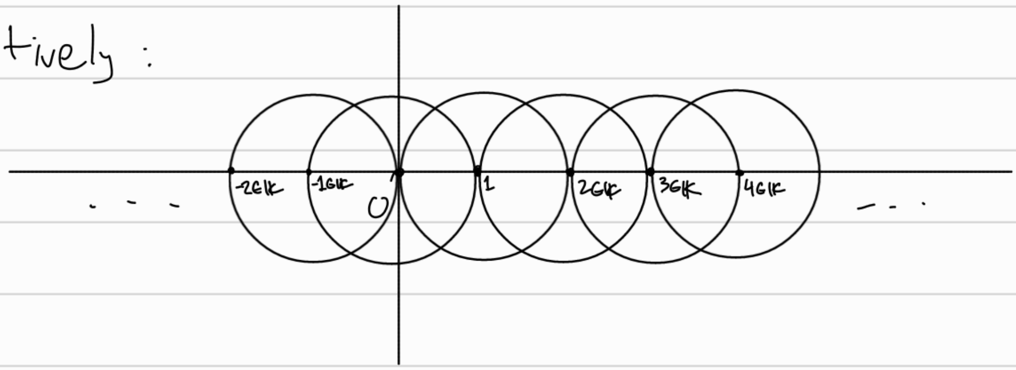
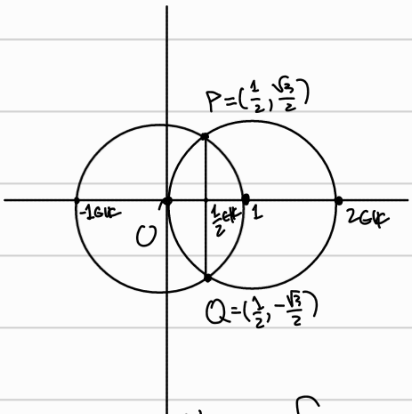
Example 17.3. (1) $\mathbb{Z} \subseteq \mathbb{K}$. Indeed, we can draw the line through $0, 1 \in \mathbb{K}$ and the circle with center 1 passing through 0 to get $2 \in \mathbb{K}$:



and inductively:



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



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

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

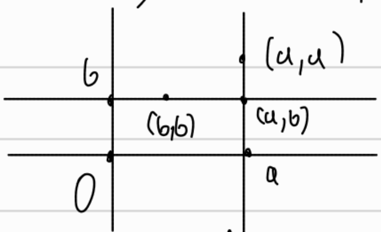
Notice that the allowed operations of constructibility coincide with those of Euclidean geometry. Hence we may also perform some standard actions of Euclidean geometry, for example drawing a line parallel to a given line and going through a given point (exercise).

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

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 sufficies 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 $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{C}$.

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

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

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 $a \in \mathbb{K} \cap \mathbb{R}$ implies $\sqrt{a} \in \mathbb{K}$. 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 $(0,\sqrt{a}) \in \mathbb{K}$ and so $\sqrt{a} \in \mathbb{K}$ by Lemma 17.4. $\square$

Theorem 17.9. The following are equivalent.
(1) $z \in \mathbb{C}$ is constructible.
(2) There exists a sequence of field extensions $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ 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) $\Rightarrow$ (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 extensions 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 β, 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 $0 \leq i \leq n$. 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 $z \in k_r \subseteq \mathbb{K}$.
(3) follows immediately by (2) since $\mathbb{Q}(z) \subseteq k_r$. $\square$

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. $\square$

Corollary 17.11. It is not possible to construct a cube with twice the volume of a given square (using ruler and compass).

Proof. Without loss of generality we may assume that we have a cube of side 1 and area $1^3 = 1$ and that we want to construct a cube of side x so that $x^3 = 2 \cdot 1 = 2$. Then $x = \sqrt[3]{2} \in \mathbb{R}$. The polynomial $x^3 - 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ (Eisenstein criterion for $p=2$) and so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3-2) = 3 \neq 2^t$. We conclude by Theorem

17.9 that $\sqrt[3]{2}$ is not constructible. $\square$

<u>Corollary 17.12.</u> It is not possible to trisect any angle (using ruler and compass).

<u>Proof.</u> Constructing an angle of measure θ is equivalent to constructing lengths a and b such that $\frac{a}{b} = \cos\theta$. Since $\mathbb{K}$ is a field, the problem is equivalent to showing that $\cos\theta$ is constructible (exercise). The triple angle formula says

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3} \tag{1}$$

and so, assuming that we have $\cos\theta$, we want to find $\cos^3\frac{\theta}{3} = a$. Then by (1) we have that a is a root of

$$f(x) = 4x^3 - 3x - \cos\theta \in \mathbb{Q}(\cos\theta)[x]$$

If $\cos\theta \in \mathbb{Q}$, then

$f(x)$ is irreducible$/\mathbb{Q} \Leftrightarrow [\mathbb{Q}(a):\mathbb{Q}] = 3 \xRightarrow{\text{Theorem 17.9}} a$ is not constructible

For $\theta = \frac{\pi}{3}$ we have $\cos\frac{\pi}{3} = \frac{1}{2} \in \mathbb{Q}$ and

$f(x) = 4x^3 - 3x - \frac{1}{2}$ is irreducible$/\mathbb{Q} \Leftrightarrow 8x^3 - 6x - 1$ is irreducible$/\mathbb{Q}$

$\overset{\text{Lemma 3.8}}{\Longleftrightarrow} 8x^3 - 6x - 1$ is irreducible$/\mathbb{Z}$.

and $8x^3 - 6x - 1$ is indeed irreducible over $\mathbb{Z}$ since it is of degree 3 and has no integer root (any integer root has to be a divisor of 1 and neither 1 nor -1 is a root). $\square$

<u>Definition 17.12.</u> A prime number p is called a <u>Fermat prime</u> if $\exists m \geq 0$ such that $p = 2^{2^m} + 1$.

<u>Example 17.13.</u> The only known Fermat primes are $3 = 2^{2^0} + 1$, $5 = 2^{2^1} + 1$, $17 = 2^{2^2} + 1$, $257 = 2^{2^3} + 1$, $65537 = 2^{2^4} + 1$.

Corollary 17.14. Let $n \geq 1$ be an integer. The following are equivalent.

(1) A regular n-gon is constructible (using ruler and compass).

(2) $\varphi(n) = 2^t$ for some $t \geq 0$.

(3) $n = 2^m p_1 \cdots p_r$ where $m \geq 0$ and $p_1, \dots, p_r$ are distinct Fermat primes.

Note: the proof in the book that (2) $\Rightarrow$ (1) is wrong since it uses the wrong implication from Theorem 17.9.

Proof (1) $\Rightarrow$ (2): Constructing a regular n-gon is equivalent to constructing the angle $\frac{2\pi}{n}$. This is equivalent to the primitive n-th root of unity $w = e^{\frac{2\pi i}{n}}$ being constructible. By Theorem 17.9 this implies that $[\mathbb{Q}(w) : \mathbb{Q}] = 2^t$ for some $t \geq 0$. Since by Theorem 14.12(2) we have $[\mathbb{Q}(w) : \mathbb{Q}] = \varphi(n)$, the claim follows.

(2) $\Rightarrow$ (1) As above it is enough to construct $e^{\frac{2\pi i}{n}}$. Since $\mathbb{Q} \subseteq \mathbb{Q}(w)$ is a Galois field extension, we have by the FTGT that $|G(\mathbb{Q}(w)/\mathbb{Q})| = [\mathbb{Q}(w) : \mathbb{Q}] = \varphi(n) = 2^t$. It follows that $G := G(\mathbb{Q}(w)/\mathbb{Q})$ is solvable (see Theorem 6.3.1 and Corollary 6.3.3 in the book). Then there exist

$$\{e\} = G_k \lhd G_{k-1} \lhd \dots \lhd G_1 \lhd G_0 = G$$

such that G_i/G_{i+1} is cyclic of prime order. In particular, since $|G_i/G_{i+1}| = |G_i|/|G_{i+1}|$ and $|G| = 2^t$, it follows that G_i/G_{i+1} is cyclic of order 2. By FTGT we obtain a sequence of field extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_k = \mathbb{Q}(w)$$

such that $[F_i : F_{i-1}] = |G_{i-1}/G_i| = 2$. Hence it follows by Theorem 17.9 that $w \in \mathbb{K}$.

(2) $\Leftrightarrow$ (3): Write $n = 2^m p_1^{m_1} \cdots p_r^{m_r}$ where $p_1, \dots, p_r > 2$ are distinct primes and $m_1, \dots, m_r \geq 1$. We use the following easy facts for φ:

- If $\gcd(a,b)=1$, then $\varphi(ab)=\varphi(a)\varphi(b)$.
- If p is prime and $k\geq 1$, then $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$.

Then

$$\varphi(n)=\varphi(2^m)\varphi(p_1^{m_1})\cdots\varphi(p_r^{m_r})=\varphi(2^m)\,p_1^{m_1-1}(p_1-1)\cdots p_r^{m_r-1}(p_r-1)$$

Since $\varphi(2^m)=2^{m-1}$ if $m\geq 1$ and $\varphi(2^0)=\varphi(1)=1$, we have that $\varphi(n)=2^t$ for $t\geq 0$ if and only if $m_1=\cdots=m_r=1$ and $p_1-1,\dots,p_r-1$ are powers of 2, or equivalently if $p_1,\dots,p_r$ are Fermat primes. $\square$