Math 412. Adventure sheet on Compass and straightedge constructions

CONSTRUCTIONS WITH COMPASS AND STRAIGHTEDGE: Athena gives you two marked points in the plane; we call them $(0, 0)$ and $(1, 0)$. You are allowed to do three things:

- use a straightedge to draw the line between two marked points
- use the compass to draw a circle whose center is a marked point, and with a radius to another marked point
- mark any point of intersection between lines and circle you draw.

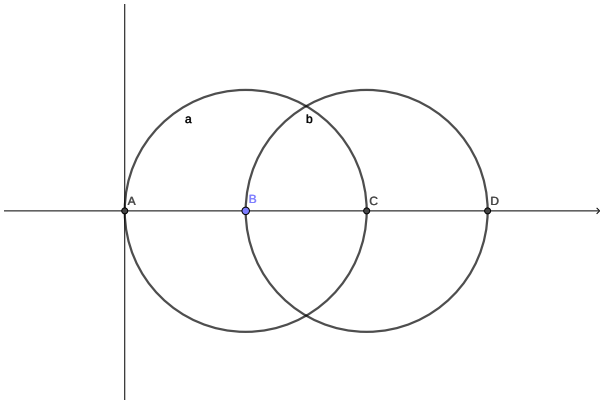
BASIC CONSTRUCTIONS:

- double or triple a length
- halve a length
- draw a perpendicular line through a point
- bisect an angle

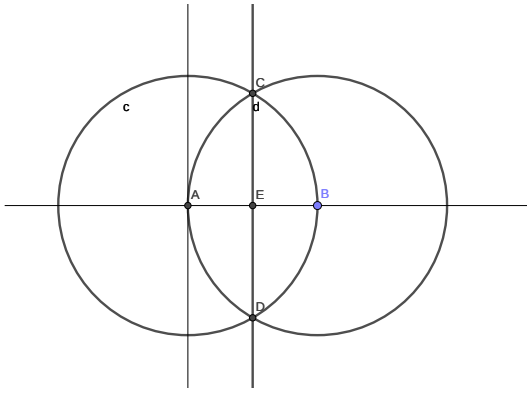
ADVANCED CONSTRUCTIONS:

- draw a parallel line though a point
- moving a segment of a given length onto a given line starting at a given point
- add or subtract two lengths
- create (α, β) from $(\alpha, 0)$ and $(\beta, 0)$
- create $(\alpha, 0)$ and $(\beta, 0)$ from (α, β)
- take the quotient of two lengths
- multiply two lengths
- take the square root of a length

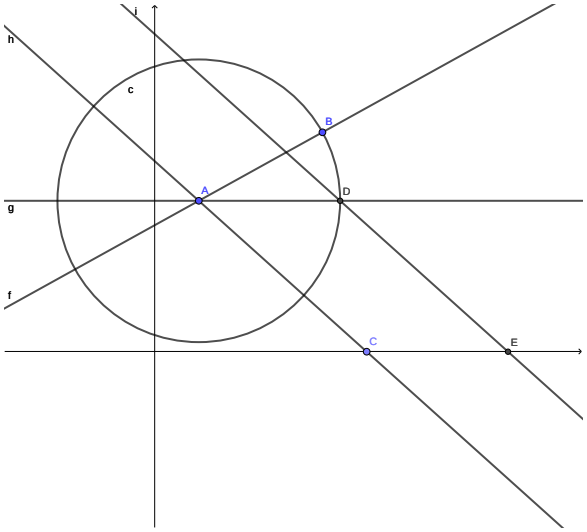
Here are examples of some of these constructions. Think about the rest or look them up in the book.



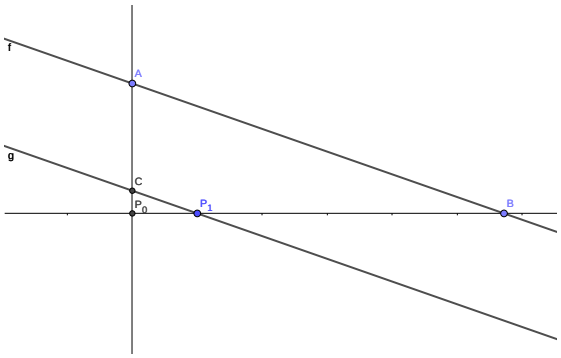
To double the length AB, make a circle centered at B passing through A, and intersect it with the line of AB. AC has twice the length.



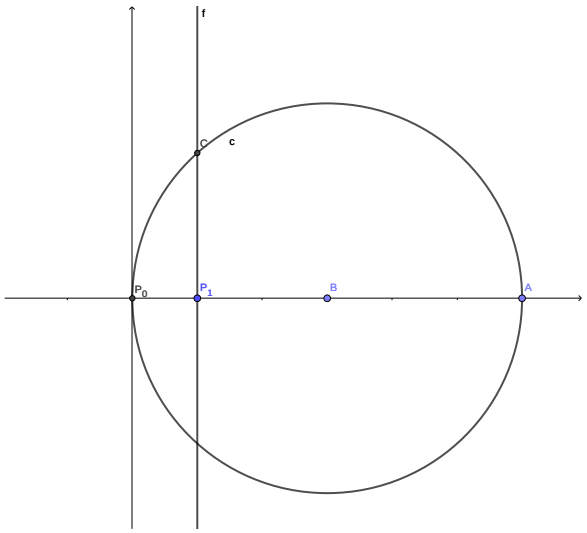
To halve the length AB, make a circle centered at A passing through B and a circle centered at B passing through A. These intersect at two points C and D. The line through CD meets the segment AB at its midpoint.



To move the segment AB to the x-axis starting at C, make a line g parallel to the x-axis passing through A. Make a circle centered at A passing through B, and mark the point of intersection with g; call it D. Finally, make a line parallel to AC passing through D. The segment CE has the same length as AB.



To make a segment whose length is the quotient of the lengths of two other segments, we can assume the given segments are on the y-axis (P_0A) and x-axis (P_0B). Remember that we have the point $P_1 = (1, 0)$ given. Make a line parallel to AB through P_1, and take its point of intersection with the y-axis; call it C. The length of P_0C is $\frac{|P_0A|}{|P_0B|}$.



To make a segment whose length is the square root of P_0A, first halve the segment; call the midpoint B. Take the circle e with center B passing through A. Make a line f parallel to the y-axis passing through $P_1 = (1, 0)$. Mark the intersection point C of e and f. The length of the segment P_1C is a the square root of P_0A.

DEFINITION: If we can mark a point $P = (\alpha, \beta)$ by using these rules repeatedly, we say that P is **constructible**. We say that a number α is **constructible** if $Q = (\alpha, 0)$ is constructible.

Our advanced constructions prove the following theorem (discuss!):

THEOREM 1:

(1) A point $P = (\alpha, y)$ is a constructible point if and only if α and β are constructible numbers.
(2) If x and y are constructible numbers, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, α/β, and $\sqrt{\alpha}$ (if $\alpha > 0$).

DEFINITION: Let $\mathbb{F} \subseteq \mathbb{R}$ be a subfield. A **quadratic extension field** of $\mathbb{F}$ is a set of the form

$$\mathbb{F}(\sqrt{k}) = \{a + b\sqrt{k} \mid a, b \in \mathbb{F}\} \subseteq \mathbb{R}$$

for some $k \in \mathbb{F}$, $k > 0$, such that k is not a square of an element in $\mathbb{F}$.

DEFINITION: A **quadratic extension tower** over $\mathbb{Q}$ is a sequence of subfields of $\mathbb{R}$

$$\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_t \subseteq \mathbb{R}$$

such that

$$F_1 = \mathbb{Q}(\sqrt{k_1}),\ F_2 = F_1(\sqrt{k_1}),\ \ldots\ ,\ F_t = F_{t-1}(\sqrt{k_t}),$$

with $k_1 \in \mathbb{Q}_{>0}$, $k_2 \in (F_1)_{>0}$, $\ldots$, $k_t \in (F_{t-1})_{>0}$.

THEOREM 2: A number $\alpha \in \mathbb{R}$ is constructible if and only if there is a quadratic extension tower over $\mathbb{Q}$ for which $\alpha \in F_t$ (with notation as above).

THEOREM 3: If α is a root of an irreducible cubic polynomial in $\mathbb{Q}[x]$, then α is not an element of any field in a quadratic extension tower over $\mathbb{Q}$.

A. DOUBLING THE CUBE: Can you construct the base of a cube C with volume 2?

(1) Explain why $\sqrt[3]{2}$ is a root of an irreducible cubic polynomial in $\mathbb{Q}[x]$.
(2) Explain how it follows from Theorems 2 and 3 that it is impossible to double the cube with straightedge and compass.

Solution.

(1) It is a root of $f(x) = x^3 - 2$. Since this has degree 3, it is irreducible if it has no roots in $\mathbb{Q}$. We showed in homework #1 that this is the case.
(2) By Theorem 3, $\sqrt[3]{2}$ is not an element of any field in a quadratic extension tower over $\mathbb{Q}$. By Theorem 2, it is not constructible.
(3) If we could make a segment of length $\sqrt[3]{2}$, that would be a constructible number, but it isn't!

B. TRISECTING AN ANGLE: Given an angle, can you divide it into three equal angles?

(1) To show this is impossible, why does it suffice to show that the number $\cos(20^\circ)$ is not constructible?
(2) The triple-angle formula for cosine says that $\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta)$. Show that $\cos(20^\circ)$ is a root of the polynomial $f(x) = 8x^3 - 6x - 1$.
(3) Show that $f(x)$ has no rational roots.[1] Conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
(4) Explain how it follows from Theorems 2 and 3 that it is impossible to trisect an angle with straightedge and compass.

Solution.

(1) The point is that we can construct an equilateral triangle, so the angle 60° is a valid given angle. If we could trisect it, we could make the angle 20°. Intersecting it with the unit circle would give us the point $(\cos(20^\circ), \sin(20^\circ))$, which would be constructible. Thus, if $\cos(20^\circ)$ is not constructible, trisecting the particular angle 60° is impossible.
(2) We have, setting $x = \cos(20^\circ)$, $\frac{1}{2} = \cos(60^\circ) = 4x^3 - 3x$.
(3) Suppose $\frac{a}{b}$, with $(a, b) = 1$, was a root of $f(x) = 8x^3 - 6x + 1$. Then $\frac{8a^3 - 6ab^2 + b^3}{b^3} = 0$, so $b^3 = 6ab^2 - 8a^3 = a(6b^2 - 8a^2)$. Since $a|b^3$, any prime that divides a also divides b. If $a \neq 1$, then this contradicts that a and b are coprime. If $a = 1$, then $b^3 - 6b^2 = 8$, so $b^2(b-2) = 8$. If $b < 2$, $b^2(b-2)$ is negative; if $b = 2$ it is zero, and if $b > 2$, $b^2(b-2) \geq 9$, so there is no solution.
Since $f(x)$ is degree three with no roots, it must be irreducible.
(4) This follows in exactly the same way as part (3) above.

C. QUADRATIC EXTENSION FIELDS: Let $\mathbb{F} \subseteq \mathbb{R}$ be a subfield.

(1) Show that[2] any quadratic extension field $\mathbb{F}(\sqrt{k})$ is a subfield of $\mathbb{R}$.
(2) Show that if $x \in \mathbb{R}$ is a solution of $Ax^2 + Bx + C = 0$ for some $A, B, C \in \mathbb{F}$, then $x \in \mathbb{F}(\sqrt{k})$ for some k.
(3) Show that the map $\phi : \mathbb{F}(\sqrt{k}) \to \mathbb{F}(\sqrt{k})$ given by $\phi(a + b\sqrt{k}) = a - b\sqrt{k}$ is a ring homomorphism, and that $\phi(f) = f$ for any element of $\mathbb{F}$.
(4) Use this fact to show that if $f(x)$ is a cubic polynomial with coefficients in $\mathbb{F}$, and $f(a + b\sqrt{k}) = 0$, then $f(a - b\sqrt{k}) = 0$.[3]

Solution.

(1) First, we observe that it is a subring of $\mathbb{R}$: $0, 1 \in \mathbb{F}$, so they are in $\mathbb{F}(\sqrt{k})$. It is clear that $\mathbb{F}(\sqrt{k})$ is closed under addition, additive inverses, and (foiling out) products. Since it is a subring of $\mathbb{R}$, it is commutative and $0 \neq 1$. Finally, since $(a + b\sqrt{k})(\frac{a - b\sqrt{k}}{a^2 - b^2 k}) = 1$, and $\frac{a - b\sqrt{k}}{a^2 - b^2 k} = \frac{a}{a^2 - b^2 k} - \frac{b}{a^2 - b^2 k}\sqrt{k}$, nonzero elements have additive inverses.
(2) This just follows from the quadratic formula!
(3) We check the second statement first: if $f \in \mathbb{F}$, we write $f = f + 0\sqrt{k}$, so $\phi(f) = \phi(f + 0\sqrt{k}) = f - 0\sqrt{k} = f$.
Now, we check the homomorphism conditions:

[1] Hint: Suppose there is a rational root a/b in lowest terms. Plug in this root, clear denominators, and show that if a prime divides a, it divides b, so WLOG $a = 1$. Now show that if $p|b$ then $p|a$ or else $p = 2\ldots$

[2] Hint: What is $(a + b\sqrt{k})(\frac{a - b\sqrt{k}}{a^2 - b^2 k})$?

[3] Hint: Let $\alpha = a + b\sqrt{k}$, and compute $\phi(f(a + b\sqrt{k}))$.

- $\phi(1) = 1$;
- $\phi((a + b\sqrt{k}) + (c + d\sqrt{k})) = \phi((a + c) + (b + d)\sqrt{k}) = (a + c) - (b + d)\sqrt{k} = (a - b\sqrt{k}) + (c - d\sqrt{k}) = \phi(a + b\sqrt{k}) + \phi(c + d\sqrt{k})$;
- $\phi((a+b\sqrt{k})(c+d\sqrt{k})) = \phi((ac+bdk)+(ad+bc)\sqrt{k}) = (ac+bdk)-(ad+bc)\sqrt{k} = (a - b\sqrt{k})(c - d\sqrt{k}) = \phi(a + b\sqrt{k})\phi(c + d\sqrt{k})$.

(4) Write $f(x) = Ax^3 + Bx^2 + Cx + D$. Let $\alpha \in \mathbb{F}(\sqrt{k})$. We have

$$\begin{aligned} 0 = \phi(0) = \phi(f(\alpha)) &= \phi(A\alpha^3 + B\alpha^2 + C\alpha + D) \\ &= \phi(A)\phi(\alpha)^3 + \phi(B)\phi(\alpha)^2 + \phi(C)\phi(\alpha) + \phi(D) \\ &= A\phi(\alpha)^3 + B\phi(\alpha)^2 + C\phi(\alpha) + D = f(\phi(\alpha)), \end{aligned}$$

so $\phi(\alpha) = a - b\sqrt{k}$ is also a root!

D. INTERSECTION POINTS: Let $\mathbb{F} \subseteq \mathbb{R}$ be a subfield. Let L_1 and L_2 be lines through two points with coordinates in $\mathbb{F}$. Let C_1 and C_2 be circles whose centers have coordinates in $\mathbb{F}$, and radii are values of $\mathbb{F}$.

(1) If L_1 is not vertical, why are the slope and y-intercept of L_1 values of $\mathbb{F}$? What can you say about the equation of L_1 if it is vertical?
(2) Explain why C_1 has an equation of the form $(x - A)^2 + (y - B)^2 = C^2$, where $A, B, C \in \mathbb{F}$.
(3) Explain why the intersection point of L_1 and L_2 (if they are not parallel) has coordinates in $\mathbb{F}$.
(4) Explain why the intersection points of L_1 and C_1 (if they exist) have coordinates in a quadratic extension field of $\mathbb{F}$.
(5) Explain why the intersection points of C_1 and C_2 (if they exist) have coordinates in a quadratic extension field of $\mathbb{F}$.

Solution.

(1) Let L_1 pass through the points (a, b) and (c, d) with $a, b, c, d \in \mathbb{F}$, and $a \neq c$. Then the slope of L is $m = \frac{d-b}{c-a} \in \mathbb{F}$, and the intercept is $b - ma \in \mathbb{F}$. If it is a vertical line, the equation is $x = a$ for some $a \in \mathbb{F}$.
(2) If C_1 has center (A, B) and radius C, the stated equation is an equation for C_1.
(3) Let $L_1 : y = mx + b$ and $L_2 : y = m'x + b'$ with $m, m', b, b' \in \mathbb{F}$. Substituting, we get an equation $(m - m')x = b' - b$ for the x-coordinate of the intersection, which has a solution in $\mathbb{F}$, and plugging back into $y = mx + b$, we can solve for y in $\mathbb{F}$.
(4) Let $L_1 : y = mx + b$ and $C_1 : (x - A)^2 + (y - B)^2 = C^2$, with $m, b, A, B, C \in \mathbb{F}$. To solve for the x-coordinate, substitute in for y to get a quadratic equation for x. Thus, the x-coordinate lives in $\mathbb{F}(\sqrt{k})$ for some k. Then, using the L_1 equation, the y-coordinate also lives in this field $\mathbb{F}(\sqrt{k})$.
(5) Let $C_1 : (x - A)^2 + (y - B)^2 = C^2$ and $C_1 : (x - A')^2 + (y - B')^2 = C'^2$ with $A', B', C' \in \mathbb{F}$. Then, taking the difference, we get an equation where the x^2 and y^2 terms cancel; we get the equation of a line L with coefficients in $\mathbb{F}$. Thus, this case follows from the previous one.

E. CONSTRUCTIBLE NUMBERS:

(1) Explain why every rational number $r \in \mathbb{Q}$ is constructible.

(2) Explain why any number in a quadratic extension field of $\mathbb{Q}$ is constructible.
(3) Show that, if every number in a subfield $\mathbb{F}$ of $\mathbb{R}$ is constructible, then every number in any quadratic extension field $\mathbb{F}(\sqrt{k})$ of $\mathbb{F}$ is constructible.
(4) Show that any element of $r \in F_t$ for a field in a quadratic extension tower over $\mathbb{Q}$ is constructible.
(5) Show that any constructible number $r \in \mathbb{R}$ is an element of some field F_t that lies in a quadratic extension tower.
(6) Conclude the proof of Theorem 2.

Solution.

(1) This is a consequence of Theorem 1: we can construct any natural number or its negative, and divide any pair of these to get any rational number.
(2) Take $a, b, k \in \mathbb{Q}$, with $k > 0$. We can construct $a, b, k, \sqrt{k}, b\sqrt{k}$, and $a + b\sqrt{k}$ by Theorem 1. This is every number we seek.
(3) It's the exact same argument, starting with $a, b, k \in \mathbb{F}$, with $k > 0$.
(4) We apply the last step t times.
(5) Any point we can get in a construction can be made by starting with two points with rational coordinates, and doing finitely many steps where we take intersection points of lines and circles. In each of our steps, the coordinates of our points live in the same field or else in a quadratic extension field. Thus, the points always have coordinates in a quadratic extension tower over $\mathbb{Q}$.
(6) This is (4) and (5).

F. CUBIC POLYNOMIALS AND QUADRATIC EXTENSIONS:

(1) Show that if $\mathbb{F}$ is a field, $\mathbb{F}(\sqrt{k})$ is a quadratic extension, and $\alpha \in \mathbb{F}(\sqrt{k})$, then $g(x) = (x-\alpha)(x-\phi(\alpha))$ has coefficients in $\mathbb{F}$ (i.e., is a polynomial in $\mathbb{F}[x]$), where ϕ is the map from the Quadratic extension fields problem.
(2) Show that if $\mathbb{F}$ is a field, $\mathbb{F}(\sqrt{k})$ is a quadratic extension, $f(x) \in \mathbb{F}[x]$ is a cubic polynomial, and $f(x)$ has a root in $\mathbb{F}(\sqrt{k})$, then $f(x)$ has a root in $\mathbb{F}$.[4]
(3) Show that if γ is a root of an irreducible cubic polynomial in $\mathbb{Q}[x]$, then γ is not an element of any field in a quadratic extension tower over $\mathbb{Q}$.[5]
(4) Conclude the proof of Theorem 3.

Solution.

(1) Let $\gamma = a + b\sqrt{k}$ with $a, b \in \mathbb{F}$. Foil out to find coefficients: the x coefficient is $-\gamma - \phi(\gamma) = -2a \in \mathbb{F}$, and the unit coefficient is $\gamma\phi(\gamma) = a^2 - kb^2 \in \mathbb{F}$.
(2) By part (4) of the quadratic extension fields problem, $\phi(\alpha)$ is also a root. Since $(x - \gamma)$ and $(x - \phi(\alpha))$ are coprime, the product $g(x)$ divides $f(x)$. The quotient is a degree one polynomial in $\mathbb{F}[x]$, so there must be a root in $\mathbb{F}$.
(3) Following the hint, to obtain a contradiction, suppose α is constructible, take a quadratic extension tower and pick F_t such that F_t contains α but F_{t-1} does not. Consider $f(x)$

[4]Hint: Show that the polynomial $g(x)$ from the previous part divides $f(x)$.

[5]Hint: To obtain a contradiction, suppose γ is constructible, take a quadratic extension tower and pick F_t such that F_t contains γ but F_{t-1} does not.

as a cubic polynomial in $F_{t-1}[x]$. The previous part applies: since it has a root in $F_t = F_{t-1}(\sqrt{k})$, it has a root in F_{t-1}, contradicting the choice of t.