Solutions to David A.Cox "Galois Theory"

Richard Ganaye

April 16, 2020

10 Chapter 10 : GEOMETRIC CONSTRUCTIONS

10.1 CONSTRUCTIBLE NUMBERS

Ex. 10.1.1 *In part (a) of Example 10.1.2 we constructed the x-axis. In a similar way show that the y-axis is constructible. For each step in your construction be sure to say which of $C1, C2, P1, P2$, and $P3$ you are using.*

Proof. Let $\mathcal{C}$ be the set of constructible numbers in $\mathbb{C}$.

Write $C(\gamma, r)$ the circle with center $\gamma \in \mathbb{C}$ and radius r.

Starting from $\{0, 1\}$, we obtain by $C1$ the x-axis and by $P2$ the point -1 at the intersection of $C(0, 1)$ with the x-axis, so

$$\{-1, 0, 1\} \subset \mathcal{C}.$$

If $\alpha = -1, \beta = 1$, then $|\beta - \alpha| = 2$, so $C(-1, 2)$ and $C(1, 2)$ are constructible by $C2$.

Using $P3$, the intersection $C(-1, 2) \cap C(1, 2) = \{\delta - \delta\}$ gives the point $\delta = i\sqrt{3}$. The y-axis that goes through 0 and δ is so constructible by $C1$. □

Ex. 10.1.2 *Suppose that α, β, γ are noncolinear and consider the rays $\overrightarrow{\alpha\beta}$ and $\overrightarrow{\alpha\gamma}$ emanating from α that go through β and γ respectively. We call this the angle formed by α, β, γ. Also assume that α, β, γ are constructible.*

(a) Prove that there is a constructible number δ with positive y-coordinate such that the angle formed by α, β, γ is congruent to the angle formed by $0, 1, \delta$. As in Exercise 1, each step in the construction should be justified by $C1, C2, P1, P2$, or $P3$.

(b) Prove that the claim made in Example 10.1.3 that $\zeta_n = e^{2\pi i/n}$ is constructible if and only if a regular n-gon can be constructed by straightedge and compass.

Proof. (a) $C(\alpha, 1)$ is constructible by $C2$. Let γ' the intersection point of the line $\alpha\beta$ with $C(\alpha, 1)$, then γ' is constructible by $P2$. Let η the orthogonal projection of γ' on the line $\alpha\beta$. Then η is constructible with the usual construction: the circle $C(\gamma', r)$, with $r = |\gamma'\alpha|$, has two intersection points α, α' with the line $\alpha\beta$, and the intersection point $\gamma'' \neq \gamma'$ of $C(\alpha, r)$ with $C(\alpha', r)$ is constructible, so is the line $\gamma'\gamma''$, and η the intersection of the line $\gamma'\gamma''$ with the orthogonal line $\alpha\beta$. Then the cosine of the angle $(\overrightarrow{\alpha\beta}, \overrightarrow{\alpha\gamma})$ is $\pm|\eta\alpha|$.

Write ξ, ξ' the two intersection points of $C(0, |\eta\alpha|)$ with the x-axis. The line passing trough ξ and orthogonal to the x-axis intersect $C(0, 1)$ in the point δ_1 with positive y-coordinate, and similarly line passing trough ξ' and orthogonal to the

x-axis intersect $C(0,1)$ in the point δ_2 with positive y-coordinate, so both are constructible. Then the cosine of the angle formed by $0, 1, \delta_1$ is the opposite of the cosine of the angle formed by $0, 1, \delta_2$, and equal in absolute value to $|\eta\alpha|$. So the angle formed by $0, 1, \delta_1$ or $0, 1, \delta_2$ is congruent to the angle formed by α, β, γ, so we can take $\delta = \delta_1$ or $\delta = \delta_2$ such that the angle formed by $0, 1, \delta$ is congruent to the angle formed by α, β, γ, and δ is constructible.

(b) • If ζ_n is constructible, so are $1, \zeta_n, \ldots, \zeta_n^{n-1}$ since $\mathcal{C}$ is a subfield of $\mathbb{C}$ (Theorem 10.1.4), and these points are the vertices of a regular n-gon.

• Suppose that a regular n-gon can be constructed by straightedge and compass. Let β, γ be two consecutive vertices. Then the center α of the n-gon is constructible, and the measure of the angle formed by α, β, γ has measure $\theta = 2\pi/n$ (see Example 10.1.3).

By part (a), we can construct δ with positive y-coordinate such that the angle formed by $0, 1, \delta$ has the same measure $2\pi/n$. The intersection ζ of the line 0δ with $C(0,1)$ is constructible, and $\arg(\zeta) = 2\pi/n, |\zeta| = 1$, so $\zeta_n = \zeta$ is constructible.

□

Ex. 10.1.3 *This exercise covers the details omitted in the proof of Theorem 10.1.4.*

(a) Let α, β be constructible numbers such that $0, \alpha, \beta$ are collinear. Prove that $\alpha + \beta$ is constructible.

(b) Let $a \in \mathcal{C} \cap \{x \in \mathbb{R} \mid x > 0\}$. Use Figure 2 in the proof of Theorem 10.1.4 to show that $1/a$ is constructible.

(c) In the proof of Theorem 10.1.4, we showed that $\mathcal{C} \cap \{x \in \mathbb{R} \mid x > 0\}$ is closed under addition, mutiplication, and multiplicative inverses. Use this to prove that $\mathcal{C} \cap \mathbb{R}$ is a subfield of $\mathbb{R}$.

(d) Prove that the number β pictured in (10.1) is constructible (assuming that r is constructible).

Proof. (a) Let D be the line passing through $0, \alpha, \beta$, and C the circle of radius $|\beta|$ with center α. Then D and C intersect in two points, one of them being $\alpha + \beta$, which is so constructible.

(b) As a is constructible, so is ia. We can construct the parallel to the line $1, ia$ passing through i. The intersection point of this parallel with the x-axis gives a point $d > 0$. As the triangles $(0, d, i)$ and $(0, 1, ia)$ are similar, $d/1 = i/ia$, so $1/a = d$ is constructible.

(c) We have proved in the text that $\mathcal{C}$ is a subgroup of $(\mathbb{C}, +)$, so $\mathcal{C} \cap \mathbb{R}$ is a subgroup of $(\mathbb{R}, +)$.

Let $a, b \in \mathcal{C} \cap \mathbb{R}$. If $a = 0$ or $b = 0$ then $a + b \in \mathcal{C} \cap \mathbb{R}$. If $a \neq 0, b \neq 0$ then $|a| = \pm a \in \mathcal{C} \cap \mathbb{R}_+^*$, so $|ab| = |a||b| \in \mathcal{C} \cap \mathbb{R}_+^*$, therefore $ab = \pm|ab| \in \mathcal{C} \cap \mathbb{R}$.

Let $a \in \mathcal{C} \cap \mathbb{R}, a \neq 0$. then $|a| \in \mathcal{C} \cap \mathbb{R}_+^*$, so $1/|a| \in \mathcal{C} \cap \mathbb{R}_+^*$. Therefore $1/a = \pm 1/|a| \in \mathcal{C} \cap \mathbb{R}$.

Conclusion : $\mathcal{C} \cap \mathbb{R}$ is a subfield of $\mathbb{R}$.

(d) We can construct the orthogonal line D to the x-axis passing through 1, the bisection of $(0, 2)$. As r is constructible, so is $1+r$ (Exercise 10.1.3(a)). The intersection of the bisection of $(0, 1 + r)$ with the x-axis gives the number $(1 + r)/2$, which is so constructible. The intersection of the circle with radius $(1 + r)/2$ centered in $(1 + r)/2$ with D give β with positive y-coordinate, and so β is constructible.

The end of the proof of Theorem 10.1.4 shows that $\sqrt{r}$ is constructible.

□

Ex. 10.1.4 *This exercise covers the details omitted in the proof of Theorem 10.1.6.*

(a) Suppose that a line l_1 goes through distinct points $\alpha_1 = u_1 + iv_1$ and $\beta_1 = u_2 + iv_2$, where u_1, v_1, u_2, v_2 lie in a subfield $F \subset \mathbb{R}$. Prove that l_1 is defined by an equation of the form $a_1x + b_1y = c_1$ where $a_1, b_1, c_1 \in F$.

(b) Suppose that $\alpha_2 \neq \beta_2$ and γ_2 are complex numbers whose real and imaginary parts lie in a subfield $F \subset \mathbb{R}$. Prove that the circle C with center γ_2 and radius $|\alpha_2 - \beta_2|$ has an equation of the form (10.3) with $a_2, b_2, c_2 \in F$.

(c) In the proof of Theorem 10.1.6, we considered the equations (10.2) and (10.3) when $a_1 \neq 0$. Explain what happens when $a_1 = 0$ in (10.2).

Proof. (a) Let $M = (x, y), A = (u_1, v_1), B = (u_2, , v_2)$ the points of $\mathbb{R}^2$ with affixes z, α_1, β_1, where $\alpha_1 \neq \beta_1$. Then

$$\begin{aligned} M \in (AB) &\iff \det(\overrightarrow{AM}, \overrightarrow{AB}) = 0 \\ &\iff \begin{vmatrix} x - u_1 & u_2 - u_1 \\ y - v_1 & v_2 - v_1 \end{vmatrix} = 0 \\ &\iff (v_2 - v_1)x - (u_2 - u_1)y - u_1(v_2 - v_1) + v_1(u_2 - u_1) = 0 \\ &\iff a_1x + b_1y = c_1 \end{aligned}$$

where $a_1 = v_2 - v_1, b_1 = -(u_2 - u_1), c_1 = u_1(v_2 - v_1) - v_1(u_2 - u_1) \in F$.

(b) Let $z = x + iy, \gamma_2 = u + iv, \alpha_2 - \beta_2 = a + ib$, where $u, v, a, b \in F$. Then

$$\begin{aligned} z \in C &\iff |z - \gamma_2|^2 = |\alpha_2 - \beta_2|^2 \\ &\iff (x - u)^2 + (y - v)^2 = a^2 + b^2 \\ &\iff x^2 + y^2 + a_2x + b_2y + c_2 = 0, \end{aligned}$$

where $a_2 = -2u, b_2 = -2v, c_2 = -(a^2 + b^2) \in F$.

(c) If $a_1 = 0$, then for all $z = x + iy \in l$, $y = c_1/b_1x = u$, where $u = c_1/b_1 \in F = F_n$. Substituting $y = u$ into (10.3) gives the quadratic equation

$$x^2 + a_2x + u^2 + b_2u + c_2.$$

Therefore x lies in a quadratic extension F_{n+1} of F_n (and $y \in F_n \subset F_{n+1}$).

□

Ex. 10.1.5 *In this exercise you will give two proof that $\zeta_3 = e^{2\pi i/3}$ is constructible.*

(a) Give a direct geometric construction of ζ_3 with each step justified by citing $C1, C2, P1, P2$ or $P3$.

(b) Use Theorem 10.1.6 to show that ζ_3 is constructible.

Proof. (a) As $\mathrm{Re}(\zeta_3) = -1/2$, ζ_3 is on the bissection of $(-1, 0)$.

We gives the details of the construction: $C(0, 1)$ and $C(-1, 0)$ are constructible by $C2$, so the two intersection points are constructibles by $P3$, and these two points are $\zeta_3, \overline{\zeta}_3$, so ζ_3 is constructible.

(b) As the minimal polynomial of ζ_3 over $\mathbb{Q}$ is $x^2 + x + 1$, the extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_3)$ is quadratic, so ζ_3 is constructible by Theorem 10.1.6.

□

Ex. 10.1.6 *Show that it is impossible to trisect a 60° angle by straightedge and compass.*

Proof. If a 20° angle was constructible by straightedge and compass, then ζ_{18} would be constructible. The minimal polynomial of ζ_{18} is $\Phi_{18}(x)$.

By Exercise 9.1.12, $\Phi_{18}(x) = \Phi_9(-x)$, and $\Phi_9(x) = \Phi_3(x^3) = x^6 + x^3 + 1$, so

$$\Phi_{18}(x) = x^6 - x^3 + 1.$$

Therefore $[\mathbb{Q}(\zeta_{18}) : \mathbb{Q}] = 6$. If ζ_{18} was constructible, by Theorem 10.1.6, there exist subfields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C},$$

with $[F_i : F_{i-1}] = 2$ for $1 \leq i \leq n$, and $\zeta_{18} \in F_n$. But then by the tower theorem, $6 = [\mathbb{Q}(\zeta_{18}) : \mathbb{Q}]$ divides $[F_n : \mathbb{Q}] = 2^n$, and $3 \mid 2^{n-1}$: this is a contradiction. So ζ_{18} is not constructible, hence it is impossible to trisect a 60° angle by straightedge and compass. □

Ex. 10.1.10 *Suppose we have extensions $\mathbb{Q} \subset F \subset \mathbb{C}$ where $[F : \mathbb{Q}]$ is finite. Prove that there is a field M such that $F \subset M \subset \mathbb{C}$ and M is a Galois closure of F over $\mathbb{Q}$.*

Proof. As $[F : \mathbb{Q}]$ is a finite extension, and as $\mathbb{Q}$ has characteristic 0, by the Theorem of the Primitive Element (Corollary 5.4.2 (b)), $F = \mathbb{Q}(\alpha)$ for some $\alpha \in F$. Let f be the minimal polynomial of α over $\mathbb{Q}$.

As $\mathbb{C}$ is an algebraically closed field, f splits completely over $\mathbb{C}$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ the roots of f in $\mathbb{C}$, and $M = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ the splitting field of f in $\mathbb{C}$. Then

(a) $\mathbb{Q} \subset M$ is a Galois extension, since the splitting field of f over $\mathbb{Q}$ is a normal extension of $\mathbb{Q}$, and separable since the characteristic of $\mathbb{Q}$ is 0.

(b) Let $M \subset M'$ by any other extension such that M' is a Galois extension over $\mathbb{Q}$. As $\alpha \in M \subset M'$ is a root of f and as M' is normal, f splits completely over M', with roots $\beta_1 = \alpha_1, \beta_2, \ldots, \beta_n, \in M'$. Let $M'' = \mathbb{Q}(\beta_1, \ldots, \beta_n)$, so M'' is a splitting field of f over $\mathbb{Q}$. By the uniqueness of splitting fields (Corollary 5.1.7), there is an isomorphism $\varphi : M \to M''$ that is the identity on L. Since $M'' \subset M'$, φ defines a field homomorphism $\varphi : M \to M'$.

So the parts (a),(b) of the definition of an Galois closure are satisfied.

Conclusion: there is a field M such that $F \subset M \subset \mathbb{C}$ and M is a Galois closure of F over $\mathbb{Q}$. □

Ex. 10.1.8 *In the Mathematical notes we defined the field $\mathcal{P} \subset \mathbb{R}$ and what it means for a subfield $F \subset \mathbb{R}$ to be Pythagorean.*

(a) Let α be a real number. Prove that $\alpha \in \mathcal{P}$ if and only if there is a sequence of fields $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{R}$ such that $\alpha \in F_n$, and for $i = 1, \ldots, n$ there are $a_i, b_i \in F_{i-1}$ such that $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$.

(b) Prove that $\mathcal{P}$ is the smallest Pythagorean subfield of $\mathbb{R}$.

Write $\mathbb{P}$ the set of points of $\mathbb{C}$ (identified with the Euclidean plane) constructible by a sequence of straightedge-and-dividers constructions, and $\mathbb{D}$ the set of lines passing through two distinct such points (so constructible by straightedge-and-dividers) .

Lemma 1. *If $A, B, C \in \mathbb{P}$, with $A \neq B$, then the parallel l to (AB) passing through C is in $\mathbb{D}$.*

Proof. Let C' the symmetric point of C relative to A, and C'' the symmetric point of C' relative to B, so $\overrightarrow{AC'} = -\overrightarrow{AC}, \overrightarrow{BC''} = -\overrightarrow{BC'}$. Since $AC = AC'$ and $BC' = BC''$, C', C'' lie in $\mathbb{P}$, and $\overrightarrow{CC''} = 2\overrightarrow{AB}$, so $C \neq C''$ and (CC'') is parallel to (AB), with $(CC'') \in \mathbb{D}$. So $l = (CC'') \in \mathbb{D}$. □

Lemma 2. *$\mathcal{P}$ is a subfield of $\mathbb{R}$.*

Proof. Using Lemma 1, we can mimic the proof of Theorem 8.1.4. □

Lemma 3. *Let $\alpha = a + ib \in \mathbb{C}$, where $a, b \in \mathbb{R}$. Then $\alpha \in \mathbb{P}$ if and only if $a, b \in \mathcal{P}$.*

Proof.

- Suppose that $\alpha = a + ib \in \mathbb{P}$. By Lemma 1, we can construct by straightedge-and-dividers constructions the lines passing through α and parallel to the axis, so a, ib are constructible, and using the divider, so are the real numbers a, b, therefore $a, b \in \mathcal{P}$.

- Suppose that $a, b \in \mathcal{P}$. Then $a, ib \in \mathbb{P}$, and the intersection $\alpha = a + ib$ of the lines passing through these two points and parallel to the y-axis and x-axis respectively lies in $\mathbb{P}$.

□

Proof. (Ex. 10.1.8)

(a) Let α be a real number.

- Suppose that there is a sequence of fields $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{R}$ such that $\alpha \in F_n$, and for $i = 1, \ldots, n$ there are $a_i, b_i \in F_{i-1}$ such that $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$.
  We prove by induction that $F_k \subset \mathcal{P}$. Since $\mathcal{P}$ is a subfield of $\mathbb{R}$, $F_0 = \mathbb{Q} \subset \mathbb{R}$. Suppose that $F_{i-1} \subset \mathcal{P}$. As $a_i, b_i \in F_{i-1} \subset \mathcal{P}$, $\sqrt{a_i^2 + b_i^2} \in \mathcal{P}$ (see the Mathematical Notes), so $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right) \subset \mathcal{P}$, and the induction is done.
  Therefore $F_n \subset \mathcal{P}$, and $\alpha \in F_n$, so $\alpha \in \mathcal{P}$.

- Conversely, suppose that $\alpha = a+ib \in \mathbb{P}$. We use induction on the number N of steps in the construction of α to prove that there is a sequence of subfield of $\mathbb{R}$, $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{R}$ such that $a, b \in F_n$, where $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$, $i = 1, \ldots, n$.

  When $N = 0$, we must have $\alpha = 0, 1$ or i, in which case we let $F_n = F_0 = \mathbb{Q}$.

  Now suppose that α is constructed in $N > 1$ steps, where the last step use the intersection of two lines l_1, l_2. As in the proof of theTheorem 10.1.6, the coordinates of α lie in the same field F_n.

  If the last step uses the divider, then their exists four points $\beta, \gamma, \delta, \varepsilon \in \mathbb{P}$ such that $\delta, \varepsilon, \alpha$ are collinear and $|\alpha - \delta| = |\beta - \gamma|$. Moreover, by the induction hypothesis, the coordinates $\beta_x, \beta_y, \gamma_x, \ldots$ of $\beta, \gamma, \delta, \varepsilon$ are in F_n.

  Then $\alpha - \delta = \lambda(\varepsilon - \delta), \lambda \in \mathbb{R}$, with

$$\lambda = \pm\frac{|\alpha - \delta|}{|\varepsilon - \delta|} = \pm\frac{|\beta - \gamma|}{|\varepsilon - \delta|}.$$

  Let

$$F_{n+1} = F_n(|\beta - \gamma|) = F_n(\sqrt{s^2 + t^2}), \text{where } s = \beta_x - \gamma_x, t = \beta_y - \gamma_y \in F_n,$$
$$F_{n+2} = F_{n+1}(|\varepsilon - \delta|) = F_{n+1}(\sqrt{u^2 + v^2}), \text{where } u = \varepsilon_x - \delta_x, v = \varepsilon_y - \delta_y \in F_n.$$

  Then $\lambda \in F_{n+2}$. As $\alpha = a + ib = \delta + \lambda(\varepsilon - \delta)$, $a, b \in F_{n+2}$, and the induction is done.

  In particular, if $\alpha = a + ib \in \mathcal{P} = \mathbb{P} \cap \mathbb{R}$, then $b = 0, \alpha = b \in F_n$, where $\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{R}$ and there are $a_i, b_i \in F_{i-1}$ such that $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$, $i = 1, \ldots, n$.

(b) By the Mathematical notes, if $a, b \in \mathcal{P}$, then $\sqrt{a^2 + b^2} \in \mathcal{P}$, so $\mathcal{P}$ is a Pythagorean subfield of $\mathbb{R}$.

  Let K any Pythagorean subfield of $\mathbb{R}$, and take any $\alpha \in \mathcal{P}$. By part (a), there exists a sequence of subfields of $\mathbb{R}$,

$$\mathbb{Q} = F_0 \subset \ldots \subset F_n \subset \mathbb{R},$$

  such that $\alpha \in F_n$, and for $i = 1, \ldots, n$ there are $a_i, b_i \in F_{i-1}$ such that $F_i = F_{i-1}\left(\sqrt{a_i^2 + b_i^2}\right)$. As any subfield of $\mathbb{R}$, K contains $\mathbb{Q}$, so $F_0 = \mathbb{Q} \in K$.

  By induction, suppose that $F_{i-1} \subset K$ for some integer $i, 1 \leq i \leq n$. Then $F_i = F_{i-1}(\sqrt{a_i^2 + b_i^2})$, where $a_i, b_i \in F_{i-1} \subset K$. As K is Pythagorean, $\sqrt{a_i^2 + b_i^2} \in K$, so $F_i \subset K$, and the induction is done.

  So $F_n \subset K$, and $\alpha \in F_n$, so $\alpha \in K$. Hence $\mathcal{P} \subset K$, so $\mathcal{P}$ is the smallest Pythagorean subfield of $\mathbb{R}$.

□

Ex. 10.1.9 *Show that the lune illustrated in the Historical Notes has the same area as the triangle AOB in the illustration.*

Proof. Let $l = OA = OB$ be the side of the triangle OAB, and $A = l^2/2$ the area of this triangle.

The area of the semicircle with diameter AB is

$$A_1 = \frac{\pi}{4} l^2.$$

The area of the quarter circle with radius $0A$ is $\frac{\pi}{4} l^2$, so the area between the arc AB and the chord AB is

$$A_2 = \frac{\pi}{4} l^2 - A.$$

Therefore the area of the lune, the shaded region of the figure in historical notes, is

$$A_1 - A_2 = \frac{\pi}{4} l^2 - \left(\frac{\pi}{4} l^2 - A \right) = A,$$

so is this area is the area $A = l^2/2$ of the triangle. □

Ex. 10.1.10 *The quadratrix is the curve $y = x \cot(\pi x/2)$ for $0 < x \leq 1$. In this problem, you will use this curve to square the circle and trisect the angle.*

(a) Show that $2/\pi = \lim_{x \to 0^+} x \cot(\pi x/2)$, i.e., the quadratrix meets the y axis at $y = 2/\pi$. We will follow Hippias and include this point in the curve.

(b) Show that we can square the circle starting from 0 and 1 and and constructing new points using $C1, C2, P1, P2$, or $P3$, together with the intersections of constructible lines with the quadratrix.

(c) A point (a, b) on the quadratrix determines an angle θ as pictured below (see fig. in Cox p. 269). Prove that $\theta = \pi a/2$.

(d) Suppose that we are given an angle $0 < \theta < \pi/2$. Prove that we can trisect θ starting from 0,1, and θ and constructing new points using $C1, C2, P1, P2$, or $P3$, together with the intersections of constructible lines with the quadratrix.

(e) Explain how the method of part (d) can be adapted to trisect arbitrary angles.

(f) Using the quadratrix, what else can you do to angles besides trisecting them?

Proof. (a) For all $x \in]0, \pi]$,

$$x \cot\left(\frac{\pi x}{2}\right) = \frac{2}{\pi} \frac{\frac{\pi x}{2}}{\sin\left(\frac{\pi x}{2}\right)} \cos\left(\frac{\pi x}{2}\right).$$

As $\lim_{u \to 0} \frac{\sin u}{u} = 1$ and $\lim_{u \to 0} \cos(u) = 1$, then

$$\lim_{x \to 0} x \cot\left(\frac{\pi x}{2}\right) = \frac{2}{\pi}.$$

(b) We say that a point $z = x + iy \in \mathbb{C}$, where $x, y \in \mathbb{R}$, is Hippias-constructible if there is a finite sequence of straightedge-and-compass constructions using $C1, C2, P1, P2$ and $P3$ that ends with α and begins with the set of points $0, 1$, together with the points $\beta = x + iy$, were (x, y) lies in the graph of the quadratrix, $(0, 2/\pi)$ included. Let $\mathbb{H}$ be the set of Hippias-constructible points. Then by Section 10.1, $\mathbb{H}$ is a subfield of $\mathbb{C}$, and $\mathcal{C}$ is a subfield of $\mathbb{H}$.

As $(0, 2/\pi)$ is on the quadratrix, $(2/\pi)i \in \mathbb{H}$. Since i is constructible and since $\mathbb{H}$ is a field, $2/\pi \in \mathbb{H}$, so $\pi/2$ and π are in $\mathbb{H}$. Then the proof of Theorem 10.1.4 shows that $\sqrt{\pi} \in \mathbb{H}$. If $r \in \mathbb{R}_+^*$ is a constructible number and the radius of a circle C, then $\sqrt{\pi}r \in \mathbb{H}$, so we can square every constructible circle with the quadratrix.

(c) As $M = (a, b)$ is on the quadratrix, $b = a\cot(\pi a/2)$. By definition, θ is a measure of the angle $(\widehat{\overrightarrow{OM}, \vec{e}_2})$ (where $\vec{e}_2 = (0, 1)$), then

$$\frac{b}{a} = \cot\theta = \cot\left(\frac{\pi}{2}a\right).$$

If $\theta = 0$, then $a = 0$. Since the restriction $\cot :]0, \pi/2] \to [0, +\infty[$ is strictly decreasing, hence is injective, and $\theta \in]0, \pi/2]$, $\frac{\pi}{2}a \in]0, \pi/2]$, then

$$\theta = \frac{\pi}{2}a, \qquad 0 \leq 1 \leq a.$$

(d) Let l a line containing the origin O, and (a, b) the intersection of l with the quadratrix. As in part (c),

$$\frac{b}{a} = \cot\theta = \cot\left(\frac{\pi}{2}a\right).$$

Let (c, d) be the point on the quadratrix corresponding with the angle $\theta/3$. Then

$$\frac{d}{c} = \cot\left(\frac{\theta}{3}\right) = \cot\left(\frac{\pi}{2}c\right),$$

therefore, as in part (c), $\frac{\theta}{3} = \frac{\pi}{2}c$, so

$$c = \frac{a}{3}.$$

Starting from the line l, the quadratrix and the points $0, 1$, We can construct with straightedge-and-compass $M = (a, b)$, and $c = a/3$ by the construction of Section 10.1, Figure 1, thus we can construct $M' = (c, d)$ at the intersection of the quadratrix and the vertical line passing through $(c, 0)$, and this gives the constructive line $l' = OM'$ corresponding to the angle $\theta/3$. So we can trisect every angle $(\widehat{\overrightarrow{OM}, \vec{e}_2})$, with measure $\theta,\ 0 < \theta < \pi/2$.

(e) Using construction given in Exercise 2 (a), we can transport with straightedge-and-compass constructions any given angle determined by α, β, γ (with measure $\theta,\ 0 < \theta < \pi/2$) on a congruent angle $(\widehat{\overrightarrow{OM}, \vec{e}_2})$. The inverse transport gives the trisection of the given angle. If $\pi/2 \leq \theta \leq \pi$ (obtuse angle), then we can trisect the constructive angle with measure $\theta - \pi/2$, the add the constructive angle with measure $\pi/6$. So we can trisect arbitrary angle with the quadratrix.

(f) In the reasoning of parts(d) and (e), we can replace $\theta/3$ by θ/n, where n is any positive integer. So we can divide any angle in n parts with the quadratrix. Thanks to the quadratrix!

□

Ex. 10.1.11 *Explain how the points of intersection of the parabolas $y = x^2$ and $x = y^2$ enable one to duplicate the cube. Your explanation should include a picture.*

Proof. Let (a, b) the intersection point (other than (0,0)) at the intersection of the two parabolas $y = x^2$ and $x = 2y^2$. Then $a^2 = b, a = 2b^2$. Multiplying these two equalities, we obtain

$$a^3 = 2b^3.$$

The volume of the cube with side a is twice the volume of the cube of side b. □

Ex. 10.1.12 *The spiral of Archimedes is the curve whose polar equation is $r = \theta$.*

(a) Explain how the spiral and $\theta = \pi/2$ enable one to square the circle.

(b) Given an angle θ_0, explain how the spiral enables one to trisect θ_0.

Proof. (a) If $M = (x, y)$ is a point of the spiral of Archimedes, then

$$r = \sqrt{x^2 + y^2} = \theta.$$

If $\theta = \pi/2$, then $x = 0, y > 0$, so $y = \pi/2$. So $\pi/2$ and π is constructible, if we add the spiral of Archimede to the starting of the construction, and also $\sqrt{pi}$ by Section 10.1. So the spiral of Archimedes enable one to square the circle.

(b) If $0 < \theta_0 < \pi$, let $M = (a, b)$ the corresponding point on the spiral, so

$$r = \sqrt{a^2 + b^2} = \theta_0.$$

We can obtain by the geometric construction of Section 10.1 the real number $r' = r/3$. Let C the circle with center 0 and radius $r' = r/3$. The intersection of C with the spiral gives is the point $M' = (\cos(\theta/3), \sin(\theta/3))$, so the measure of the angle $\widehat{\vec{e}_1, \overrightarrow{OM'}}$ is $\theta_0/3$. So the spiral enables one to trisect θ_0.

□

10.2 REGULAR POLYGONS AND ROOTS OF UNITY

Ex. 10.2.1 *Suppose that $2^k + 1$ is an odd prime. Prove that k is a power of 2.*

Proof. Let $N = 2^k + 1,\ k \geq 1$ an odd prime. Suppose that there exists an odd divisor q of k, so $k = ql$. Since q is odd,

$$2^k + 1 = 2^{ql} + 1 = (2^q + 1)(2^{q(l-1)} - 2^{q(l-2)} + \cdots - 2^q + 1) = (2^q + 1)\sum_{j=0}^{l-1}(-1)^j 2^{qj},$$

so $2^q + 1$ divides $2^k + 1$, and $1 \leq q \leq k$, hence $1 < 3 \leq 2^q + 1 \leq 2^k < 2^k + 1$, so $2^q + 1$ is a nontrivial divisor of $N = 2^k + 1$. Therefore N is composite: this is a contradiction.

Thus k has no odd divisor, so $k = 2^n$ for some integer n, and $N = 2^{2^n} + 1$ is a Fermat prime. □

Ex. 10.2.2 *Let p be prime. In Example 9.1.6, we showed that*

$$\Phi_{p^2}(x) = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^{2p} + x^p + 1.$$

The goal of this exercise is to prove that $\Phi_{p^2}(x)$ is irreducible over $\mathbb{Q}$ using only the Schönemann-Eisenstein criterion.

(a) Explain how the formulas of Example 9.1.6 imply that

$$(x+1)^{p^2} - 1 = ((x+1)^p - 1)\Phi_{p^2}(x+1).$$

(b) Let $\overline{\Phi}_{p^2}(x+1)$ be the reduction of $\Phi_{p^2}(x+1)$ modulo p. Show that

$$x^{p^2} = x^p\,\overline{\Phi}_{p^2}(x+1).$$

(c) Show that $\Phi_{p^2}(x+1)$ is irreducible over $\mathbb{Q}$ by the Schönemann-Eisenstein criterion. As in the proof of Proposition 4.2.5, this will imply that the same is true for $\Phi_{p^2}(x)$.

Lemma. If $0 < k < p^2$, then $p \mid \binom{p^2}{k}$.

Proof. Write $\nu_p(n)$ (or $\mathrm{ord}_p(n)$) the exponent of p in the prime decomposition of the positive integer n. Then, for all positive integer N,

$$\nu_p(N!) = \sum_{i=1}^{\infty} \left\lfloor \frac{N}{p^i} \right\rfloor = \left\lfloor \frac{N}{p} \right\rfloor + \left\lfloor \frac{N}{p^2} \right\rfloor + \cdots .$$

where the sum ends when $p^i > N$ (see a proof of this formula in Ireland-Rosen Exercise 2.6 on github.com/RichardGanaye/Ireland-Rosen).

Note that the $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ if $p^k > n$, so the sum is finite.

Suppose that $0 < k < n$. Then

$$\begin{aligned}
\nu_p\left(\frac{p^2}{k}\right) &= \sum_{i=1}^{2} \left(\left\lfloor \frac{p^2}{p^i} \right\rfloor - \left\lfloor \frac{p^2-k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor \right) \\
&= p - \left\lfloor \frac{p^2-k}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor + 1 - \left\lfloor \frac{p^2-k}{p^2} \right\rfloor - \left\lfloor \frac{k}{p^2} \right\rfloor \\
&= p + 1 - \left\lfloor p - \frac{k}{p} \right\rfloor - \left\lfloor \frac{k}{p} \right\rfloor .
\end{aligned}$$

Moreover, for all real a, b, $\lfloor a \rfloor + \lfloor b \rfloor \leq a + b$, and $\lfloor a \rfloor + \lfloor b \rfloor \in \mathbb{Z}$, hence

$$\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor,$$

therefore

$$\left\lfloor p - \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p} \right\rfloor \leq p,$$

so

$$\nu_p\left(\frac{p^2}{k}\right) \geq 1,$$

thus $p \mid \binom{p^2}{k}$.

□

Proof. (Ex 10.2.2)

(a) As in Example 9.1.6, using Proposition 9.1.5, we obtain

$$x^p - 1 = \Phi_1(x)\Phi_p(x) \quad \text{and} \quad x^{p^2} - 1 = \Phi_1(x)\Phi_p(x)\Phi_{p^2}(x).$$

Thus

$$x^{p^2} - 1 = (x^p - 1)\Phi_{p^2}(x).$$

The substitution $x \to x + 1$ gives

$$(x+1)^{p^2} - 1 = ((x+1)^p - 1)\Phi_{p^2}(x+1).$$

(b) We know that $p \mid \binom{p}{k},\ 1 \leq k \leq p-1$, and by Lemma, $p \mid \binom{p^2}{k},\ 1 \leq k \leq p^2 - 1$, so

$$(x+1)^p - 1 \equiv x^p \pmod{p} \quad \text{and} \quad (x+1)^{p^2} - 1 \equiv x^{p^2} \pmod{p}.$$

The reduction modulo p of the equality proved in part (a) gives

$$x^{p^2} = x^p\, \overline{\Phi}_{p^2}(x+1).$$

(c) As $\overline{\Phi}_{p^2}(x+1) = x^{p^2-p}$, all the the coefficients of $\Phi_{p^2}(x+1)$ are divisible by p, except the leading coefficient. Moreover $\Phi_{p^2}(1) = p$, so the constant coefficient of $\Phi_{p^2}(x+1)$ is not divisible by p^2, so the Schönemann-Eisenstein criterion shows that $\Phi_{p^2}(x+1)$ is irreducible over $\mathbb{Q}$, and this is equivalent to the irreducibility of $\Phi_p(x)$ over $\mathbb{Q}$.

□

Ex. 10.2.3 *Using only Proposition 4.2.5, Theorem 10.1.12, and Exercise 1, show that ζ_p is constructible if and only if p is a Fermat prime.*

Proof. Here we suppose that p is an odd prime.

The splitting field of Φ_p over $\mathbb{Q}$ is $L = \mathbb{Q}(\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p)$. As $\Phi_p(\zeta_p) = 0$, and as $\Phi_p(x)$ is irreducible over $\mathbb{Q}$ (Proposition 4.2.5), Φ_p is the minimal polynomial of ζ_p over $\mathbb{Q}$, hence

$$[L : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \deg(\Phi_p) = p - 1.$$

- Suppose that p is a Fermat prime, so $p = 2^n + 1$, where $n = 2^k, k \in \mathbb{N}$. Then $[L : \mathbb{Q}] = 2^n$, where L is the splitting field of Φ_p over $\mathbb{Q}$. By the authorized Theorem 10.1.12, ζ_p is constructible.

- Conversely, if we suppose that ζ_p is constructible, by the same Theorem 10.1.12, $[L : \mathbb{Q}] = 2^n$ for some integer $n \geq 0$, so $p = 2^n + 1$. As p is prime, by Exercise 1, $p = 2^k,\ k \in \mathbb{N}$, so $= 2^{2^k} + 1$ is a Fermat prime.

Conclusion: if p is an odd prime, ζ_p is constructible if and only if p is a Fermat prime. □

Ex. 10.2.4 *Prove that*

$$(\zeta_n)^{\frac{n}{m}} = \zeta_m$$

when $m \mid n,\ m > 0$, *and use this to conclude that if* ζ_n *is constructible and* $m \mid n,\ m > 0$, *then* ζ_m *is constructible.*

Proof.

- Suppose that $m \mid n,\ m > 0$. Since n/m is an integer,

$$(\zeta_n)^{\frac{n}{m}} = \left(e^{\frac{2\pi i}{n}}\right)^{\frac{n}{m}} = e^{\frac{n}{m}\frac{2\pi i}{n}} = e^{\frac{2\pi i}{m}} = \zeta_m.$$

- If ζ_n is constructible, and $m \mid n, m > 0$, by part (a)

$$\zeta_m = (\zeta_n)^{\frac{n}{m}}$$

is a power of ζ_n.

As the set of constructible points is a subfield of $\mathbb{C}$, ζ_m is constructible.

□

Ex. 10.2.5 *Suppose that* $n = 2^s p_1 \cdots p_r$, *where* $p_1, \ldots, p_r$ *are distinct Fermat primes. Then* ζ_{p_i} *is constructible by Exercise 3.*

(a) Show that ζ_{2^s} *is constructible.*

(b) Assume that ζ_a, ζ_b *are constructible and* $\gcd(a, b) = 1$. *Prove that* ζ_{ab} *is constructible.*

(c) Conclude that ζ_n *is constructible, since* $\zeta_{2^s}, \zeta_{p_1}, \ldots, \zeta_{p_r}$ *are.*

Proof. (a) The minimal polynomial of ζ_{2^s} over Q is $\Phi_{2^s}(x)$, and

$$\deg(\Phi_{2^s}(x)) = \phi(2^s) = 2^{s-1}(2-1) = 2^{s-1}.$$

Therefore $[\mathbb{Q}(\zeta_s) : \mathbb{Q}] = \deg(\Phi_{2^s}(x)) = 2^{s-1}$ is a power of 2. Since $\mathbb{Q}(\zeta_{2^s})$ is the splitting field of $\Phi(\zeta_{2^s})$ over $\mathbb{Q}$, by Theorem 10.1.12, ζ_{2^s} is constructible.

Note 1. Since $x^{2^s} - 1 = \Phi_1(x)\Phi_2(x)\cdots\Phi_{2^{s-1}}(x)\Phi_{2^s}(x) = (x^{2^{s-1}} - 1)\Phi_{2^s}(x)$, we see that $\Phi_{2^s}(x) = x^{2^{s-1}} + 1$.

Note 2. Without Theorem 10.1.12, we can prove that ζ_{2^s} is constructible more geometrically by constructing a 2^s-gon. $\zeta_2 = -1$ is constructible. Reasoning by induction, suppose that $\zeta_{2^{s-1}}$ is constructible. Since $(\zeta_{2^s})^2 = \zeta_{2^{s-1}}$, ζ_{2^s} is the intersection point of the circle $C(0,1)$ with the constructible bisector of the angle determined by $0, 1, \zeta_{2^{s-1}}$, so is constructible.

(b) Since $\gcd(a, b) = 1$, there exists $u, v \in \mathbb{Z}$ such that $ua + vb = 1$.

Then $\frac{v}{a} + \frac{u}{b} = \frac{1}{ab}$, thus

$$\zeta_a^v \zeta_b^u = e^{2\pi i\left(\frac{v}{a} + \frac{u}{b}\right)} = e^{\frac{2\pi i}{ab}} = \zeta_{ab}.$$

So $\zeta_{ab} = \zeta_a^v \zeta_b^u$, product of constructible numbers, is constructible.

(c) We show first that two distinct Fermat primes $F_n = 2^{2^n} + 1, F_m = 2^{2^m} + 1,\ n < m$ are relatively prime. By reductio ad absurdum, suppose that a prime q divides F_n and F_m. Then $2^{2^n} \equiv -1 \pmod{q}$, and

$$-1 \equiv 2^{2^m} \equiv (2^{2^n})^{2^{m-n}} \equiv (-1)^{2^{m-n}} \equiv 1 \pmod{q}.$$

Therefore $q \mid 2$, so $q = 2$, but this is impossible since F_n is odd.

So $n \neq m \Rightarrow \gcd(F_n, F_m) = 1$.

Since since $\zeta_{2^s}, \zeta_{p_1}, \ldots, \zeta_{p_r}$ are constructible, and $2^s, p_1, p_r$ are relatively prime, by part (b), $\zeta_{2^s p_1}, \zeta_{2^s p_1 p_2}, \ldots, \zeta_{2^s p_1 \cdots p_r} = \zeta_n$ are constructible.

Conclusion: if $p_1, \ldots, p_r$ are Fermat primes, and $n = 2^s p_1 \cdots p_r$, then ζ_n is constructible. □

Ex. 10.2.6 *Now suppose that ζ_n is constructible for some $n > 2$. The goal of this exercise is to prove that p is an odd prime dividing n, then p is a Fermat prime and $p^2 \nmid n$. This and Exercise 5 will give a proof of Theorem 10.2.1 that doesn't require knowing that $\Phi_n(x)$ is irreducible for arbitrary n.*

(a) Let p be an odd prime dividing n. Use Exercises 3 and 4 to show that p is a Fermat prime.

(b) Now assume that p is an odd prime and $p^2 \mid n$. Use Exercise 4 to show that ζ_{p^2} is constructible. Then use Theorem 10.1.12 and Exercise 2 to obtain a contradiction.

Proof. (a) If p is an odd prime factor of n, then by Exercise 4, $\zeta_p = (\zeta_n)^{n/p}$ is constructible, so p is a Fermat prime by Exercise 3.

(b) Assume that p is an odd prime and $p^2 \mid n$.

By Exercise 4, $\zeta_{p^2} = (\zeta_n)^{n/p^2}$ is then constructible. The splitting field of ζ_{p^2} over $\mathbb{Q}$ is $L = \mathbb{Q}(\zeta_{p^2})$. As Φ_{p^2} is irreducible, by Exercise 2,

$$[L : \mathbb{Q}] = \deg(\Phi_{p^2}) = p(p-1).$$

By Theorem 10.1.12, ζ_{p^2} being constructible, $[L : \mathbb{Q}] = p(p-1)$ is a power or 2, so p is a power of 2 , where p is an odd prime. This is a contradiction.

Conclusion: if ζ_n is constructible, then $n = 2^s p_1 \cdots p_r$, where $p_1, \ldots, p_r$ are distinct Fermat primes.

□

Ex. 10.2.7

Proof. $F_0 = 2^{2^0} + 1 = 3, F_1 = 2^{2^1} + 1 = 5, F_2 = 2^{2^2} + 1 = 17, F_3 = 2^{2^3} + 1 = 257, F_4 = 2^{2^4} + 1 = 65537$.

$3, 5, 17$ are well-known primes.

Since $3^{(F_3-1)/2} = 3^{128} \equiv -1 \pmod{257}$, and $3^{(F_4-1)/2} = 3^{32768} \equiv -1 \pmod{65537}$, the order of [3] is $2^{2^n} = F_n - 1$ in $(\mathbb{Z}/F_n\mathbb{Z})^*$ for $n = 3, 4$, so the Lucas test proves that F_3, F_4 are prime numbers.

(Thanks to SAGE for the numerical results.) □

Ex. 10.2.8 *Use* $\log_{10}(F_{33}) \approx 2^{33}\log_{10}(2)$ *to estimate the number of digits in the decimal expansion of* F_{33}*. The do the same for* $F_{2478782}$*.*

Proof. The number of digits in the decimal expansion of F_{33} is

$$\lfloor \log_{10}(F_{33}) \rfloor \approx 2^{33}\log_{10}(2) = 2,585,827,972.$$

(2.6 gigabytes in the RAM of my computer.)
The number of digits in the decimal expansion of $F_{2478782}$ is

$$\lfloor \log_{10}(F_{2478782}) \approx 2^{2478782}\log_{10}(2) \approx 1.634 \times 10^{746187}.$$

(my computer is not so big!) □

10.3 ORIGAMI(OPTIONAL)

Ex. 10.3.1 *This exercise will use the diagram of page 284 to prove that the origami construction described at the beginning of the section trisects the angle* θ *formed by the line* l_2 *and the bottom of the square.*

(a) Let Q *be the intersection of the line segments* $\overline{P_1Q_2}$ *and* $\overline{P_2Q_1}$*. Prove that* Q *lies on the dashed line* l*.*

(b) Prove that θ *is congruent to* $\alpha + \beta$*.*

(c) Use triangles $\triangle P_1PQ_1$ *and* $\triangle P_2PQ_1$ *to prove that* β *and* γ *are congruent.*

(d) Use triangle $\triangle P_1QQ_1$ *to prove that* α *is congruent to* $\beta + \gamma$*.*

(e) Conclude that α *is congruent to* $2\theta/3$ *and that the angle formed by* $\overline{P_1Q_1}$ *and the bottom of the square is* $\theta/3$*.*

Proof. (a) The dashed line l is the fold of the sheet that applies P_1 on Q_1 and P_2 on Q_2. Let s the reflection (orthogonal symmetry) with regard to the line l.

Then $s(P_2) = Q_2$, and $s(Q_1) = P_1$, so s applies the line $\overline{P_2Q_1}$ on the line $\overline{P_1Q_2}$. Let Q be the intersection point of these two lines.

Then $s(Q)$ is on the images of these two lines, so

$$s(Q) \in s(\overline{P_1Q_2}) \cap s(\overline{P_2Q_1}) = \overline{P_2Q_1} \cap \overline{P_1Q_2} = \{Q\},$$

therefore $s(Q) = Q$.

Since the set of points M such that $s(M) = M$ is the line l, we conclude that $Q \in l$.

(b) Let D the point at the bottom right corner, and δ a measure of the angle $(\overrightarrow{P_1D}, \overrightarrow{P_1Q_1})$.

As $(\overrightarrow{P_1D}, \overrightarrow{P_1Q_1}) + (\overrightarrow{P_1Q_1}, \overrightarrow{P_1Q_2}) = (\overrightarrow{P_1D}, \overrightarrow{P_1Q_2})$, then $\theta = \delta + \alpha$.

Since PQ_1 and P_1D are parallel, $(\overrightarrow{P_1D}, \overrightarrow{P_1Q_1}) = (\overrightarrow{Q_1P}, \overrightarrow{Q_1P_1})$ (alternate interior angles), so $\beta = \delta$. We can deduce of these two equalities that

$$\theta = \alpha + \beta.$$

(c) The reflection r with regard to the line l_1 sends P_1 on P_2 and Q_1 on Q_1, therefore $Q_1P1 = Q_1P_2$, so the triangle $\triangle Q_1P_1P_2$ is isosceles, and

$$(\overrightarrow{Q_1P}, \overrightarrow{Q_1P_2}) = -(\overrightarrow{r(Q_1)r(P)}, \overrightarrow{r(P_1)r(Q_1)}) = -(\overrightarrow{Q_1P}, \overrightarrow{Q_1P_1}),$$

so the absolute value of the measures of these angles are the same, so

$$\beta = \gamma.$$

(d) The reflection s of part (a) sends Q on Q, and P_1 on Q_1, therefore $QP_1 = QQ_1$. The triangle $\triangle QP_1Q_1$ is isosceles, so the corresponding angles are equal:

$$-(\overrightarrow{P_1Q_1}, \overrightarrow{P_1Q}) = (\overrightarrow{Q_1P_1}, \overrightarrow{Q_1Q}) = (\overrightarrow{Q_1P_1}, \overrightarrow{Q_1P}) + (\overrightarrow{Q_1P}, \overrightarrow{Q_1Q}),$$

so

$$\alpha = \beta + \gamma.$$

(d) From $\delta = \beta$ and from the three equalities obtained in parts (b),(c),(d):

$$\begin{aligned} \theta &= \alpha + \beta, \\ \beta &= \gamma, \\ \alpha &= \beta + \gamma, \end{aligned}$$

we conclude that $\alpha = 2\beta$, $\theta = 3\beta = 3\delta$, so $\alpha = 2\theta/3$, and

$$\delta = \theta/3.$$

This means that the measure of the angle formed by the bottom of the square and $\overline{P_1Q_1}$ is $\theta/3$.

□

Ex. 10.3.2 *In the text we showed how to trisect an angle between $\pi/4$ and $\pi/2$ by origami.*

(a) Explain how to bisect and double angles by origami.

(b) Explain how to trisect an arbitrary angle by origami.

Proof.

(a) To bisect the same angle θ, we apply the same line l_2 on the bottom line. The fold is on the bisector of the angle. To double the angle, we fold the sheet along the line l_2. Then the bottom line goes on the line that makes a double angle with the bottom line.

(b) If the angle θ is between 0 and $\pi/4$, the angle $\theta' = \pi/2 - \theta$ is constructible by origami with the symmetry with regard to the bisector of the bottom left corner, and θ' is between $\pi/4$ and $\pi/2$, so we can trisect it, and we obtain the angle $\pi/6 - \theta/3$. As $\pi/6$ is origami-constructible by trisection of the angle $\pi/2$ (here $Q = P_2 = Q_2$) and as we can add or remove an origami-constructible angle, then so is the angle $\theta/3$.

If θ is between $\pi/2$ and π, Then $\theta'' = \pi - \theta$ is origami-constructible and between 0 and $\pi/2$, so we can trisect it. We obtain the angle $\pi/3 - \theta/3$, where $\pi/3$ is the double of the origami-constructible angle $\pi/6$, so the angle $\theta/3$ is also origami-constructible. □

Ex. 10.3.3 *Let P_1 be a point not lying on a line l_1 in the plane. Drop a perpendicular from P_1 to l_1 that meets l_1 at a point S. Then choose rectangular coordinates such that P_1 lies on the positive y-axis and the x-axis is the perpendicular bisector of the segment $\overline{P_1S}$. In this coordinate system, $P_1 = (0, a)$ and l_1 is defied by $y = -a$, where $a > 0$.*

(a) The parabola with focus P_1 and directrix l_1 is defined to be the set of all points Q that are equidistant from P_1 and l_1. Prove that it is defined by the equation $4ay = x^2$.

(b) Let $Q = (x_0, y_0)$ be a point on the parabola. Prove that the y-intercept of its tangent line is $-y_0$.

(c) Let $Q = (x_0, y_0)$ be a point on the parabola, and let $Q_1 \in l_1$ be obtained by dropping a perpendicular from Q. Prove that Q_1 is the reflection of P_1 about the tangent line to the parabola at Q.

(d) Part (c) proves one direction of Lemma 10.3.1. Prove the other direction to complete the proof of the lemma.

Proof. (a) Let $\mathcal{P}$ be the parabola with focus P_1 and directrix l_1.

With the chosen coordinates system, let $Q(x, y)$ a point in the plane, and Q_1 the orthogonal projection of Q on the directrix. Since $P_1(0, a)$ and $Q_1(x, -a)$,

$$\begin{aligned} Q \in \mathcal{P} &\iff QP_1^2 = QQ_1^2 \\ &\iff x^2 + (y-a)^2 = (y+a)^2 \\ &\iff x^2 + y^2 - 2ay + a^2 = y^2 + 2ay + a^2 \\ &\iff x^2 = 4ay \end{aligned}$$

So the equation of $\mathcal{P}$ is

$$\mathcal{P} : x^2 = 4ay.$$

(b) Let $Q(x_0, y_0)$ be a point on the parabola, so $x_0^2 = 4ay_0$.

Write $F(x, y) = x^2 - 4ay$. The equation of the tangent T to $\mathcal{P}$ at the point Q is given by

$$\begin{aligned} 0 &= \frac{\partial F}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial F}{\partial y}(x_0, y_0)(y - y_0), \\ 0 &= 2x_0(x - x_0) - 4a(y - y_0), \\ 2x_0x - 4ay &= 2x_0^2 - 4ay_0 = 4ay_0. \end{aligned}$$

So the equation of T is

$$T : x_0x - 2ay = 2ay_0.$$

Let $R(x_R, y_R)$ the intersection point of T with the y-axis.

Then $x_R = 0$, so $-2ay_R = 2ay_0,\ y_R = -y_0$,

$$R(0, -y_0).$$

(c) Write $MN = ||\overrightarrow{MN}||$ the length of the segment $\overline{MN}$.

$$P_1(0,a), \quad R(0,-y_0), \quad Q_1(x_0,-a), \quad Q(x_0,y_0), \quad (a>0, y_0>0),$$

thus $\overrightarrow{P_1R} = (0,-a-y_0) = \overrightarrow{QQ_1}$, hence $P_1R = QQ_1$. By definition of the parabola, $QP_1 = QQ_1$, so

$QP_1 = y_0 + a = \sqrt{x_0^2 + (y_0-a)^2} = RQ_1$, therefore

$$QP_1 = QQ_1 = P_1R = RQ_1 :$$

(Q, P_1, R, Q_1) is a rhombus, whose length of side is $c = a + y_0$. Hence the diagonals (P_1Q_1) and $T = (QR)$ are perpendicular. We give a direct proof: as $\overrightarrow{P_1R} = \overrightarrow{QQ_1}$,

$$\begin{aligned}
\overrightarrow{QR} \,.\, \overrightarrow{P_1Q_1} &= (\overrightarrow{QP_1} + \overrightarrow{P_1R}) \,.\, (\overrightarrow{P_1Q} + \overrightarrow{QQ_1}) \\
&= \overrightarrow{QP_1} \,.\, \overrightarrow{P_1Q} + \overrightarrow{QP_1} \,.\, \overrightarrow{QQ_1} + \overrightarrow{P_1R} \,.\, \overrightarrow{P_1Q} + \overrightarrow{P_1R} \,.\, \overrightarrow{QQ_1} \\
&= -c^2 + \overrightarrow{QP_1}(\overrightarrow{QQ_1} - \overrightarrow{P_1R}) + c^2 \\
&= 0
\end{aligned}$$

As in any parallelogram, the intersection of the diagonals is the middle point of (P_1, Q_1) and (Q, R), so Q_1 is the reflection of P_1 about the tangent line to the parabola at Q.

(d) Conversely, let $Q_1(x_0, -a)$ be any point on the directrix l_1, and l the bisection of (P_1, Q_1). We must prove that l is tangent to the parabola $\mathcal{P}$. Let $M(x, y)$ a point of the plane. With $P_1(0, a)$, and $Q_1(x_0, -a)$,

$$\begin{aligned}
M \in l &\iff MP_1^2 = MQ_1^2 \\
&\iff x^2 + (y-a)^2 = (x-x_0)^2 + (y+a)^2 \\
&\iff x^2 + y^2 - 2ay + a^2 = x^2 - 2x_0x + x_0^2 + y^2 + 2ay + a^2 \\
&\iff x_0x - 2ay = \frac{x_0^2}{2}
\end{aligned}$$

If we write $y_0 = \frac{x_0^2}{4a}$, then the point $M_0(x_0, y_0)$ lies on the parabola $\mathcal{P}$. Since $x_0^2 - 2ay_0 = \frac{x_0^2}{2}$, M_0 lies also on l. By part (b), the equation of the tangent T at point M_0 is $x_0x - 2ay_0 = 2ay_0 = x_0^2/2$, hence $T = l$, so l is tangent to the parabola $\mathcal{P}$.

Conclusion: the reflexion of P_1 about l lies on the directrix l_1 if and only if l is tangent to the parabola with focus P_1 and directrix l_1.

□

Ex. 10.3.4 *Show that the tangent line at a point (x_1, y_1) on the first parabola in (10.9) has slope given by*

$$m = \frac{b}{y_1 - \frac{1}{2}a}.$$

Proof. The equation of the tangent T at the point $M_1(x_1, y_1)$ to the parabola whose equation is

$$f(x,y) = 2bx - \left(y - \frac{1}{2}a\right)^2 = 0,$$

is

$$\begin{aligned} 0 &= \frac{\partial f}{\partial x}(x_1,y_1)(x-x_1) + \frac{\partial f}{\partial y}(x_1,y_1)(y-y_1), \\ &= 2b(x-x_1) - 2\left(y_1 - \frac{1}{2}a\right)(y-y_1), \end{aligned}$$

so the equation of T is

$$T : bx - \left(y_1 - \frac{1}{2}a\right)y - bx_1 + \left(y_1 - \frac{1}{2}a\right)y_1 = 0.$$

So the slope of T is

$$m = \frac{b}{y_1 - \frac{1}{2}a}.$$

□

Ex. 10.3.5 *In the text we showed that the slopes of the simultaneous tangents to the parabolas in (10.9) are roots of (10.12). In this exercise, you will give an origami version of this in the special case when $a = 2$ and $b = 1$. Begin with a square sheet of paper folded so that the bottom edge touches the top. This fold will be the positive x-axis, and the left edge of the sheet will be the directrix for the first parabola in (10.9).*

(a) Describe the origami moves one would use to construct the foci and directrices of the parabolas in (10.9) when $a = 2$ and $b = 1$. Also construct the y-axis. Exercise 7 will be helpful.

(b) Now perform an origami move that takes the focus of each parabola to a point on the corresponding directrix . Explain why there is only one way to do this.

(c) Part (b) gives a line whose slope m is the real root of $x^3 + 2x + 1$. Explain what origami moves you would use to find the point on the x-axis whose coordinates are $(m, 0)$.

Proof. As the discriminant of $f(x) = x^3 + 2x + 1$ ($p = 2, q = 1$) is $\Delta_f = -4p^3 - 27q^2 = -59 < 0$, there is a unique real root. First we compute this real root α with Cardano's method. There exists a pair of complex numbers u, v such that

$$u + v = \alpha, \qquad uv = -\frac{2}{3}$$

(the roots of $y^2 - \alpha y - \frac{2}{3}$).

Since $2 + 3uv = 0$,

$$\begin{aligned} 0 &= \alpha^3 + 2\alpha + 1 \\ &= u^3 + v^3 + 1 + (2 + 3uv)(u + v) \\ &= u^3 + v^3 + 1 \end{aligned}$$

So u^3, v^3 satisfy

$$-1 = u^3 + v^3$$
$$-\frac{8}{27} = u^3 v^3$$

Therefore u^3, v^3 are the roots of $y^2 + y - \frac{8}{27}$:

$$\{u^3, v^3\} = \left\{ \frac{1}{18}\sqrt{177} - \frac{1}{2}, \quad -\frac{1}{18}\sqrt{177} - \frac{1}{2} \right\}.$$

Thus

$$\alpha = \sqrt[3]{\frac{1}{18}\sqrt{177} - \frac{1}{2}} - \sqrt[3]{\frac{1}{18}\sqrt{177} + \frac{1}{2}},$$

which is equal to

$$\alpha = \sqrt[3]{\frac{1}{18}\sqrt{177} - \frac{1}{2}} - \frac{2}{3\sqrt[3]{\frac{1}{18}\sqrt{177} - \frac{1}{2}}} \approx -0.4534.$$

(a) By Exercise 7, the focus and directrix of $\mathcal{P}_1 : (y-1)^2 = 2x$ are

$$F_1\left(\frac{1}{2}, 1\right), \qquad D_1 : x = -\frac{1}{2},$$

and the focus and directrix of $\mathcal{P}_2 : y = \frac{x^2}{2}$ are

$$F_2\left(0, \frac{1}{2}\right), \qquad D_2 : y = -\frac{1}{2}.$$

As all the points have rational coordinates, and the lines rational coefficients, they are constructible by origami. More precisely, take two arbitrary points on the x-axis to represent $(0,0)$ and $(1,0)$. For instance the middle point of the sheet, obtained by folding the paper so that the left edge touches the right, represent the origin, and the fold is then the y axis. A second fold so that the right edge touches the y-axis gives an intersection point with the x-axis which we take as the point $(1,0)$.

We obtain similarly the point $(0,1)$ and dividing by 2 with horizontal and vertical folds, we obtain F_1, D_1, F_2, D_2.

(b) As seen in part (a), the discriminant of $x^3 + 2x + 1$ is $\Delta_f = -59 < 0$, the equation (10.12) $m^3 + am + b = 0$, where $a = 2, b = 1$, has a unique real solution α. As the slope of a commune tangent to the parabolas $\mathcal{P}_1, \mathcal{P}_2$ is a root of this equation, the slope of such a tangent is $m = \alpha$. Since the intersection point $M_1(x_1, y_1)$ of the tangent with the parabola $\mathcal{P}_1$ satisfies (10.10)

$$x_1 = \frac{b}{2m^2}, \qquad y_1 = \frac{b}{m} + \frac{a}{2}$$

this intersection point is determined by $m = \alpha$, and similarly the tangent point $M_2(x_2, y_2)$ with $\mathcal{P}_2$ is uniquely determined by

$$x_2 = m, \qquad y_2 = \frac{m^2}{2},$$

so there is at most one common tangent to the two parabolas, and at most one way to take the focus of each parabola to a point on the corresponding directrix.

Conversely, we must prove the existence of a common tangent.

Let D the line of slope α passing by $M_2(x_2, y_2)$, with $(x_2, y_2) = (\alpha, \frac{\alpha^2}{2})$. The equation of D is given by $y - \frac{\alpha^2}{2} = \alpha(x - \alpha)$, so

$$D : -\alpha x + y + \frac{\alpha^2}{2}.$$

D contains $M_1(x_1, y_1)$, where $(x_1, y_1) = (\frac{1}{2\alpha^2}, 1 + \frac{1}{\alpha})$, since

$$-\alpha\left(\frac{1}{2\alpha^2}\right) + 1 + \frac{1}{\alpha} + \frac{\alpha^2}{2} = \frac{1}{2\alpha}(\alpha^3 + 2\alpha + 1) = 0.$$

By Example 10.3.2 and Exercise 4, the slope of the tangent T_1 to $\mathcal{P}_1$ at M_1 is $m = \frac{b}{y_1 - \frac{1}{2}a} = \alpha$, and the slope of the tangent T_2 to $\mathcal{P}_2$ at M_2 is $m = x_2 = \alpha$, so $D = T_1 = T_2$, therefore D is tangent to $\mathcal{P}_1$ and $\mathcal{P}_2$. This proves the existence of one common tangent D to the two parabolas, with equation

$$D : -\alpha x + y + \frac{\alpha^2}{2}.$$

Conclusion : there is exactly one way to take the focus of each parabola to a point on the corresponding directrix.

(c) Let F_2' be the reflexion of the focus F_2 of $\mathcal{P}_2$ about the common tangent D. By Exercise 3, the line (M_2F_2) is parallel to the y-axis, so the abscissa of F_2' is

$$x_2 = m.$$

A vertical fold is obtained by the perpendicular line tho the horizontal fold passing by F_2. The intersection of this fold with the x-axis gives the point $(m, 0)$, with $m \approx -0.45$

(Another method consists to construct the parallel to the tangent D passing by the origin. The intersection of this parallel with the line $x = 1$ gives the point $(1, m)$.) □

Ex. 10.3.6 *Supose that in the situation of C3, we have points $\alpha_1 \neq \alpha_2$ not lying on lines $l_1 \neq l_2$. Also assume that l_1 and l_2 are parallel and that there is a line l satisfying C3 (i.e., l reflects α_i to a point of l_i for $i = 1, 2$). Prove that the distance between l_1 and l_2 is at most the distance between α_1 and α_2. This makes it easy to find examples where the line described in C3 does not exist.*

Proof. Suppose that l reflects α_1 to $\beta_1 \in l_1$ and α_2 to $\beta_2 \in l_2$.

Let $d = d(l_1, l_2)$ the distance between l_1 and l_2. If γ is the orthogonal projection of β_1 on l_2, then by definition, $d = |\beta_1 - \gamma|$. By Pythagoras Theorem,

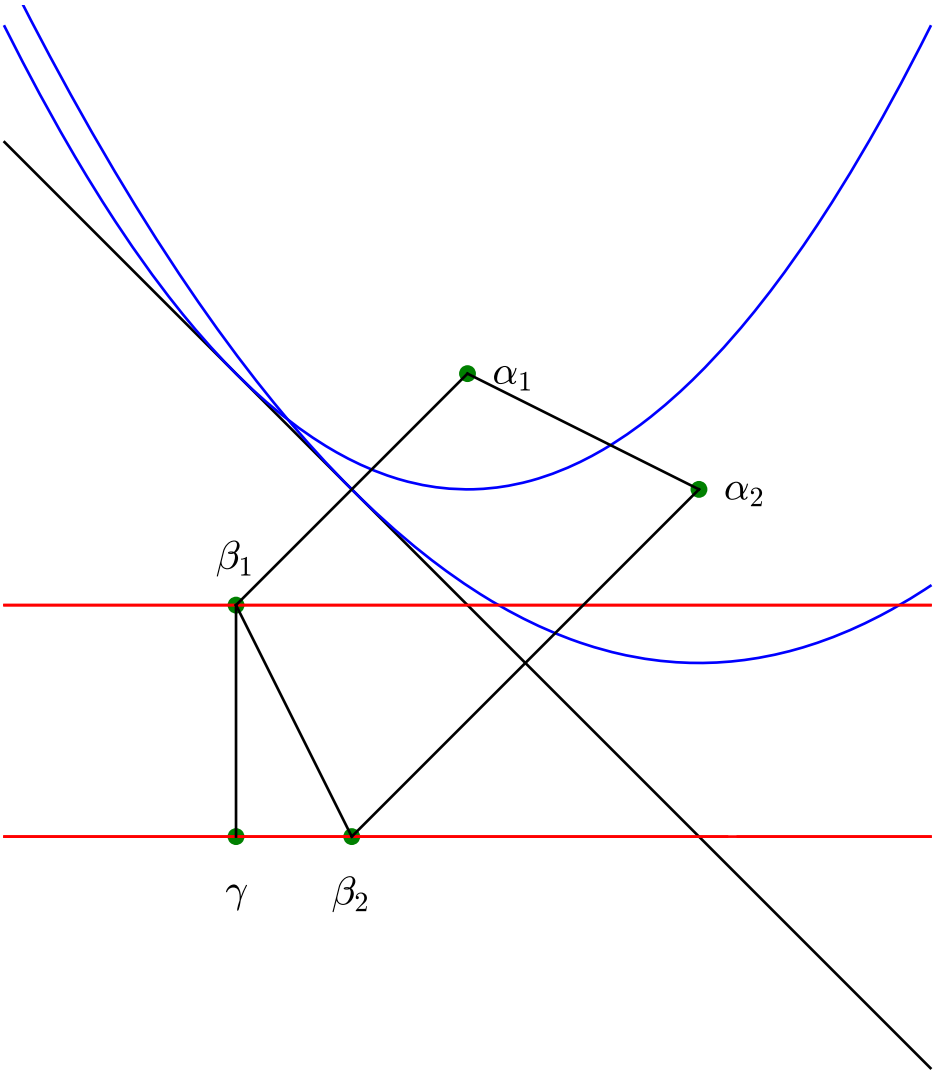
$$|\beta_1 - \gamma|^2 + |\gamma - \beta_2|^2 = |\beta_1 - \beta_2|^2.$$

Therefore $d^2 = |\beta_1 - \gamma|^2 \leq |\beta_1 - \beta_2|^2$, so

$$d \leq |\beta_1 - \beta_2|.$$

Moreover the the reflexion about l preserves the distances between points, so

$$|\beta_1 - \beta_2| = |\alpha_1 - \alpha_2|.$$

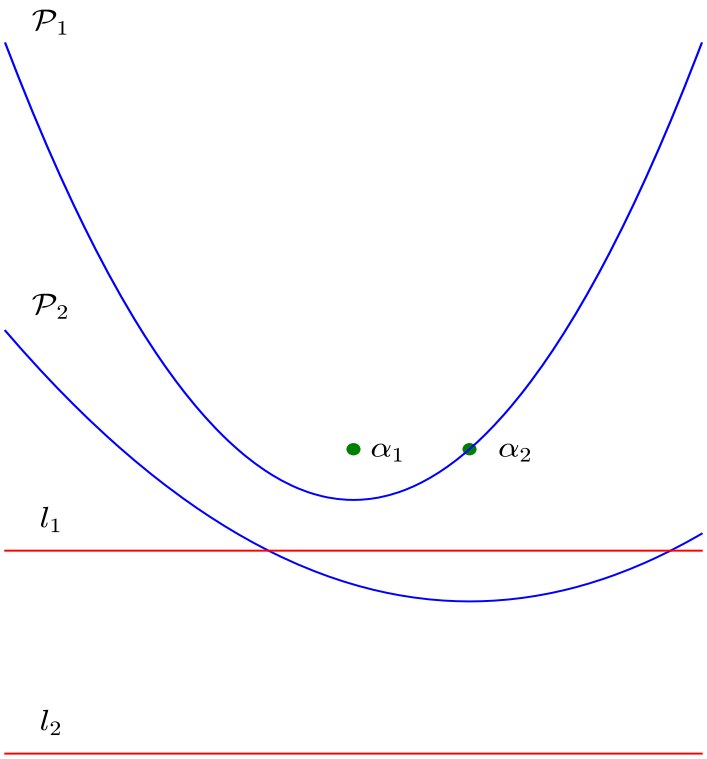

α_1
α_2
β_1
γ
β_2

To conclude, the distance d between l_1 and l_2 is at most the distance between α_1 and α_2.

For instance, let l_1 be the line with equation $y = 0$, l_2 with equation $y = -2$, $\alpha_1 = i, \alpha_2 = 1 + i$. Then $d = d(l_1, l_2) = 2 > |\alpha_1 - \alpha_2|$, so there is no line l that reflects α_1 on a point on l_1 and α_2 on a point on l_2. In other words, there is no common tangent to the two parabolas with focus α_i and directrix l_i, $i = 1, 2$, with equations

$$\mathcal{P}_1 : y = \frac{1}{2}(x^2 + 1)$$
$$\mathcal{P}_2 : y = \frac{1}{6}(x^2 - 2x - 2)$$

(see figure). □



Ex. 10.3.7 *Consider the parabolas* $\left(y - \frac{1}{2}a\right)^2 = 2bx$ *and* $y = \frac{1}{2}x^2$ *from (10.9).*

(a) Show that the first parabola has focus $\left(\frac{1}{2}b, \frac{1}{2}a\right)$ *and directrix* $x = -\frac{1}{2}b$.

(b) Show that the second parabola has focus $\left(0, \frac{1}{2}\right)$ *and directrix* $y = -\frac{1}{2}$.

Hence the focus and directrix of the first parabola are defined over any subfield of $\mathbb{R}$ *containing* a *and* b. *For the second, this is true over any subfield of* $\mathbb{R}$.

Proof.

(a) Let $\mathcal{P}_1$ the parabola with focus $F\left(\frac{1}{2}b, \frac{1}{2}a\right)$ and directrix $D : x = -\frac{1}{2}b$. Let $M(x, y)$ a point of the plane and $H(-\frac{1}{2}b, y)$ the orthogonal projection of M on D. Then

$$\begin{aligned} M(x,y) \in \mathcal{P}_1 &\iff MF^2 = MH^2 \\ &\iff \left(x - \frac{b}{2}\right)^2 + \left(y - \frac{a}{2}\right)^2 = \left(x + \frac{b}{2}\right)^2 \\ &\iff \left(y - \frac{a}{2}\right)^2 = 2bx \end{aligned}$$

So the first parabola $\left(y - \frac{1}{2}a\right)^2 = 2bx$ has focus $\left(\frac{1}{2}b, \frac{1}{2}a\right)$ and directrix $x = -\frac{1}{2}b$.

(b) Let $\mathcal{P}_2$ the parabola with focus $F\left(0, \frac{1}{2}\right)$ and directrix $D : x = -\frac{1}{2}$. Let $M(x, y)$ a point of the plane and $H(0, -\frac{1}{2})$ the orthogonal projection of M on D. Then

$$\begin{aligned} M(x,y) \in \mathcal{P}_2 &\iff MF^2 = MH^2 \\ &\iff x^2 + \left(y - \frac{1}{2}\right)^2 = \left(y + \frac{1}{2}\right)^2 \\ &\iff x^2 = 2y \end{aligned}$$

So the second parabola $y = x^2/2$ has focus $\left(0, \frac{1}{2}\right)$ and directrix $y = -\frac{1}{2}$. □

Ex. 10.3.8 *Complete the proof of Theorem 10.3.6 sketched in the text.*

Theorem 10.3.6 *Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$ and let $\mathbb{Q} \subset L$ be the splitting field of the minimal polynomial of α over $\mathbb{Q}$. Then α is an origami number if and only if $[L : \mathbb{Q}] = 2^a 3^b$ for some integer $a, b \geq 0$.*

Proof. We first prove that $\mathbb{Q} \subset \mathcal{O}$ is a normal extension. Let $\alpha \in \mathcal{O}$, and let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. By Theorem 10.3.4, there are subfields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbb{C}$$

such that $\alpha \in F_n$ and $[F_i : F_{i-1}] = 2$ or 3 for $1 \leq i \leq n$.

By Exercise 10.1.7, there exists a Galois closure $\mathbb{Q} \subset M$ of $\mathbb{Q} \subset F$ such that $M \subset \mathbb{C}$, so $\mathbb{Q} \subset F_n \subset M \subset \mathbb{C}$ and $\mathbb{Q} \subset M$ is a Galois extension. Note that f splits completely in M, since M is normal over $\mathbb{Q}$, f is irreducible over $\mathbb{Q}$, and $\alpha \in F_n \subset M$ is a root of f.

Now let $\beta \in M$ be any root of f. By Proposition 5.1.8, there is $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ such that $\sigma(\alpha) = \beta$. Applying σ to the fields $\mathbb{Q} = F_0 \subset \cdots \subset F_n \subset M$ gives

$$\mathbb{Q} \subset \sigma(\mathbb{Q}) = \sigma(F_0) \subset \cdots \subset \sigma(F_n)$$

such that $[\sigma(F_i) : \sigma(F_{i-1}] = [F_i : F_{i-1}] = 2$ or 3 for all i.

By Theorem 10.3.4, $\beta = \sigma(\alpha) \in \sigma(F_n)$ is an origami number, so $\beta \in \mathcal{O}$, so we can conclude that $\mathbb{Q} \subset \mathcal{O}$ is a normal extension.

- Suppose that $\alpha \in \mathcal{O}$ and let $\mathbb{Q} \subset L$ be the splitting field of the minimal polynomial f of α over $\mathbb{Q}$. Since $\mathbb{Q} \subset \mathcal{O}$ is normal, $L \subset \mathcal{O}$. By the theorem of the Primitive Element, we have $L = \mathbb{Q}(\gamma)$ for some $\gamma \in L$. Since $\gamma \in \mathcal{O}$, there are subfields

  $$\mathbb{Q} = F'_0 \subset F'_1 \subset \cdots \subset F'_{n-1} \subset F'_m \subset \mathbb{C}$$

  such that $\gamma \in F_m$ and $[F'_i : F'_{i-1}] = 2$ or 3 for $1 \leq i \leq m$.

  As $\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset F'_m$, by the Tower Theorem,

  $[L : \mathbb{Q}] = [\mathbb{Q}(\gamma) : \mathbb{Q}]$ divides $[F'm : \mathbb{Q}] = 2^u 3^v,\ u, v \in \mathbb{N}$, so

$$[L:\mathbb{Q}] = 2^a 3^b \text{ for some integer } a, b \geq 0.$$

- Conversely, suppose that $[L:\mathbb{Q}] = 2^a 3^b$ for some integer $a, b \geq 0$.

  Since $\mathbb{Q} \subset L$ is Galois, then $G = \mathrm{Gal}(L/\mathbb{Q})$ satisfies $|G| = [L:\mathbb{Q}]$ is of the form

  $$|G| = 2^a 3^b.$$

  By Burnside's $p^n q^m$ Theorem (Theorem 8.1.8), G is solvable., so we have subgroups

  $$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = G = \mathrm{Gal}(L/\mathbb{Q})$$

  such that G_i is normal in G_{i-1} of index 2 or 3, since $|G| = 2^a 3^b$. The Galois Correspondence Theorem gives

  $$\mathbb{Q} = L_{G_0} \subset L_{G_1} \subset \cdots \subset L_{G_m} = L,$$

  where $[L_{G_i} : L_{G_{i-1}}] = 2$ or 3 for all i.

  By Theorem 10.3.4, $\alpha \in L$ is an origami number.

□

Ex. 10.3.9 *Prove Corollary 10.3.9.*

Corollary 10.3.9 *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree ≤ 4. Then the roots of $f(x)$ are origami numbers, i.e, we can solve $f(x) = 0$ by origami.*

Proof. Let α be a root of $f(x)$, with $d = \deg(f) \leq 4$.

Let L be the splitting field of α.

Recall that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of S_4, so

$$|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] \text{ divides } 4!.$$

So $[L:\mathbb{Q}]$ divides $4! = 2^3 \times 3$, therefore $[L:\mathbb{Q}] = 2^a 3^b$ for some a, b with $0 \leq a \leq 3,\ 0 \leq b \leq 1$. By Theorem 10.3.6 and Exercise 8, α is an origami number.

□

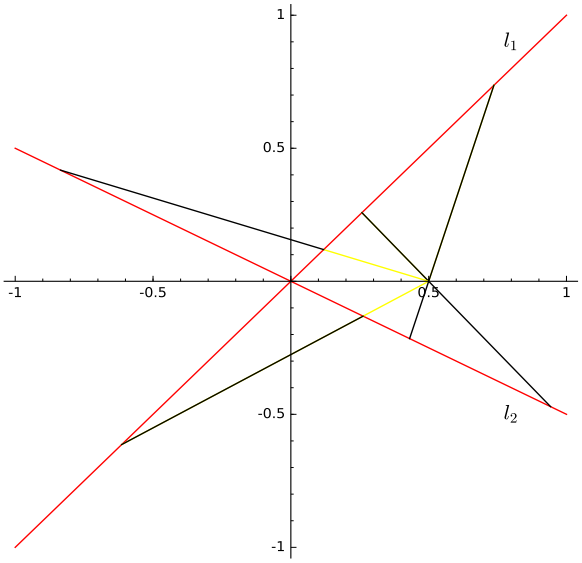
Ex. 10.3.10 *In Example 10.3.10, prove that l meets l_1 and l_2 at the points Q_1 and Q_2 given in (10.13) and (10.14). Also draw the four lines whose slopes are the roots of (10.15).*

Proof. The equation of the line l with slope m through $P = (\frac{1}{2}, 0)$ is

$$l : y = m\left(x - \frac{1}{2}\right).$$

The intersection point (x_1, y_1) of l with $l_1 : y = x$ is given by the system

$$\begin{aligned} y_1 &= x_1 \\ y_1 &= m\left(x_1 - \frac{1}{2}\right) \end{aligned}$$



which gives $x_1 = m\left(x_1 - \frac{1}{2}\right)$, $2x_1 = 2mx_1 - m$, so

$$Q_1 = (x_1, y_1) = \left(\frac{m}{2m-2}, \frac{m}{2m-2}\right).$$

The intersection point (x_2, y_2) of l with $l_2 : y = -\frac{1}{2}x$ is given by the system

$$\begin{aligned} y_2 &= -\frac{1}{2}x_2 \\ y_2 &= m\left(x_2 - \frac{1}{2}\right) \end{aligned}$$

which gives $-\frac{1}{2}x_2 = m\left(x_2 - \frac{1}{2}\right)$, so

$$Q_2 = (x_2, y_2) = \left(\frac{m}{2m+1}, -\frac{m}{2(2m-2)}\right).$$

Therefore

$$\begin{aligned} Q_1Q_2 = 1 &\iff 1 = (x_2 - x_1)^2 + (y_2 - y_1)^2 \\ &\iff 1 = \left(\frac{m}{2m+1} - \frac{m}{2m-2}\right)^2 + \left(-\frac{m}{2(2m+1)} - \frac{m}{2m-2}\right)^2 \\ &\iff 1 = m^2\left[\left(\frac{2}{4m+2} - \frac{1}{2m-2}\right)^2 + \left(\frac{1}{4m+2} + \frac{1}{2m-2}\right)^2\right] \\ &\iff 1 = \frac{m^2}{(4m+2)^2(2m-2)^2}\left\{[(2(2m-2) - (4m+2)]^2 + [2m-2+4m+2]^2\right\} \\ &\iff (4m+2)^2(2m-2)^2 = m^2(36 + 36m^2) \\ &\iff 16(2m+1)^2(m-1)^2 = 36m^2(1+m^2) \\ &\iff 4(2m+1)^2(m-1)^2 = 9m^2(1+m^2) \\ &\iff 16m^4 - 16m^3 - 12m^2 + 8m + 4 = 9m^4 + 9m^2 \\ &\iff 7m^4 - 15m^3 - 21m^2 + 8m + 4 = 0 \end{aligned}$$

We obtain the four slopes and the figure with the following SAGE instructions:

```
m = var('m')
p = 7*m^4-16*m^3-21*m^2+8*m+4
l = solve(p,m)
sols = [eq.right() for eq in l]
slopes = [sol.n() for sol in sols]; slopes
```

```
[-1.06517627861170, -0.312773186089791, 0.551041848035361, 3.11262190238042]
```

```
P = (1/2,0)
g = plot(x,x,xmin,xmax,color = 'red')
g += plot(-1/2*x,x,xmin,xmax, color = 'red')
for m in slopes:
    x1,x2 = m/(2*m-2),m/(2*m+1)
    Q1,Q2 = (x1,x1),(x2,-1/2*x2)
    g += line([Q1,P], color = 'yellow')
    g += line([Q1,Q2], color = 'black')

texte1 = text("$l_1$",(0.8,0.9), fontsize=15, rgbcolor=(0,0,0))
texte2 = text("$l_2$",(0.8,-0.5), fontsize=15, rgbcolor=(0,0,0))
g += texte1 + texte2
g.show(aspect_ratio=1)
g.save('marquedRulers.pdf',aspect_ratio=1,xmin=-1,xmax=1,ymin=-1,ymax=1)
```

□

Ex. 10.3.11 *This exercise will give an example of a cubic equation that arises from verging. Consider the lines l_1 defined by $y = 0$ and l_2 defined by $y = x$ and verge from $P = (1, \frac{1}{2})$ using a marked ruler. Show that this gives the vertical line $x = 1$ together with three nonvertical lines whose slopes m satisfy the cubic equation*

$$4m^3 + m^2 - 4m + 1 = 0.$$

Also show that the nonvertical lines cannot be constructed by straightedge and compass.

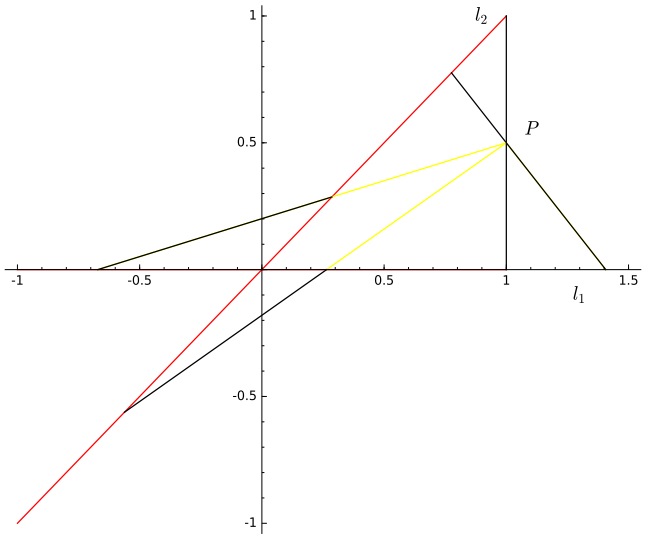
Proof. Here a solution is the vertical line $x = 1$, corresponding to $m = \infty$, since the intersection of this line with l_1 and l_2 are the points $Q_1 = (1, 0), Q_2 = (1, 1)$ such that $Q_1Q_2 = 1$.

Any nonvertical line l with slope m through $P = (1, \frac{1}{2})$ has an equation

$$l : y - \frac{1}{2} = m(x - 1).$$

The intersection point of l with $l_1 : y = 0$ and the intersection of l with $l_2 : y = x$ are the points

$$Q_1 = (x_1, y_1) = \left(\frac{2m-1}{2m}, 0\right),$$
$$Q_2 = (x_2, y_2) = \left(\frac{2m-1}{2m-2}, \frac{2m-1}{2m-2}\right)$$



Therefore

$$\begin{aligned}
Q_1Q_2 = 1 &\iff 1 = (x_2 - x_1)^2 + (y_2 - y_1)^2 \\
&\iff 1 = \left(\frac{2m-1}{2m-2} - \frac{2m-1}{2m}\right)^2 + \left(\frac{2m-1}{2m-2}\right)^2 \\
&\iff (2m-1)^2 \left[\left(\frac{2}{2m(2m-2)}\right)^2 + \frac{1}{(2m-2)^2}\right] \\
&\iff 1 = \frac{(2m-1)^2}{(2m-2)^2}\left(\frac{1}{m^2} + 1\right) \\
&\iff 4m^2(m-1)^2 = (2m-1)^2(m^2+1) \\
&\iff 4m^4 - 8m^3 + 4m^2 = 4m^4 - 4m^3 + 5m^2 - 4m + 1 \\
&\iff 4m^3 + m^2 - 4m + 1 = 0
\end{aligned}$$

Let $f(x) = 4x^3 + x^2 - 4x + 1$, then

$$\lim_{x\to-\infty} f(x) = -\infty, \quad f\left(-\frac{2}{3}\right) = \frac{79}{27} > 0, \quad f\left(\frac{1}{2}\right) = -\frac{1}{4} < 0, \quad \lim_{x\to+\infty} f(x) = +\infty.$$

Therefore $f(x)$ has three real roots

$$m_1 \approx 0.2991, m_2 \approx -1.2290, m_3 \approx 0.6799.$$

This gives 4 solutions with $m = \infty$. (see figure.)

$f(x)$ has no rational root. Indeed , if $\alpha = \frac{p}{q}, p, q \in \mathbb{Z}, q > 0, p \wedge q = 1$ is a root of f, then $4p^3 + p^2q - 4pq^2 + q^3 = 0$, so $p^3 \mid 1, q^3 \mid 2$, therefore $p = \pm 1, q = 1$, so $\alpha = \pm 1$, but neither 1 nor -1 is a root of f. Since$\deg(f) = 3$, f is irreducible over $\mathbb{Q}$ and the minimal polynomial of m_1, m_2 or m_3 over $\mathbb{Q}$ is f.

Let $L = \mathbb{Q}(m_1) = \mathbb{Q}(m_1, m_2, m_3)$ the splitting field of f. The discriminant of f is $\Delta_f = 316 = 2^2 \times 79$, where 79 is prime, so Δ_f is not a square in $\mathbb{Q}$, so $\mathrm{Gal}(L : \mathbb{Q}) \simeq S_3$, therefore $[L : \mathbb{Q}] = 6$ is not a power of 2, so m_1, m_2, m_3 are not constructible numbers. Therefore the nonvertical lines are not constructible by straightedge and compass. □

Ex. 10.3.12 *Prove that $\angle PRO = \theta/3$ in the construction (10.18).*

Proof. Let $\alpha = \angle PRO$. Since $QR = QO = 1$, $\triangle QRO$ is isosceles, so $\angle QOR = \alpha$. Therefore the extern angle $\angle OQP = 2\alpha$. Since $OQ = OP = 1$, $\triangle OPQ$ is isosceles, so

$$\angle OQP = \angle OPQ = 2\alpha.$$

Therefore $\angle QOP = \pi - 4\alpha$. Since $\angle ROQ + \angle QOP + \theta = \pi$, $\alpha + (\pi - 4\alpha) + \theta = \pi$, so $\theta = 3\alpha$,

$$\angle PRO = \frac{\theta}{3}.$$

□

Ex. 10.3.13 *According to [15] (G.E.Martin, Geometric Constructions), Pappus used a marked ruler to trisect angles as follows. Given an angle $0 < \theta < \pi/2$, write it as $\theta = \angle POA$, where:*

- *The distance between P and O is $1/2$.*
- *The line l_1 determined by P and A is perpendicular to the line determined by O and A.*

Any angle $0 < \theta < \pi/2$ can be put in this form by a marked-ruler construction. Finally, let l_2 be the line through P that is perpendicular to l_1. Then verging with O and the lines l_1 and l_2 gives points $Q \in l_1$ and $R \in l_2$ such that Q and R are one unit apart.

Prove that $\angle QOA = \theta/3$.

Proof. As $OP = \frac{1}{2}$, $P = \left(\frac{1}{2}\cos\theta, \frac{1}{2}\sin\theta\right)$, and $A = \left(\frac{1}{2}\cos\theta, 0\right)$. The vertical line is not a solution. The equation of every nonvertical line l with slope m passing through Q is

$$l : y = mx,$$

where $m = \tan\alpha$ and $\alpha \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ is a measure of $\angle AOR$. The equations of l_1, l_2 are

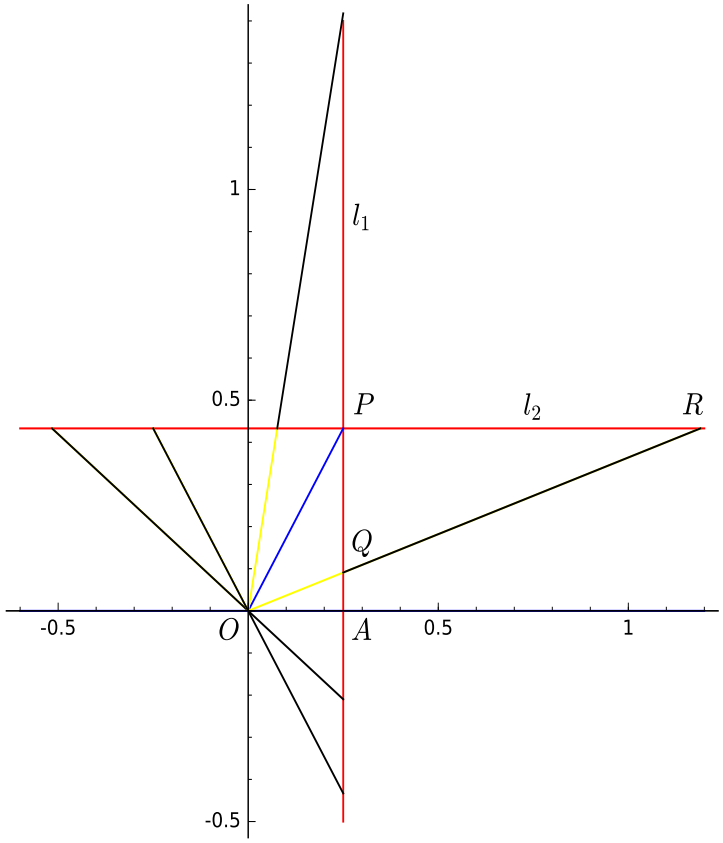
$$l_1 : x = \frac{1}{2}\cos\theta,$$
$$l_2 : y = \frac{1}{2}\sin\theta.$$

The intersection point $Q = (x_1, y_1)$ of l with l_1 is given by

$$x_1 = \frac{1}{2}\cos\theta,$$
$$y_1 = m\frac{1}{2}\cos\theta,$$

and the intersection point R of l with l_2 is given by

$$x_2 = \frac{1}{2m}\sin\theta,$$
$$y_2 = \frac{1}{2}\sin\theta.$$


1
0.5
-0.5
-0.5
0.5
1
l_1
l_2
P
R
Q
O
A

Therefore

$$\begin{aligned}
QR = 1 &\iff 1 = (x_2 - x_1)^2 + (y_2 - y_1)^2 \\
&\iff 1 = \left(\frac{1}{2m}\sin\theta - \frac{1}{2}\cos\theta\right)^2 + \left(\frac{1}{2}\sin\theta - m\frac{1}{2}\cos\theta\right)^2 \\
&\iff 1 = \frac{1}{4m^2}(sin\theta - m\cos\theta)^2 + \frac{1}{4}(\sin\theta - m\cos\theta)^2 \\
&\iff 4m^2 = (sin\theta - m\cos\theta)^2(m^2+1) \\
&\iff 0 = \left(\sin\theta - m\cos\theta - \frac{2m}{\sqrt{m^2+1}}\right)\left(\sin\theta - m\cos\theta + \frac{2m}{\sqrt{m^2+1}}\right)
\end{aligned}$$

Note that, since $m = \tan\alpha$,

$$\frac{2m}{\sqrt{m^2+1}} = \frac{2\,\frac{\sin\alpha}{\cos\alpha}}{\sqrt{\frac{\sin^2\alpha}{\cos^2\alpha}+1}} = 2\sin\alpha.$$

Moreover

$$\sin\theta - m\cos\theta = \sin\theta - \frac{\sin\alpha}{\cos\alpha}\cos\theta = \frac{\sin(\theta-\alpha)}{\cos\alpha}.$$

Therefore

$$\begin{aligned}
QR = 1 &\iff 0 = \left(\frac{\sin(\theta-\alpha)}{\cos\alpha} - 2\sin\alpha\right)\left(\frac{\sin(\theta-\alpha)}{\cos\alpha} + 2\sin\alpha\right) \\
&\iff 0 = (\sin(\theta-\alpha) - \sin(2\alpha))(\sin(\theta-\alpha) + \sin(2\alpha)) \\
&\iff \sin(\theta-\alpha) = \pm\sin(2\alpha) \\
&\iff \theta - \alpha = 2\alpha - k\pi \quad \text{or} \quad \theta - \alpha = \pi - 2\alpha + k\pi \qquad (k \in \mathbb{Z}) \\
&\iff \alpha = \frac{\theta}{3} + k\frac{\pi}{3} \quad \text{or} \quad \alpha = \pi - \theta + k\pi \qquad (k \in \mathbb{Z}).
\end{aligned}$$

Since $0 < \theta < \frac{\pi}{2}$ and $-\frac{\pi}{2} < \alpha < \frac{\pi}{2}$, we obtain finally

$$QR = 1 \iff \alpha = \frac{\theta}{3} \quad \text{or} \quad \alpha = \frac{\theta+\pi}{3} \quad \text{or} \quad \alpha = \frac{\theta-\pi}{3} \quad \text{or} \quad \alpha = -\theta.$$

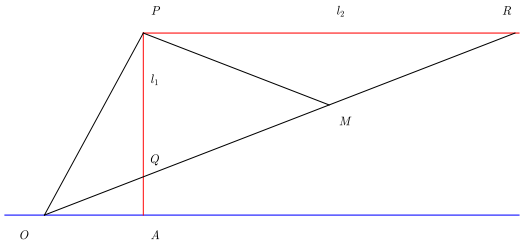
The only solution $0 < \alpha < \theta$ is $\alpha = \theta/3$.

In the example of the angle $\theta = 60^\circ = \pi/3$, where $\theta/3 = 20^\circ = \pi/9$ is not constructible by straightedge and compass, we obtain $\alpha \in \left\{\frac{\pi}{9}, \frac{4\pi}{9}, -\frac{2\pi}{9}, -\frac{\pi}{3}\right\}$, all constructible with the marked ruler (see figure). □

Solution 2

Proof. We follow the indication of David A. Cox and give the more geometric proof of [15] (G.E.Martin, Geometric Constructions):

"Let $\angle AOR$ have measure t. Then $\angle PRO$ has measure t. Let M be the midpoint of Q and R. Since $\angle RPQ$ is right, then P lies on the circle with diameter $\overline{RQ}$ by the converse of the Theorem of Thales. So $MQ = MP = MR = OP = 1/2$, and $\triangle MPR$ and $\triangle POM$ are isosceles triangles. Hence, $\angle MPR$ has measure t by the Pons Asinorum, $\angle OMP$ has measure $2t$ by the Exterior Angle Theorem, and $\angle POM$ has measure $2t$ by the Pons Asinorum. Therefore, $\overrightarrow{OR}$ trisects $\angle POA$." □



Ex. 10.3.14 *As explained in [21](C.R. Videla, On points constructible from conics), Pappus used intersections of conics to trisect angles as follows. Consider the unit circle centered at the origin, and let $0 < \theta < \pi/2$. Then $P = (\cos\theta, \sin\theta)$ is the corresponding point on the unit circle. We assume that P is known. Also let $O = (0,0)$ and set $A = (1,0)$. Thus $\theta = \angle POA$.*

(a) Consider the curve C consisting of all points $Q = (x,y)$ such that the distance from P to Q is twice the distance from Q to the y-axis. The curve C intersects the unit circle at a point R lying in the interior of $\angle POA$. Prove that $\angle ROA = \theta/3$.

(b) Show that the curve C is a hyperbola. It follows that we have trisected an angle using the intersection of a hyperbola and a circle, i.e., an intersection of conics.

Proof. (a) Let H the orthogonal projection of R on the x-axis, and S such that H is the midpoint of RS, so S is the reflection of R with regard to the x-axis. Since R is on the curve C,

$$PR = 2RA = RS,$$

therefore the measures of $\angle ROP$ and $\angle SOR$ are equal, and is twice the measure of $\angle AOP$, so $\overrightarrow{OR}$ trisects the angle $\angle POA$ and a measure of $\angle ROA$ is $\theta/3$.

(b) Let $Q = (x,y), H = (x,0), P = (\cos\theta, \sin\theta)$

$$\begin{aligned} Q \in C &\iff QP = 2QH \iff QP^2 = 4QH^2 \\ &\iff (x - \cos\theta)^2 + (y - \sin\theta)^2 = 4y^2 \\ &\iff x^2 - 3y^2 - 2x\cos\theta - 2y\sin\theta + 1 = 0 \end{aligned}$$

The discriminant of the quadratic form $ax^2 + bxy + cy^2 = x^2 - 3y^2$ is $\Delta = 12 > 0$, so C is not empty and C is a hyperbola.

□

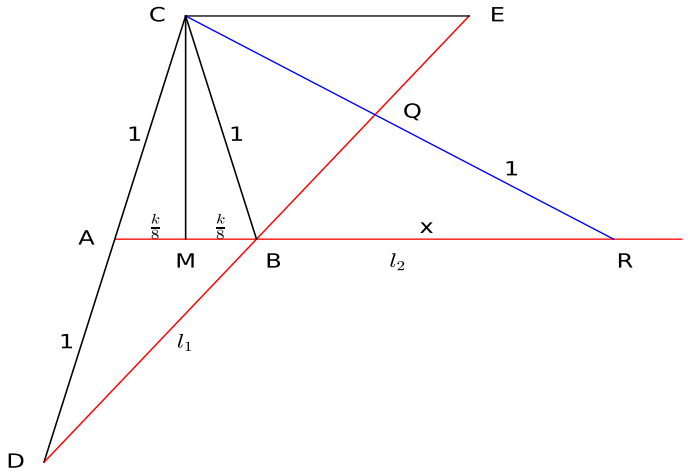
Ex. 10.3.15 *In this exercise, we discuss a marked-ruler construction of cube roots due to Nicomedes and taken from [15]. Let k be a real number such that $0 < k < 8$, and consider an isosceles triangle $\triangle ABC$ such that AC and BC have length 1 and AB has length $k/4$. Then extend AC and AB as indicated in the picture below, and choose D on the extension of AC so that AD also has length 1. Finally, draw the line through D and B.*

Verging from C with the lines l_1 and l_2 indicated above gives points $Q \in l_1$ and $R \in l_2$ that are one unit apart. Assume that $Q \neq D$.

(a) *Explain why the restriction* $0 < k < 8$ *is necessary.*

(b) *Prove that the distance between* B *and* R *is* $\sqrt[3]{k}$.

(c) *Explain how to give a marked-ruler construction for any* $k > 0$.



Proof.

(a) We suppose that $k \geq 0$. Let I be the midpoint of AB. As $\triangle ABC$ is isosceles, by Pythagoras' Theorem, $CI^2 + (k/8)^2 = AC^2 = 1$, therefore $0 \leq k/8 \leq 1$, so $k \leq 8$. If $k > 8$, there exists no point C with the conditions of the text. If $k = 8$, C is the midpoint of AB and $l_1 = l_2$, and if $k = 0$, $A = B$ and l_2 is not defined. The restriction $0 < k < 8$ is necessary.

(b) 2 solutions.

Solution 1. Personal solution with analytic geometry.

Take the origin in $O = M$, where M is the midpoint of AB, and take MB, MC as the x and y-axis. Write for simplicity $\lambda = MB = k/8, \mu = MC$, so $\lambda^2 + \mu^2 = 1$. The unknown is $x = \overline{BR}$.

The coordinates of A, B, C, D, R are

$$A \begin{vmatrix} -\lambda \\ 0 \end{vmatrix}, \quad B \begin{vmatrix} \lambda \\ 0 \end{vmatrix}, \quad C \begin{vmatrix} 0 \\ \mu \end{vmatrix}, \quad D \begin{vmatrix} -2\lambda \\ -\mu \end{vmatrix}, \quad R \begin{vmatrix} \lambda + x \\ 0 \end{vmatrix}.$$

Let $M = (X, Y)$ a point.

$$\begin{aligned} (X,Y) \in l_1 = (DB) &\iff 0 = \begin{vmatrix} X - x_B & x_B - x_D \\ Y - y_B & y_B - y_D \end{vmatrix} = \begin{vmatrix} X - \lambda & 3\lambda \\ Y & \mu \end{vmatrix} \\ &\iff \mu X + (\lambda + x)Y = 0. \end{aligned}$$

So the equation of (DB) is

$$(DB) : \mu x + (\lambda + x)Y = \mu(\lambda + x).$$

Similarly,

$$\begin{aligned}(X,Y) \in (CR) &\iff 0 = \begin{vmatrix} X - x_C & -(x_R - x_C) \\ Y - y_C & -(y_R - y_C) \end{vmatrix} = \begin{vmatrix} X & -(\lambda + x) \\ Y - \mu & \mu \end{vmatrix} \\ &\iff \mu(X - \lambda) - 3\lambda = 0.\end{aligned}$$

So the equation of (CR) is

$$(CR) : \mu x - 3\lambda Y = \lambda\mu.$$

The coordinates (x_Q, y_Q) are given by the system

$$\begin{aligned}\mu X - 3\lambda Y &= \lambda\mu \\ \mu X + (\lambda + x)Y &= \mu(\lambda + X)\end{aligned}$$

Since $\mu \neq 0$, this is equivalent to

$$\begin{aligned}(4\lambda + x)X &= 4\lambda(\lambda + x) \\ (4\lambda + x)Y &= \mu x,\end{aligned}$$

so

$$Q \begin{vmatrix} \frac{4\lambda(\lambda+x)}{4\lambda+x} \\ \frac{\mu x}{4\lambda+x} \end{vmatrix} \quad , \quad R \begin{vmatrix} \lambda + x \\ 0 \end{vmatrix} \quad .$$

Therefore

$$\begin{aligned}QR = 1 &\iff \left[\frac{4\lambda(\lambda + x)}{4\lambda + x} - (\lambda + x)\right]^2 + \left[\frac{\mu x}{4\lambda + x}\right]^2 \\ &\iff (4\lambda + x)^2 = (\lambda + x)^2 x^2 + \mu^2 x^2 \\ &\qquad\qquad = x^4 + 2\lambda x^3 + (\lambda^2 + \mu^2)x^2 \\ &\qquad\qquad = x^4 + 2\lambda x^3 + x^2 \\ &\iff x^4 + 2\lambda x^3 - 8\lambda x - 16\lambda^2 = 0 \\ &\iff (x + 2\lambda)(x^3 - 8\lambda) = 0 \\ &\iff \left(x + \frac{k}{4}\right)(x^3 - k) = 0\end{aligned}$$

As $Q \neq D, R \neq A$, so $x \neq -k/4$. Therefore

$$QR = 1 \iff x = \sqrt[3]{k}.$$

Note: the factorization is easy because $x = -2\lambda = -k/4$ gives the particular solution $R = A$.

The marked-ruler constructions of Pappus (for the trisection) and Nicomedes (for the cube root) give both a fourth degree equation with a known obvious solution.

Solution2. From [15] (G.E. Martin, Geometric Constructions):

" Let the parallel to (AB) that passes through C intersect (DB) at E. So $\triangle ABD$ and $\triangle CDE$ are similar. Then, since A bisects CD, we have $CE = 2AB = k/2$. Also, since $\triangle QBR$ and $\triangle QCE$ are similar, we have $(k/2)/CQ = BR/1$. With $x = BR$, then $CQ = k/(2x)$. With M the midpoint of A and B, by two aplications of the Pythagorean Theorem, we now have

$$\left(1 + \frac{k}{2x}\right)^2 = CR^2 = CM^2 + MR^2 = (CA^2 - AM^2) + MR^2$$
$$= 1^2 - \left(\frac{k}{8}\right)^2 + \left(x + \frac{k}{8}\right)^2$$

(So, multiplying the two members by 8^2x^2,

$$16(2x + k)^2 = 8^2x^2 - k^2x^2 + x^2(8x + k)^2$$
$$64x^2 + 64kx + 16k^2 = 64x^2 - k^2x^2 + 64x^4 + 16kx^3 + k^2x^2$$
$$0 = 64x^4 + 16kx^3 - 64kx - 16k^2$$
$$0 = 4x^4 + kx^3 - 4kx - k^2.)$$

Fortunately, this quartic easily factors as $(4x + k)(x^3 - k) = 0$. Since $4x + k > 0$, then we must have $x^3 - k = 0$. Therefore, x is the real cube root of k, as desired."

(c) If k is any positive number, let s an integer such that $0 < k < 2^{3s+3}$, so $0 < K < 8$, where $K = \frac{k}{2^{3s}}$. The Nicomedes' construction applied to K gives $\sqrt[3]{K}$, thus $\sqrt[3]{k} = 2^s\sqrt[3]{K}$ is constructible by marked-ruler. □

Ex. 10.3.16 *Let P be a point distance $b > 0$ from a line l. Put a marked ruler though P with one mark at $R \in l$. When R moves along l, the other mark Q_1 or Q_2 (depending on which side of l it is on) traces out the conchoid of Nicomedes.*

We can relate the conchoid to constructions problems as follows.

(a) Suppose we are given a point P and lines l_1, l_2, and assume that $P \notin l_1$. Prove that a point Q is obtained by verging with P and l_1, l_2 if and only if Q is one of the points of intersection of l_2 with the conchoid determined by P and l_1.

(b) Prove that the angle trisection of (10.18) can be interpreted as the intersection of the unit circle with the conchoid determined by P and l_1.

(c) Suppose that $P = (0, 0)$ and l is the horizontal line $y = -b$. Prove that the polar equation of the conchoid is

$$r = b\csc\theta \pm 1,$$

where the minus sign gives the portion of the curve above l and the plus sign gives the portion below.

(d) Under the assumptions of part (c), show that the Cartesian equation of the conchoid is

$$(x^2 + y^2)(y - b)^2 = y^2.$$

By part (a), verging is the same as intersecting the conchoid with a line. Since the above equation has degree 4, this explains why verging leads to an equation of degree 4.

Proof. (a) Let $Q \in l_2$. Then Q is obtained by verging with P and l_1, l_2 if and only if there is a point $R \in l_1$ such that $QR = 1$, if and only if R is on the conchoid.

(b) As $QR = 1$, with R on l, Q is on the conchoid determined by P and l, and on the unit circle, so Q is at the intersection of the unit circle and the conchoid.

(c) Here $P = (0, 0)$ and l is the horizontal line $y = -b$, in the Cartesian coordinates system $(P, \vec{e}_1, \vec{e}_2)$.

If R is any point on l, then $\overrightarrow{PR} = \rho\vec{u}$, where $\vec{u} = \cos\theta\,\vec{e}_1 + \sin\theta\,\vec{e}_2,\ 0 < \theta < \pi$, and $\rho = PM > 0$. The equation of the line $l_R = (PR)$ is

$$x \sin\theta - y\cos\theta = 0,$$

thus

$$R = \left(-b\,\frac{\cos\theta}{\sin\theta}, -b\right).$$

If C is the conchoid, and $Q = (x, y) = (r\cos\theta, r\sin\theta),\ r > 0, 0 < \theta < \pi$ any point of the line l_R, then

$$\begin{aligned}
Q \in C &\iff QR = 1 \\
&\iff 1 = \left(x + b\,\frac{\cos\theta}{\sin\theta}\right)^2 + (y + b)^2 \\
&\iff \left(r\cos\theta + b\frac{\cos\theta}{\sin\theta}\right)^2 + (r\sin\theta + b)^2 = 1 \\
&\iff \left(r + \frac{b}{\sin\theta}\right)^2 = 1 \\
&\iff r = \frac{-b}{\sin\theta} \pm 1 \quad (= -b\csc\theta \pm 1).
\end{aligned}$$

So the polar equation of the conchoid of Nicomedes is

$$r = \frac{-b}{\sin\theta} \pm 1, \qquad 0 < \theta < \pi,$$

where the sign gives the two portions of the curve.

(c) Any non horizontal line l_1 has an equation $x = py$, where $p = 0$ or $p = 1/m$, m being the slope of l_1. The intersection point R of l with l_1 is $R = (-pb, -b)$, so

$$\begin{aligned}
Q \in C &\iff \exists p \in \mathbb{R},\ Q \in l_1 \quad \text{and} \quad QR = 1 \\
&\iff \exists p \in \mathbb{R}, \quad \begin{cases} x &= py \\ 1 &= (x + pb)^2 + (y + b)^2 \end{cases} \\
&\iff (x, y) = (0, 0) \text{ or } \left(x + b\frac{x}{y}\right)^2 + (y + b)^2 = 1 \\
&\iff x^2(y + b)^2 + y^2(y + b)^2 = y^2 \\
&\iff (x^2 + y^2)(y + b)^2 = y^2
\end{aligned}$$

(The polar equation gives the same Cartesian equation. For $r \neq 0$,

$$\left(r + \frac{b}{\sin\theta}\right)^2 = 1 \iff (y + b)^2 = \sin^2\theta = \frac{y^2}{r^2}$$
$$\iff (x^2 + y^2)(y + b)^2 = y^2.)$$

The sign $-$ in the text seems to be a misprint, if the equation of l is $y = -b$ (correct if the equation of l is $y = b$). □

Ex. 10.3.17 *Let P a point on a circle, and consider a marked ruler that goes through P. If we place one mark on a point Q on the circle, then the other mark R_1 or R_2 traces out a curve called the limaçon of Pascal.*

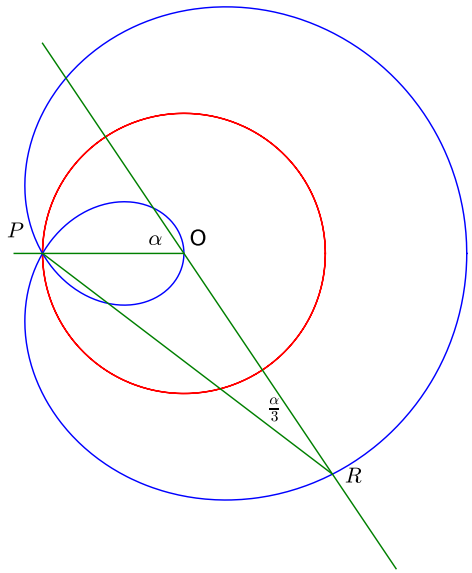
(a) Show that the angle trisection (10.18) can be interpreted as the intersection of the line l with the limaçon determined by the circle and the point P.

(b) Let $P = (0, 0)$ and let C be the circle of radius a and center $(a, 0)$. Show that the corresponding limaçon has polar equation

$$r = 1 + 2a\cos\theta.$$

(c) In the situation of part (b), show that the Cartesian equation of the limaçon is

$$(x^2 + y^2 - 2ax)^2 = x^2 + y^2.$$



Proof. (a) As $QR = 1$, where $Q \in C$ and R is on the line (PQ), $R \in l$ is by definition on the limaçon determined by P and C,

(b) Let $l_1 : y = mx$ be any nonvertical line passing through $P = (0, 0)$, with $m = \tan\theta$, $-\pi/2 < \theta < \pi/2$, so the measure of the angle between the x-axis and l_1 is θ. Let $Q = (x_Q, y_Q), Q \neq P$ be the intersection point of l_1 with C. Then $x_Q \neq 0$. (x_Q, y_Q) is solution of the system

$$\begin{aligned} y &= mx \\ a^2 &= (x - a)^2 + y^2 \end{aligned}$$

which gives

$$y_Q = mx_Q, \qquad 0 = x_Q\,[(m^2 + 1)x_Q - 2a],$$

with $x_Q \neq 0$, so

$$Q = \left(\frac{2a}{m^2+1}, \frac{2am}{m^2+1} \right).$$

Since $m = \tan\theta$,

$$Q = (2a\cos^2\theta, 2a\sin\theta\cos\theta) = (a(\cos(2\theta)+1), a\sin(2\theta)).$$

Let $R = (r\cos\theta, r\sin\theta)$ any point of l_1. Then R is on the limaçon determined by C and P if and only if $QR = 1$ (by continuity, the points at distance 1 on the vertical tangent to the circle at point P are considered to be on the limaçon):

$$\begin{aligned} QR = 1 &\iff 1 = (r\cos\theta - 2a\cos^2\theta)^2 + (r\sin\theta - 2a\sin\theta\cos\theta)^2 \\ &\iff 1 = (\cos^2\theta + \sin^2\theta)(r - 2a\cos\theta)^2 \\ &\iff 1 = (r - 2a\cos\theta)^2 \\ &\iff r = 1 + 2a\cos\theta \quad \text{or} \quad r = -1 + 2a\cos\theta \end{aligned}$$

This can be interpreted geometrically. Let P, A the intersection points of C with the x-axis. As PA is a diameter of C, the angle $\angle PQR$ is a right angle, so $PQ = 2a\cos\theta$. Therefore $PR = |PQ \pm 1| = |\pm 1 + 2a\cos\theta|$.

The limaçon is the union of the curves C_1, C_2 with polar equations

$$r = 1 + 2a\cos\theta, \qquad r = -1 + 2a\cos\theta, \qquad -\frac{\pi}{2} < \theta < \frac{\pi}{2}.$$

As $\cos(\theta+\pi) = -\cos(\theta)$, if the point R with polar coordinates (r,θ) is on C_1, then $(-r, \theta+\pi)$ is on C_2. But (r,θ) and $(-r,\theta+\pi)$ are polar coordinates of the same point! Therefore the two curves are identical if we let θ vary in $\mathbb{R}$, and we obtain the complete curve if we let θ vary in $]-\pi,\pi]$ in the equation of C_1.

The limaçon determined by P and C has polar equation

$$r = 1 + 2a\cos\theta, \qquad \theta \in \mathbb{R}.$$

(c) Let L the limaçon. By part (b), if $x \neq 0$

$$\begin{aligned} (x,y) \in L &\iff \exists m \in \mathbb{R}, \begin{cases} y &= mx \\ 1 &= \left(x - \frac{2a}{m^2+1}\right)^2 + \left(y - \frac{2am}{m^2+1}\right) \end{cases} \\ &\iff 1 = \left(x - \frac{2a}{\frac{x^2}{y^2}+1} \right)^2 + \left(y - \frac{2a\frac{x}{y}}{\frac{x^2}{y^2}+1} \right) \\ &\iff x^2(x^2+y^2-2ax)^2 + y^2(x^2+y^2-2ax)^2 = (x^2+y^2)^2 \\ &\iff (x^2+y^2-2ax)^2 = x^2+y^2 \end{aligned}$$

The two exceptional points $(0, \pm 1)$ satisfy this equation, so the Cartesian equation of the limaçon is

$$L : (x^2+y^2-2ax)^2 = x^2+y^2.$$

(We can also obtain this equation from the polar equation $r = 1 + 2a\cos\theta$.) □

Ex. 10.3.18 *A Pierpont prime is a prime $p > 3$ of the form $p = 2^k 3^l + 1$. Prove that a regular n-gon can be constructed by origami (or by marked ruler or by intersections of conics) if and only if $n = 2^a 3^b p_1 \cdots p_s$ where $a, b \geq 0$ and $p_1, \ldots, p_s$ are distinct Pierpont primes.*

Proof. A regular n-gon can be constructed by origami if and only if $\zeta_n = e^{2\pi i/n}$ is an origami number (see Exercise 10.1.2, where the figures constructible by straightedge and compass are a fortiori constructible by origami).

The splitting field of ζ_n over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_n)$. By Theorem 10.3.6, ζ_n is an origami number if and only if $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2^a 3^b$ for some integers $a, b \geq 0$, and the minimal polynomial of ζ_n over $\mathbb{Q}$ is $\Phi_n(x)$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n) = \phi(n)$, so

$$\zeta_n \in \mathcal{O} \iff \phi(n) = 2^a 3^b, \ a, b \in \mathbb{N}.$$

- First suppose that $n = 2^u 3^v p_1 \cdots p_s, \ u, v \geq 0$, where $p_1, \ldots, p_s$ are distinct Pierpont numbers.

  Write $p_k = 2^{u_k} 3^{v_k} + 1, \ u_k, v_k \in \mathbb{N}$, for $k = 1, \ldots, s$. As $2^u, 3^v, p_1, \ldots, p_s$ are relatively prime, if $u \geq 1, v \geq 1$

  $$\begin{aligned} \phi(n) &= \phi(2^u)\phi(3^v)\phi(p_1)\cdots\phi(p_s) \\ &= (2^a - 2^{a-1})(3^b - 3^{b-1})(p_1 - 1)\cdots(p_s - 1) \\ &= 2^{a-1}(2 \times 3^{b-1})(2^{u_1}3^{v_1})\cdots(2^{u_s}3^{v_s}) \\ &= 2^a 3^b, \qquad a, b \in \mathbb{N}. \end{aligned}$$

  If $u = 0$, $\phi(2^u) = 1$, and if $v = 0$, $\phi(3^v) = 1$. In all cases,

  $$\phi(n) = 2^a 3^b, \quad a, b \in \mathbb{N}.$$

- Conversely, suppose that $\phi(n) = 2^a 3^b, \ a, b \geq 0$, and let the factorization of n be $n = q_1^{a_1} \cdots q_s^{a_s}$, where $q_1, \ldots, q_s$ are distinct primes and the exponents $a_1, \ldots, a_s$ are all ≥ 1. Then

  $$\phi(n) = 2^a 3^b = q_1^{a_1 - 1}(q_1 - 1)\cdots q_s^{a_s - 1}(q_s - 1).$$

  If $a_i > 1$, then $q_i \mid 2^a 3^b$, so $q_i = 2$, or $q_i = 3$, and $q_i^{a_i}$ is a power of 2 or 3.

  If $a_i = 1$, then $q_i - 1 \mid 2^a 3^b$, therefore $q_i - 1 = 2^{u_i} 3^{v_i}$, and so q_i is a Piermont prime number, and $q_i^{a_i} = q_i = 2^{u_i} 3^{v_i} + 1$.

  So $n = 2^a 3^b p_1 \cdots p_s$ where $a, b \geq 0$ and $p_1, \ldots, p_s$ are distinct Pierpont primes.

  Conclusion: a regular n-gon can be constructed by origami if and only if $n = 2^a 3^b p_1 \cdots p_s$ where $a, b \geq 0$ and $p_1, \ldots, p_s$ are distinct Pierpont primes.

□