15 Chapter 15 : THE LEMNISCATE

15.1 DIVISION POINTS AND ARC LENGTH

Ex. 15.1.1 *Prove that the numbers described in Abel's theorem at the beginning of the chapter are precisely those in Theorem 10.2.1, provided we replace "product of several numbers" with "product of distinct numbers" in Abel's statement of the theorem.*

Proof. The numbers described in Theorem 10.2.1 are the integers $n = 2^s p_1 \cdots p_r$, where $p_1, \ldots, p_r$ are distinct Fermat primes, of the form $p_k = 2^{n_k} + 1$. Thus these numbers are the product of *distinct* numbers of the form 2^m, or $2^m + 1$, where $2^m + 1$ is prime, as described in the Theorem of Abel. □

Ex. 15.1.2 *Show that in polar coordinates, the equation of the lemniscate is $r^2 = \cos(2\theta)$.*

Proof. By definition, a point $M = (x, y) \in \mathbb{R}^2$ is a point of the lemniscate L if and only if

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

If (r, θ) are polar coordinates of $M = M(r, \theta)$, then $x = r\cos\theta, y = r\sin\theta$, thus, using $\cos^2\theta + \sin^2\theta = 1$, and $\cos(2\theta) = \cos^2\theta) - \sin^2\theta$, we obtain

$$\begin{aligned} M(r,\theta) \in L &\iff (r^2\cos^2\theta + r^2\sin^2\theta)^2 = r^2\cos^2\theta - r^2\sin^2\theta \\ &\iff r^4 = r^2\cos(2\theta) \\ &\iff r^2 = \cos(2\theta). \end{aligned}$$

The equation of the lemniscate is $r^2 = \cos(2\theta)$. □

Ex. 15.1.3 *Prove that the two improper integrals $\int_0^1 (1-t^4)^{-1/2} \mathrm{d}t$ and $\int_{-1}^0 (1-t^4)^{-1/2} \mathrm{d}t$ converge.*

Proof. The map $t \mapsto (1 - t^4)^{-1/2}$ is continuous on $[0, 1[$, thus $t \mapsto (1 - t^4)^{-1/2}\mathrm{d}t$ is summable on $[1, x]$ for all $x \in [0, 1]$.

Since $1 - t^4 = (1-t)(1+t+t^2+t^3)$, $(1-t^4)^{-1/2} \sim [4(1-t)]^{-1/2}$ in the neighborhood of 1. The Riemann Criterium shows that $\int_0^1 (1 - t)^{-\alpha}\mathrm{d}t$ converges if $\alpha < 1$, and here $\alpha = 1/2$. Since $(1-t^4)^{-1/2} > 0$, this is sufficient to prove that $\int_0^1 (1-t^4)^{-1/2}\mathrm{d}t$ converges.

Since $t \mapsto (1 - t^4)^{-1/2}$ is even, the same is true in the neighborhood of -1, thus $\int_{-1}^0 (1 - t^4)^{-1/2}\mathrm{d}t$ converges. □

Ex. 15.1.4 *Prove the arc length formula stated in (15.6)*

Proof. Here the equation of the ellipse E is

$$x^2 + \frac{y^2}{b^2} = 1,$$

with eccentricity $k = \sqrt{1 - b^2}$.

We compute the arc length l of (E) between $x = u, y = v$ $(-1 < u < v < 1)$ on the upper part of the curve. Then

$$l = \int_u^v \sqrt{1 + \left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2}\, \mathrm{d}x,$$

where $y = f(x) = b\sqrt{1-x^2}$. Then $f'(x) = \frac{\mathrm{d}y}{\mathrm{d}x} = -\frac{2x}{\sqrt{1-x^2}}$, thus

$$\begin{aligned} l &= \int_u^v \sqrt{1 + \left(\frac{bx}{\sqrt{1-x^2}}\right)^2}\,\mathrm{d}x \\ &= \int_u^v \sqrt{\frac{1 - x^2 + b^2x^2}{1-x^2}}\,\mathrm{d}x \\ &= \int_u^v \sqrt{\frac{1-k^2x^2}{1-x^2}}\,\mathrm{d}x \end{aligned}$$

We have proved

$$l = \int_u^v \sqrt{1 + \left(\frac{\mathrm{d}y}{\mathrm{d}x}\right)^2}\,\mathrm{d}x = \int_u^v \sqrt{\frac{1-k^2x^2}{1-x^2}}\,\mathrm{d}x = \int_u^v \frac{\sqrt{(1-x^2)(1-k^2x^2)}}{1-x^2}\,\mathrm{d}x.$$

The arc length of the ellipse is given by an elliptic integral. $\square$

Ex. 15.1.5 *Shows that (15.7) reduces to $(x^2+y^2)^2 = x^2 - y^2$ when $a = b = 1/\sqrt{2}$.*

Proof. If we take $a = b = 1/\sqrt{2}$ in the formula of the ovals of Cassini

$$((x-a)^2 + y^2)((x+a)^2 + y^2) = b^4,$$

we obtain

$$\begin{aligned} \frac{1}{4} &= \left[\left(x - \frac{1}{\sqrt{2}}\right)^2 + y^2\right]\left[\left(x + \frac{1}{\sqrt{2}}\right)^2 + y^2\right] \\ &= \left(x^2 + y^2 + \frac{1}{2} - \sqrt{2}\,x\right)\left(x^2 + y^2 + \frac{1}{2} + \sqrt{2}\,x\right) \\ &= \left((x^2 + y^2 + \frac{1}{2}\right)^2 - 2x^2 \\ &= (x^2+y^2)^2 + (x^2+y^2) - 2x^2 \\ &= (x^2+y^2)^2 + y^2 - x^2 + \frac{1}{4}. \end{aligned}$$

Therefore, for $a = b = 1/\sqrt{2}$, the equation $((x-a)^2 + y^2)((x+a)^2 + y^2) = b^4$ reduces to

$$(x^2+y^2)^2 = x^2 - y^2,$$

which is the equation of the Lemniscate. $\square$

Ex. 15.1.6 *Let $n > 0$ be an odd integer, and assume that the n-division points of the lemniscate can be constructed with straightedge and compass. Prove that the same is true for the $2n$-division points. Your proof should include a picture.*

Proof. Suppose that $n = 2N+1$ is odd, and consider $M_0 = 0, \ldots, M_{n-1}$ the n-divisions points, where M_k has positive arc length $s_k = k\frac{2\varpi}{n},\ k = 0, \ldots, n-1$.

Then $s_k = (2k)\frac{2\varpi}{2n}$, so that $N_{2k} = M_k$ is also a $2n$-division point. The other $2n$-division points are the points N_{2k+1} corresponding to the arc length $k\frac{2\varpi}{n}+\frac{\varpi}{n} = (2k+1)\frac{\varpi}{n}$. Then the symmetric point N'_{2k+1} about the x-axis has arc length

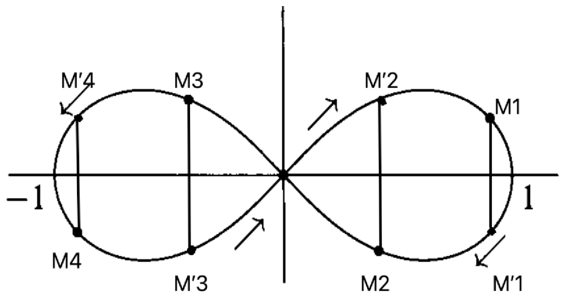
$$\varpi - (2k+1)\frac{\varpi}{n} = \varpi - (2k+1)\frac{\varpi}{2N+1} = (N-k)\frac{2\varpi}{n},$$

thus is the n-division point M_{2n+1-k}. This proves that the symmetric points $M'_0 = 0, \ldots, M'_{n-1}$ of $M_0, \ldots, M_{n-1}$ about the x-axis are $2n$-divisions points.

Therefore we can complete $M_0, M_1, \ldots, M_{n-1}$ by the symmetric points $M'_0 = O, \ldots, M'_{n-1}$ relative to the x-axis to obtain the $2n$-division points (the point O is counted twice).

Since the M_k can be constructed with straightedge and compass, the symmetric points M'_k are also constructible, thus the $2n$-division points are constructible.

Figure for $n = 5$: the 10-division points are $0, M'_2, M_1, M'_1, M_2, 0, M_3, M'_3, M_4, M'_3$. □



Ex. 15.1.7 *Recall that in Greek geometry, the ellipse is defined to be the locus of all points whose* **sum** *of distances to two given points is constant. Suppose instead we consider the locus of all points whose* **product** *of distances to two given points is constant. Show that this leads to (15.7) when the given points are* $(a, 0), (-a, 0)$ *and the constant is* b^4 *(*).*

(*) Read b^2.

Proof. Let Γ the locus of all points whose product of distances to two points $(a, 0), (-a, 0)$ is the constant b^2. Then

$$\begin{aligned} M(x,y) \in \Gamma &\iff \sqrt{(x-a)^2+y^2}\sqrt{(x+a)^2+y^2} = b^2 \\ &\iff ((x-a)^2+y^2)((x-a)^2+y^2) = b^4. \end{aligned}$$

We obtain the formula of the ovals of Cassini. □

15.2 THE LEMNISCATIC FUNCTION

Ex. 15.2.1 *Give a careful proof of (15.9) using the hints given in the text.*

Proof. By section 15.2, we know that φ is 2ϖ periodic,

$$\varphi(s + 2\varpi) = \varphi(s), \qquad (s \in \mathbb{R}).$$

Moreover, for $-1 \le r \le 1$, and $\frac{-\varpi}{2} \le s \le \frac{\varpi}{2}$,

$$r = \varphi(s) \iff s = \int_0^r \frac{1}{\sqrt{1-t^4}} \mathrm{d}t.$$

Write $r' = \varphi(-s) \in [-1, 1]$. Then for every $s \in [-\frac{\varpi}{2}, \frac{\varpi}{2}]$,

$$\begin{aligned}
r' = \varphi(-s) &\iff -s = \int_0^{r'} \frac{1}{\sqrt{1-t^4}} \mathrm{d}t \\
&\iff -s = -\int_0^{-r'} \frac{1}{\sqrt{1-\tau^4}} \mathrm{d}\tau \qquad (\tau = -t) \\
&\iff s = \int_0^{-r'} \frac{1}{\sqrt{1-\tau^4}} \mathrm{d}\tau \\
&\iff -r' = \varphi(s)
\end{aligned}$$

This proves that

$$\varphi(-s) = -\varphi(s) \qquad \left(-\frac{\varpi}{2} \leq s \leq \frac{\varpi}{2}\right). \tag{1}$$

Write $M(s)$ the point on the lemniscate with signed arc length s. Consider $M' = M(s')$ the symmetric point of $M(s)$ about the origin. Since the lemniscate is symmetric about the origin, Consider first the case where $0 \leq s \leq \varpi$, then the signed arc length is the positive arc length. Let $M(s)$ the point on the lemniscate with arc length s. Then the symmetric point $M(s')$ about the x-axis is such that $r' = OM(s') = OM(s) = r$, thus, by definition of φ, $\varphi(s) = \varphi(s')$. The total arc length from $O = M(0)$ to $O = M(\varpi)$ in the first loop is ϖ, and the symmetry of the lemniscate about the x-axis implies that the arc length $\varpi - s$ between $M(s)$ and $O = M(\varpi)$ is equal to the arc length s' between $O = M(0)$ and $M(s')$, thus $s' = \varpi - s$. This proves

$$\varphi(\varpi - s) = \varphi(s) \qquad (0 \leq s \leq \varpi). \tag{2}$$

Now, if $\frac{\varpi}{2} \leq s \leq \varpi$, then $0 \leq \varpi - s \leq \frac{\varpi}{2}$, thus, using (1), (2), (3)

$$\begin{cases} \varphi(s) & = \varphi(\varpi - s) = -\varphi(s - \varpi) = -\varphi(s + \varpi), \\ \varphi(-s) & = \varphi(\varpi - (-s)) = \varphi(s + \varpi). \end{cases}$$

Therefore $\varphi(-s) = -\varphi(s)$ if $\frac{\varpi}{2} \leq s \leq \varpi$. Now, if we suppose $-\varpi \leq s \leq -\frac{\varpi}{2}$, then $\frac{\varpi}{2} \leq -s \leq \varpi$, so we can apply the last equality to $-s$: $\varphi(s) = \varphi(-(-s)) = -\varphi(-s)$. This proves

$$\varphi(-s) = \varphi(s) \qquad (-\varpi \leq s \leq \varpi). \tag{3}$$

Using the periodicity, if $s \in \mathbb{R}$, the is some $n \in \mathbb{Z}$ and $s' \in [-\varpi, \varpi[$ such that $s = 2n\varpi + s'$. Then

$$\varphi(-s) = \varphi(-s - 2n\varpi) = \varphi(-s') = -\varphi(s') = -\varphi(s - 2n\varphi) = -\varphi(s).$$

We have proved

$$\varphi(-s) = \varphi(s) \qquad (s \in \mathbb{R}).$$

We can now complete (2) to $-\varpi \leq s \leq 0$. Then $0 \leq -s \leq \varpi$, and by (2) applied to $-s$, $\varphi(s + \varpi) = \varphi(-s) = -\varphi(s)$, thus

$$\varphi(\varpi - s) = -\varphi(s - \varpi) = -\varphi(s + \varpi) = \varphi(s)$$

.

We have proved, for all $s \in \mathbb{R}$,

$$\begin{aligned}
\varphi(-s) &= -\varphi(s) \\
\varphi(\varpi - s) &= \varphi(s).
\end{aligned}$$

$\square$

Ex. 15.2.2 *Supply the details needed to complete the proof of Proposition 15.2.1.*

Proof. The proof of Proposition 15.2.1 shows that

$$\varphi'(s) = \sqrt{1 - \varphi^4(s)}, \qquad 0 \leq s \leq \frac{\varpi}{2}.$$

By Exercise 3, parts (a) and (b), φ' is even and has period 2ϖ, and by part (c),

$$\varphi'(\varpi - s) = -\varphi'(s), \qquad s \in \mathbb{R}.$$

Therefore, if $-\frac{\varpi}{2} \leq s \leq 0$, then

$$\varphi'(s) = -\varphi'(-s) = -\sqrt{1 - \varphi^4(-s)} = -\sqrt{1 - \varphi^4(s)}.$$

Now, if $\frac{\varpi}{2} \leq s \leq \varpi$, then $0 \leq \varpi - s \leq \frac{\varpi}{2}$, thus

$$\varphi'(s) = -\varphi'(\varpi - s) = -\sqrt{1 - \varphi^4(\varpi - s)} = -\sqrt{1 - \varphi^4(s)}.$$

If $-\varpi \leq s \leq -\frac{\varpi}{2}$, then $\frac{\varpi}{2} \leq -s \leq \varpi$. Using the above equality, we obtain

$$\varphi'(s) = -\varphi(-s) = -\sqrt{1 - \varphi^4(-s)} = -\sqrt{1 - \varphi^4(s)}.$$

We have proved

$$\varphi'^2(s) = 1 - \varphi^4(s), \qquad -\varpi \leq s \leq \varpi.$$

Now if s is any real number, there is some $n \in \mathbb{Z}$ and $s' \in [-\varpi, \varpi[$ such that $s = 2n\varpi + s'$. Since 2ϖ is a period of φ and φ',

$$\varphi'^2(s) = \varphi'^2(s') = 1 - \varphi^4(s') = 1 - \varphi^4(s).$$

This complete the proof of Proposition 15.2.1. □

Ex. 15.2.3 *Here are some useful properties of φ'.*

(a) φ has period 2ϖ. Explain why this implies that the same is true for φ'.

(b) φ is an odd function by (15.9). Explain why this implies that φ' is even.

(c) Use (15.9) to prove that $\varphi'(\varpi - s) = -\varphi'(s)$.

(d) Use Proposition 15.2.1 to prove that $\varphi''(s) = -2\varphi^3(s)$.

Proof.

(a) For all $s \in \mathbb{R}$, $\varphi(s + 2\varpi) = \varphi(s)$. By differentiation, and the chain rule, we obtain

$$\varphi'(s + 2\varphi)(s) = \varphi(s).$$

φ' has period 2ϖ.

(b) Since $\varphi(-s) = -\varphi(s)$ for all $s \in \mathbb{R}$, the chain rule gives

$$-\varphi'(-s) = -\varphi'(s),$$

thus φ' is even.

(c) By (15.9), $\varphi(\varpi - s) = \varphi(s)$ for all $s \in \mathbb{R}$. Then the chain rule gives $-\varphi'(\varpi - s) = \varphi'(s)$, thus

$$\varphi'(\varpi - s) = -\varphi'(s), \qquad s \in \mathbb{R}.$$

(d) By differentiation of $\varphi'^2(s) = 1 - \varphi^4(s)$ $(s \in \mathbb{R})$, we obtain

$$2\varphi'(s)\varphi''(s) = -4\varphi^3(s)\varphi'(s).$$

If $s \neq \frac{\varpi}{2} + n\varpi, n \in \mathbb{Z}$, then $\varphi'(s) \neq 0$, so that

$$\varphi''(s) = -2\varphi^3(s), \qquad s \neq \frac{\varpi}{2} + n\varpi, n \in \mathbb{Z}.$$

If $s = \frac{\varpi}{2} + n\varpi$ for some integer $n \in \mathbb{Z}$, since φ is infinitely differentiable, φ'' is continuous, therefore

$$\varphi''(s) = \lim_{t \to s, t \neq s} \varphi''(t) = \lim_{t \to s, t \neq s} (-2\varphi^3(t)) = -2\varphi^3(s).$$

Therefore

$$\varphi''(s) = -2\varphi^3(s), \qquad s \in \mathbb{R}.$$

□

Ex. 15.2.4 *Suppose that we define* $\sin(x)$ *by* $y = \sin(x) \iff x = \int_0^y (1 - t^2)^{-1/2} \mathrm{d}t$. *Then define* $\cos(x)$ *to be* $\sin'(x)$. *Use the method of Proposition 15.2.1 to prove the standard trigonometric identity* $\cos^2(x) = 1 - \sin^2(x)$.

Proof. We obtain the analog of (15.9) as in Exercise 1: for all $x \in \mathbb{R}$,

$$\sin(-x) = -\sin(x),$$
$$\sin(\pi - x) = \sin(x).$$

Now we use the definition of sin: for all $y \in [-1, 1]$, for all $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$,

$$y = \sin(x) \iff x = \int_0^y (1 - t^2)^{-1/2} \mathrm{d}t,$$

where $\int_0^1 (1 - t^2)^{-1/2} \mathrm{d}t$ and $\int_0^{-1} (1 - t^2)^{-1/2} \mathrm{d}t$ converge.

If $x \in [0, \frac{\pi}{2}[$, differentiating each side of

$$s = \int_0^{\sin(x)} \frac{1}{\sqrt{1 - t^2}} \mathrm{d}t,$$

we obtain

$$1 = \frac{1}{\sqrt{1 - \sin^2(x)}} \sin'(x).$$

If $x = \frac{\pi}{2}$, then $\sin(x) = 1, \sin'(x) = 0$, thus $\sin'^2(x) = 1 - \sin^2(x)$. Therefore

$$\cos(x) = \sin'(x) = \sqrt{1 - \sin^2(x)}, \qquad 0 \leq x \leq \frac{\pi}{2}.$$

We extend the equality $\sin^2(x) + \cos^2(x) = 1$ to all $x \in \mathbb{R}$ as in Exercise 2. □

Ex. 15.2.5 *Here is Abel's proof of the addition law for φ.*

(a) Let $g(x, y)$ be differentiable on $\mathbb{R}^2$, and set $h(u, v) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)$. Use the chain Rule to prove that

$$\frac{\partial h}{\partial v}(u, v) = \frac{1}{2}\frac{\partial g}{\partial x}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) - \frac{1}{2}\frac{\partial g}{\partial y}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v).\right)$$

(b) Use part (a) to show that $g(x, y) = g(x+y, 0)$ on, $\mathbb{R}^2$ if and only if $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ on $\mathbb{R}^2$.

(c) Prove the addition law for φ by applying part (b) to

$$g(x, y) = \frac{\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)}{1 + \varphi^2(x)\varphi^2(y)}.$$

Part (d) of Exercise 3 will be useful.

Proof.

(a) To apply the Chain Rule, we suppose that g is continuously differentiable ($g \in C_1(\mathbb{R}^2)$). Write $x, y : \mathbb{R}^2 \to \mathbb{R}^2$ the two maps defined by

$$x(u, v) = \frac{1}{2}(u+v), \qquad y(u, v) = \frac{1}{2}(u-v),$$

Then

$$\frac{\partial x}{\partial v}(u, v) = \frac{1}{2}, \qquad \frac{\partial y}{\partial v}(u, v) = -\frac{1}{2},$$

and

$$h(u, v) = g(x(u, v), y(u, v)), \qquad (u, v) \in \mathbb{R}^2.$$

The Chain Rule gives

$$\begin{aligned}\frac{\partial h}{\partial v}(u, v) &= \frac{\partial g}{\partial x}\left(x(u, v), y(u, v)\right)\frac{\partial x}{\partial v}(u, v) + \frac{\partial g}{\partial y}\left(x(u, v), y(u, v)\right)\frac{\partial y}{\partial v}(u, v) \\ &= \frac{1}{2}\frac{\partial g}{\partial x}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) - \frac{1}{2}\frac{\partial g}{\partial y}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right)\end{aligned}$$

(b) Suppose that $g(x+y, 0) = g(x, y)$ for all $x, y \in \mathbb{R}$. Write $f(x) = g(x, 0)$. Then f is continuously differentiable, and $g(x, y) = f(x+y)$. By the Chain Rule, for all $(x, y) \in \mathbb{R}^2$,

$$\frac{\partial g}{\partial x}(x, y) = f'(x+y) = \frac{\partial g}{\partial y}(x, y),$$

therefore $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ on $\mathbb{R}^2$.

Conversely, suppose that $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ on $\mathbb{R}^2$. Then, for all $(u, v) \in \mathbb{R}^2$,

$$\frac{\partial h}{\partial v}(u, v) = \frac{1}{2}\frac{\partial g}{\partial x}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) - \frac{1}{2}\frac{\partial g}{\partial y}\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) = 0.$$

This means that for every fixed $u_0 \in \mathbb{R}$, the map $v \mapsto h(u_0, v)$ has a null derivative, thus is constant: $h(u_0, v) = h(u_0, 0)$ for all $v \in \mathbb{R}$. Since this is true for every u_0, we obtain

$$h(u, v) = h(u, 0), \qquad \text{for all } u, v \in \mathbb{R}.$$

Write $f(u) = h(u,0)$ for all $u \in \mathbb{R}$. Then f is continuously differentiable, and for all $u, v \in \mathbb{R}$, $h(u,v) = f(u)$ depends only of u.

By definition of h, this means that, for all $u, v \in \mathbb{R}$,

$$g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) = f(u).$$

Taking $v = u$ in $g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right) = h(u,v) = h(u,0)$, we obtain $g(u,0) = h(u,u) = h(u,0)$, therefore

$$g(u,0) = h(u,u) = h(u,0) = h(u,v) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right),$$

thus

$$g(u,0) = g\left(\frac{1}{2}(u+v), \frac{1}{2}(u-v)\right), \qquad u, v \in \mathbb{R}.$$

If (x,y) is any pair in $\mathbb{R}^2$, there exists a unique pair $(u,v) \in \mathbb{R}^2$ such that $x = \frac{1}{2}(u+v), y = \frac{1}{2}(u-v)$, given by $u = x+y, v = x-y$. Therefore, the preceding equality implies that

$$g(x+y, 0) = g(x,y), \qquad x, y \in \mathbb{R}.$$

(c) Define $g : \mathbb{R}^2 \to \mathbb{R}$ by

$$g(x,y) = \frac{\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)}{1 + \varphi^2(x)\varphi^2(y)}.$$

The partial derivative of this quotient relative to the variable x gives, using $\varphi''(x) = -2\varphi^3(x)$ (see Exercise 3, part (d)), and $\varphi'(x)^2 = 1 - \varphi^4(x)$

$$\begin{aligned}
&\left(1 + \varphi^2(x)\varphi^2(y)\right)^2 \frac{\partial g}{\partial x}(x,y) \\
&= \left(\varphi'(x)\varphi'(y) + \varphi(y)\varphi''(x)\right)\left(1 + \varphi^2(x)\varphi^2(y)\right) - 2\varphi(x)\varphi'(x)\varphi^2(y)\left(\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)\right) \\
&= \left(\varphi'(x)\varphi'(y) - 2\varphi(y)\varphi^3(x)\right)\left(1 + \varphi^2(x)\varphi^2(y)\right) - 2\varphi(x)\varphi'(x)\varphi^2(y)\left(\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)\right) \\
&= \varphi'(x)\varphi'(y) + \varphi'(x)\varphi'(y)\varphi^2(x)\varphi^2(y) - 2\varphi(y)\varphi^3(x) - 2\varphi^3(y)\varphi^5(x) \\
&\qquad - 2\varphi^2(x)\varphi^2(y)\varphi'(x)\varphi'(y) - 2\varphi(x)\varphi^3(y)\varphi'(x)^2 \\
&= \varphi'(x)\varphi'(y) + \varphi'(x)\varphi'(y)\varphi^2(x)\varphi^2(y) - 2\varphi(y)\varphi^3(x) - 2\varphi^3(y)\varphi^5(x) \\
&\qquad - 2\varphi^2(x)\varphi^2(y)\varphi'(x)\varphi'(y) - 2\varphi(x)\varphi^3(y)(1 - \varphi^4(x)) \\
&= \varphi'(x)\varphi'(y) + \varphi'(x)\varphi'(y)\varphi^2(x)\varphi^2(y) - 2\varphi(y)\varphi^3(x) - 2\varphi(x)\varphi^3(y) \\
&\qquad - 2\varphi^2(x)\varphi^2(y)\varphi'(x)\varphi'(y).
\end{aligned}$$

This last expression is symmetric relatively to x, y, and also the denominator $(1 + \varphi^2(x)\varphi^2(y))^2$. Since $g(x,y) = g(y,x) = \frac{\varphi(y)\varphi'(x) + \varphi(x)\varphi'(y)}{1 + \varphi^2(y)\varphi^2(x)}$, this proves that

$$\begin{aligned}
&\left(1 + \varphi^2(y)\varphi^2(x)\right) \frac{\partial g}{\partial y}(x,y) \\
&= \varphi'(y)\varphi'(x) + \varphi'(y)\varphi'(x)\varphi^2(y)\varphi^2(x) - 2\varphi(x)\varphi^3(y) - 2\varphi(y)\varphi^3(x) - 2\varphi^2(y)\varphi^2(x)\varphi'(y)\varphi'(x) \\
&= \left(1 + \varphi^2(x)\varphi^2(y)\right) \frac{\partial g}{\partial x}(x,y),
\end{aligned}$$

where $1 + \varphi^2(y)\varphi^2(x) > 0$. Therefore $\frac{\partial g}{\partial x} = \frac{\partial g}{\partial y}$ on $\mathbb{R}^2$.

By part (b), $g(x,y) = g(x+y,0)$. Using $\varphi(0) = 0$, and $\varphi'(0) = \sqrt{1-\varphi^4(0)} = 1$,

$$\begin{aligned} g(x,y) &= g(x+y,0) \\ &= \varphi'(0)\varphi(x+y) \\ &= \varphi(x+y). \end{aligned}$$

We have proved the addition law for φ:

$$\varphi(x+y) = \frac{\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}, \qquad x,y \in \mathbb{R}.$$

$\square$

Ex. 15.2.6 *Show that the subtraction law*

$$\varphi(x-y) = \frac{\varphi(x)\varphi'(y) - \varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}.$$

follows from the addition law together with (15.9) and Exercise 3.

Proof. Starting from the Addition Law for φ

$$\varphi(x+y) = \frac{\varphi(x)\varphi'(y) + \varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}, \qquad x,y \in \mathbb{R},$$

we obtain for all $x,y \in \mathbb{R}$, substituting $-y$ to y,

$$\varphi(x-y) = \frac{\varphi(x)\varphi'(-y) + \varphi(-y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(-y)}.$$

Since φ is odd, and φ' even (see 15.9 and Exercise 3), we obtain

$$\varphi(x-y) = \frac{\varphi(x)\varphi'(y) - \varphi(y)\varphi'(x)}{1+\varphi^2(x)\varphi^2(y)}.$$

$\square$

Ex. 15.2.7 *The proof of Theorem 15.2.5 uses induction on n.*

(a) Assume that n is even. In (15.18), we gave a formula for $Q_{n+1}(u)$ in terms of $Q_n(u)$ and $Q_{n-1}(u)$. Derive the corresponding formula for $P_{n+1}(u)$.

(b) Suppose that polynomials $P_n(u), Q_n(u)$ satisfy all of the conditions of the theorem except for the requirement that they be relatively prime. Since $\mathbb{Z}[u]$ is a UFD, we can write $P_n(u) = C_n\tilde{P}_n(u), Q_n(u) = C_n(u)\tilde{Q}_n(u)$, where $C_n(u), \tilde{P}_n(u), \tilde{Q}_n(u) \in \mathbb{Z}[u]$ and $\tilde{P}_n(u), \tilde{Q}_n(u)$ are relatively prime. Prove that we can assume that $\tilde{Q}_n(0) = 1$ and that $\tilde{P}_n(u), \tilde{Q}_n(u)$ satisfy all conditions of Theorem 15.2.5.

(c) Complete the inductive step of the proof when n is odd.

Proof.

(a,c) We will prove the theorem by induction on n. The theorem holds for $n = 1, n = 2$ with $P_1(u) = Q_1(u) = 1$, and $P_2(u) = 2, Q_2(u) = 1 + u$ (misprint in Cox p. 477). Now assume that it holds for $n - 1$ and n.

• If n is even,

$$\varphi((n-1)x) = \varphi(x)\frac{P_{n-1}\left(\varphi^4(x)\right)}{Q_{n-1}\left(\varphi^4(x)\right)},$$
$$\varphi(nx) = \varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\varphi'(x).$$

Using (15.13), we obtain

$$\begin{aligned}\varphi\left((n+1)x\right) &= -\varphi\left((n-1)x\right) + \frac{2\varphi(nx)\varphi'(x)}{1+\varphi^2(nx)\varphi^2(x)}\\ &= -\varphi(x)\frac{P_{n-1}\left(\varphi^4(x)\right)}{Q_{n-1}\left(\varphi^4(x)\right)} + \frac{2\left(\varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\varphi'(x)\right)\varphi'(x)}{1+\left(\varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\varphi'(x)\right)^2\varphi^2(x)}.\end{aligned}$$

To simplify, we write $a = \varphi(x), p_n = P_n(\varphi^4(x)), q_n = Q_n(\varphi^4(x))$.

Then, using $\varphi'(x)^2 = 1 - \varphi^4(x)$,

$$\begin{aligned}\varphi\left((n+1)x\right) &= a\left[-\frac{p_{n-1}}{q_{n-1}} + \frac{2(1-a^4)\frac{p_n}{q_n}}{1+a^4(1-a^4)\frac{p_n^2}{q_n^2}}\right]\\ &= a\left[-\frac{p_{n-1}}{q_{n-1}} + \frac{2(1-a^4)p_nq_n}{q_n^2+a^4(1-a^4)p_n^2}\right]\\ &= a\frac{-p_{n-1}(q_n^2+a^4(1-a^4)p_n^2)+2(1-a^4)p_nq_nq_{n-1}}{q_{n-1}(q_n^2+a^4(1-a^4)p_n^2)},\end{aligned}$$

that is

$$\varphi\left((n+1)x\right) = \varphi(x)\frac{P_{n+1}(\varphi^4(x))}{Q_{n+1}(\varphi^4(x))},$$

where

$$\begin{aligned}P_{n+1}(u) &= -P_{n-1}(u)(Q_n^2(u)+u(1-u)P_n^2(u)) + 2(1-u)P_n(u)Q_n(u)Q_{n-1}(u),\\ Q_{n+1}(u) &= Q_{n-1}(u)(Q_n^2(u)+u(1-u)P_n^2(u)).\end{aligned}$$

Verification : with $n = 2$, we obtain $P_3(u) = 3 - 6u - u^2, Q_3(u) = 1 + 6u - 3u^2$, which gives the tripling formula (15.17).

• If n is odd,

$$\varphi((n-1)x) = \varphi(x)\frac{P_{n-1}\left(\varphi^4(x)\right)}{Q_{n-1}\left(\varphi^4(x)\right)}\varphi'(x),$$
$$\varphi(nx) = \varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}.$$

Then(15.13) gives

$$
\begin{aligned}
\varphi\left((n+1)x\right) &= -\varphi\left((n-1)x\right) + \frac{2\varphi(nx)\varphi'(x)}{1+\varphi^2(nx)\varphi^2(x)} \\
&= -\varphi(x)\frac{P_{n-1}\left(\varphi^4(x)\right)}{Q_{n-1}\left(\varphi^4(x)\right)}\varphi'(x) + \frac{2\left(\varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\right)\varphi'(x)}{1+\left(\varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\right)^2\varphi^2(x)} \\
&= \varphi(x)\left[-\frac{P_{n-1}\left(\varphi^4(x)\right)}{Q_{n-1}\left(\varphi^4(x)\right)} + \frac{2\left(\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\right)}{1+\left(\varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\right)^2\varphi^2(x)}\right]\varphi'(x)
\end{aligned}
$$

With the same notations as in the even case, and with $a' = \varphi'(x)$,

$$
\begin{aligned}
\varphi\left((n+1)x\right) &= a\left[-\frac{p_{n-1}}{q_{n-1}} + \frac{2\frac{p_n}{q_n}}{1+a^4\frac{p_n^2}{q_n^2}}\right]a' \\
&= a\left[-\frac{p_{n-1}}{q_{n-1}} + \frac{2p_nq_n}{q_n^2+a^4p_n^2}\right]a' \\
&= a\left[\frac{-p_{n-1}(q_n^2+a^4p_n^2)+2p_nq_nq_{n-1}}{q_{n-1}(q_n^2+a^4p_n^2)}\right]a'
\end{aligned}
$$

that is

$$
\varphi\left((n+1)x\right) = \varphi(x)\frac{P_{n+1}(\varphi^4(x))}{Q_{n+1}(\varphi^4(x))}\varphi'(x),
$$

where

$$
\begin{aligned}
P_{n+1}(u) &= -P_{n-1}(u)(Q_n^2(u)+uP_n^2(u)) + 2P_n(u)Q_n(u)Q_{n-1}(u), \\
Q_{n+1}(u) &= Q_{n-1}(u)(Q_n^2(u)+uP_n^2(u)).
\end{aligned}
$$

The induction is done, and the induction formulas concerning P_n, Q_n are

$$
\begin{array}{ll}
 & \text{for } n \text{ even}, \\
P_{n+1}(u) & = -P_{n-1}(u)(Q_n^2(u)+u(1-u)P_n^2(u)) + 2(1-u)P_n(u)Q_n(u)Q_{n-1}(u), \\
Q_{n+1}(u) & = Q_{n-1}(u)(Q_n^2(u)+u(1-u)P_n^2(u)), \\
 & \text{for } n \text{ odd}, \\
P_{n+1}(u) & = -P_{n-1}(u)(Q_n^2(u)+uP_n^2(u)) + 2P_n(u)Q_n(u)Q_{n-1}(u), \\
Q_{n+1}(u) & = Q_{n-1}(u)(Q_n^2(u)+uP_n^2(u)).
\end{array}
$$

Note that we can take $P_0 = 0, Q_1 = 1$ (and $P_1 = 1, Q_1 = 1$).

We give a Sage function to compute P_n, Q_n:

```
R.<u> = ZZ[]

def divisionPolynomial(n):
    P0, Q0 = 0, 1
    P1, Q1 = 1, 1
    for i in range(n):
        if i % 2 != 0:
```

```
            S = Q1^2 + u * (1-u) *P1^2
            P2 = -P0 * S + 2 * (1-u) * P1 * Q1 * Q0
            Q2 = Q0  * S
        else:
            S = Q1^2 + u * P1^2
            P2 = -P0 * S + 2 * P1 * Q1 * Q0
            Q2 = Q0  * S
        D = gcd(P2,Q2)
        (P2, Q2) = (P2/D, Q2/D)
        (P0, Q0) = (P1, Q1)
        (P1, Q1) = (P2, Q2)
    return (P0,Q0)
```

```
P5, Q5 = divisionPolynomial(5); P5,Q5
```

$u^6+50u^5-125u^4+300u^3-105u^2-62u+5, 5u^6-62u^5-105u^4+300u^3-125u^2+50u+1$

```
P5.factor(), Q5.factor()
```

$(u^2-2u+5)\cdot(u^4+52u^3-26u^2-12u+1), (5u^2-2u+1)\cdot(u^4-12u^3-26u^2+52u+1)$

(b) We can write $P_n(u) = C_n\tilde{P}_n(u), Q_n(u) = C_n(u)\tilde{Q}_n(u)$, where $C_n(u), \tilde{P}_n(u), \tilde{Q}_n(u) \in \mathbb{Z}[u]$ and $\tilde{P}_n(u), \tilde{Q}_n(u)$ are relatively prime.

Since $Q_n(0) = 1$, then $C_n(0)\tilde{Q}_n(0) = 1$, where $C_n(0), \tilde{Q}_n(0)$ are integers, thus $\tilde{Q}_n(0) = \pm 1$.

If $\tilde{Q}_n(0) = 1$, we are done, and if $\tilde{Q}_n(0) = -1$ We replace $\tilde{P}_n, \tilde{Q}_n$ by $-\tilde{P}_n, -\tilde{Q}_n$, which satisfy all conditions of Theorem 15.2.5. $\square$

Ex. 15.2.8 *Let n be even, and let $P_n(u)$ be the polynomial from Theorem 15.2.5. Complete the proof of Corollary 15.2.6 by showing that the polar distances of the n-division points of the lemniscate are roots of $uP_n(u^4)(1-u^2)$.*

Proof. The polar distances of the n-division points are

$$u_m = \varphi\left(m\frac{2\varpi}{n}\right), \qquad m = 0, 1, \ldots, n-1.$$

If n is even, then

$$\varphi(nx) = \varphi(x)\frac{P_n\left(\varphi^4(x)\right)}{Q_n\left(\varphi^4(x)\right)}\varphi'(x).$$

With $x = \frac{2\varpi}{n}$, we obtain

$$0 = \varphi(m\cdot 2\varpi) = \varphi\left(n\cdot m\frac{2\varpi}{n}\right) = \varphi\left(m\frac{2\varpi}{n}\right)\frac{P_n\left(\varphi^4\left(m\frac{2\varpi}{n}\right)\right)}{Q_n\left(\varphi^4\left(m\frac{2\varpi}{n}\right)\right)}\varphi'\left(m\frac{2\varpi}{n}\right),$$

where, by Exercise 9, the denominator $Q_n\left(\varphi^4\left(m\frac{2\varpi}{n}\right)\right)$ is non vanishing.

Since $\varphi'\left(m\frac{2\varpi}{n}\right) = \pm\sqrt{1-\varphi^4\left(m\frac{2\varpi}{n}\right)}$, we obtain

$$0 = u_m P_n(u_m^4)\sqrt{1-u_m^4}.$$

$\sqrt{1-u_m^4} = \sqrt{1-u_m^2}\sqrt{1+u_m^2}$, where $1+u_m^2 \neq 0$, thus $\sqrt{1-u_m^4} = 0 \iff 1-u_m^2 = 0$. Therefore $u_m = \varphi\left(m\frac{2\varpi}{n}\right)$ is a root of

$$uP_n(u^4)(1-u^2).$$

$\square$

Ex. 15.2.9 *This exercise is concerned with the proof of Corollary 15.2.7.*

(a) Suppose that $P(u), Q(u) \in \mathbb{Z}[u]$ are relatively prime and $Q(0) = 1$. Prove that $uP(u^4)$ and $Q(u^4)$ have no common roots in any extension of $\mathbb{Q}$.

(b) Fix x in $\mathbb{R}$ and $m > 0$ in $\mathbb{Z}$, and let $P_m(u), Q_m(u) \in \mathbb{Z}[u]$ be as in Theorem 15.2.5. Thus $\varphi(mx)Q_m(\varphi^4(x)) = \varphi(x)P_m(\varphi^4(x))$. Prove that $Q_m(\varphi^4(x)) \neq 0$ when $\varphi(x) \neq 0$.

(c) Show that $\varphi\left(\frac{2\varpi}{n}\right) \neq 0$ when $n > 2$ is in $\mathbb{Z}$ and conclude that $Q_m\left(\varphi^4\left(\frac{2\varpi}{n}\right)\right) \neq 0$.

Proof.

(a) Since $P(u), Q(u)$ are relatively prime in $\mathbb{Q}[u]$, there are some polynomials $A, B \in \mathbb{Q}[u]$ such that $A(u)P(u) + B(u)Q(u) = 1$, thus the substitution $u \to u^4$ gives $A(u^4)P(u^4) + B(u^4)Q(u^4) = 1$. Reasoning by contradiction, suppose that $uP(u^4)$ and $Q(u^4)$ have a common root α in some extension of $\mathbb{Q}$. Since $Q(0) = 1$, $\alpha \neq 0$, thus $P(\alpha^4) = 0$. Then $P(\alpha^4) = Q(\alpha^4) = 0$ implies $1 = A(\alpha^4)P(\alpha^4) + B(\alpha^4)Q(\alpha^4) = 0$: this is a contradiction.

So $uP(u^4)$ and $Q(u^4)$ have no common roots in any extension of $\mathbb{Q}$.

(b) If m is odd, then $\varphi(mx)Q_m(\varphi^4)(x)) = \varphi(x)P_m(\varphi^4(x))$. Reasoning by contradiction, suppose that, for some $x \in \mathbb{R}$, $Q_m(\varphi^4(x)) = 0$. Then $\varphi(x)P_m(\varphi^4(x) = 0$, so that $\alpha = \varphi(x)$ is a common root of $Q_m(u^4)$ and $uP_m(u^4)$. Since P_m, Q_m are relatively prime, and $Q_m(0) = 1$, this is impossible by part (a).

If m is even, then $\varphi(mx)Q_m(\varphi^4(x)) = \varphi(x)P_m(\varphi^4(x))\varphi'(x)$. Suppose that, for some $x \in \mathbb{R}$, $Q_m(\varphi^4(x)) = 0$. Then $\varphi(x)P_m(\varphi^4(x))\varphi'(x) = 0$. If $\varphi'(x) = 0$, then $\sqrt{1 - \varphi^4(x)} = 0$, thus $\varphi^4(x) = 1$, and $\varphi(x) = \pm 1$. If $\varphi(x) \notin \{-1, 1\}$, then $\varphi(x)P_m(\varphi(x)) = 0$, so that $\alpha = \varphi(x)$ is a common root of $Q_m(u^4)$ and $uP_m(u^4)$, which is impossible by part (a).

We have proved that $Q_m(\varphi^4(x)) \neq 0$ when $\varphi(x) \notin \{-1, 1\}$.

(Misprint in the sentence of part (b) ? If $\varphi(x) = 0$, then $Q_m(\varphi^4(x)) = Q_m(0) = 1 \neq 0$, so there is no need to suppose $\varphi(x) \neq 0$.)

(c) For all $x \in \mathbb{R}$, $\varphi(x) = 0$ if and only if $x = k\varpi$ for some $k \in \mathbb{Z}$.

We must verify that $\varphi\left(\frac{2\varpi}{n}\right) \notin \{-1, 1\}$. If $n > 2$, then $0 < \frac{2\varpi}{n} < \varpi$. This proves that $0 < \varphi\left(\frac{2\varpi}{n}\right) < 1$, thus $\varphi\left(\frac{2\varpi}{n}\right) \notin \{-1, 0, 1\}$.

By our version of part (b), this implies that

$$Q_m\left(\varphi^4\left(\frac{2\varpi}{n}\right)\right) \neq 0.$$

Note: If we read the proof of Theorem 15.2.5, it is obvious that the denominators $Q_n(\varphi^4(x))$ never vanish, for all $x \in \mathbb{R}$, because $1 + \varphi^2(nx)\varphi^2(x) \neq 0$. □

Ex. 15.2.10 *The polar distances of the 5-division points of the lemniscate satisfy the equation*

$$0 = r_0(r_0^{24} + 50r_0^{20} - 125r_0^{16} + 300r_0^{12} - 105r_0^8 - 62r_0^4 + 5).$$

This equation was first derived by Fagnano in 1718.

(a) Show that the r_0 corresponding to the 10-division points also satisfy this equation.

(b) Use Maple or Mathematica (or Sage!) to show that this equation factors as

$$0 = r_0(r_0^8 - 2r_0^4 + 5)(r_0^{16} + 52r_0^{12} - 26r_0^8 - 12r_0^4 + 1)$$

and that the only positive real solutions are

$$\sqrt[4]{-13+6\sqrt{5}\pm 2\sqrt{85-38\sqrt{5}}}.$$

Explain (with a picture) how these solutions relate to the 5- *and* 10-*division points.*

Proof.

(a) Since 5 is odd, the 5-division points are roots of $uP_5(u^4)$ by Corollary 15.2.6. We obtain P_5 with the Sage function given in Exercise 7:

$$P_5(u) = u^6 + 50u^5 - 125u^4 + 300u^3 - 105u^2 - 62u + 5.$$

Therefore the polar distances r_0 of the 5-divisions points of the lemniscate satisfy the equation

$$0 = r_0(r_0^{24} + 50r_0^{20} - 125r_0^{16} + 300r_0^{12} - 105r_0^8 - 62r_0^4 + 5).$$

We have seen in Exercise 6 that the 10-division points are the 5-divisions points, together with the symmetric points about the x-axis, which have same polar distances. Therefore the polar distance of any 10-division point is also a polar distance of a 5-division point, thus verify the given equation (see figure in Exercise 6).

(b) We saw in Exercise 7 that $P_5(u)$ factors as

$$P_5(u) = (u^2 - 2u + 5)(u^4 + 52u^3 - 26u^2 - 12u + 1).$$

Therefore the polar distances of the 5-division points (and of the 10-division points) satisfy

$$0 = r_0P_5(r_0^4) = r_0(r_0^8 - 2r_0^4 + 5)(r_0^{16} + 52r_0^{12} - 26r_0^8 - 12r_0^4 + 1).$$

$r_0^8 - 2r_0^4 + 5 = (r_0^4 - 1)^2 + 4 > 0$ thus $r_0^8 - 2r_0^4 + 5$ has no real root.

We obtain the positive roots of $u^4 + 52u^3 - 26u^2 - 12u + 1$ with Sage:

```
u = var('u')
P = u^4+52*u^3-26*u^2-12*u+1;
S = P.solve(u)
S
```

$$\begin{aligned}
[u &= -6\sqrt{5} - \frac{1}{2}\sqrt{608\sqrt{5} + 1360} - 13,\\
u &= -6\sqrt{5} + \frac{1}{2}\sqrt{608\sqrt{5} + 1360} - 13,\\
u &= 6\sqrt{5} - \frac{1}{2}\sqrt{-608\sqrt{5} + 1360} - 13,\\
u &= 6\sqrt{5} + \frac{1}{2}\sqrt{-608\sqrt{5} + 1360} - 13]
\end{aligned}$$

```
[e.right().n() for e in S]
```

$$[-52.4909612184115, -0.341854511585989, 0.0733810146911846, 0.759434715306293]$$

```
S[2].right()^(1/4),S[3].right()^(1/4)
```

$$\left(\left(6\sqrt{5}-\frac{1}{2}\sqrt{-608\sqrt{5}+1360}-13\right)^{\frac{1}{4}},\left(6\sqrt{5}+\frac{1}{2}\sqrt{-608\sqrt{5}+1360}-13\right)^{\frac{1}{4}}\right)$$

Since $1360 = 16 \times 85$, and $608 = 16 \times 38$, we obtain the two positive solutions of the equation

$$\sqrt[4]{-13+6\sqrt{5}\pm 2\sqrt{85-38\sqrt{5}}}.$$

Since there are only two 5-division points M_1, M_2 in the right loop of the lemniscate, the 5 division points have polar distances (using $OM_1 > OM_2$)

$$\begin{aligned}
OM_0 &= 0\\
OM_1 = OM_4 &= \left(\sqrt[4]{-13+6\sqrt{5}+2\sqrt{85-38\sqrt{5}}}\right),\\
OM_2 = OM_3 &= \left(\sqrt[4]{-13+6\sqrt{5}-2\sqrt{85-38\sqrt{5}}}\right).
\end{aligned}$$

(See the figure of Exercise 6).

By Proposition 15.1.1, all these points are constructible. The 10-division points have same polar distances, and are also constructible. □

Ex. 15.2.11 *Use* $\sin(x+y) = \sin x \cos y + \sin y \cos x$ *to show that if* $\alpha, \beta \in [0,1]$, *then*

$$\int_0^\alpha \frac{1}{\sqrt{1-t^2}}\mathrm{d}t + \int_0^\beta \frac{1}{\sqrt{1-t^2}}\mathrm{d}t = \int_0^\gamma \frac{1}{\sqrt{1-t^2}}\mathrm{d}t,$$

where γ *is the real number defined by*

$$\gamma = \alpha\sqrt{1-\beta^2} + \beta\sqrt{1-\alpha^2}.$$

Note the similarity to (15.10).

Proof. If $\alpha, \beta \in [0,1]$, then there are unique $x, y \in [0, \pi/2]$ such that $\alpha = \sin x$, $\beta = \sin y$. Then $x = \arcsin(\alpha), y = \arcsin(\beta))$, where arcsin is the reciprocal function of f, f being the restriction of sin to $[0,\pi]$. For every $t \in]-1,1[$, f is differentiable at $f^{-1}(t) \in]0,\pi[$, and $f'(f^{-1}(t) \neq 0$, thus $f^{-1} = \arcsin : [-1,1] \to [0,\pi]$ is differentiable on $]-1,1[$, and for all $t \in]-1,1[$,

$$\arcsin'(t) = (f^{-1})'(t) = \frac{1}{f'(f^{-1}(t))} = \frac{1}{\cos(\arcsin(t))} = \frac{1}{\sqrt{1-\sin^2(\arcsin(t))}} = \frac{1}{\sqrt{1-t^2}}.$$

Since $t \mapsto \frac{1}{\sqrt{1-t^2}}$ is continuous on $]-1,1[$, for all $z \in]-1,1[$,

$$\arcsin(x) = \int_0^x \frac{1}{\sqrt{1-t^2}}\mathrm{d}t.$$

(This equality remains true for $x = \pm 1$:

$\int_0^1 \frac{1}{\sqrt{1-t^2}}\mathrm{d}t$ is convergent, and $\int_0^1 \frac{1}{\sqrt{1-t^2}}\mathrm{d}t = \lim\limits_{x\to 1} \int_0^x \frac{1}{\sqrt{1-t^2}}\mathrm{d}t$, with value $\arcsin(1) = \pi/2$).

Therefore, for all $\theta \in [0,\pi]$, and for all $z \in [-1,1]$,

$$z = \sin\theta \iff \theta = \arcsin(z) \iff \theta = \int_0^z \frac{1}{\sqrt{1-t^2}}\mathrm{d}t.$$

(Alternatively, we can take this equivalence as a definition of $\sin\theta$, to continue Exercise 4.)

Write $\gamma = \sin(x+y)$. Since $0 \le x+y \le \pi$, we obtain $x+y = \arcsin(\gamma)$, that is

$$\int_0^\alpha \frac{1}{\sqrt{1-t^2}}\mathrm{d}t + \int_0^\beta \frac{1}{\sqrt{1-t^2}}\mathrm{d}t = \int_0^\gamma \frac{1}{\sqrt{1-t^2}}\mathrm{d}t.$$

Moreover, since $x, y \in [0, \frac{\pi}{2}]$, $\cos x \ge 0, \cos y \ge 0$, thus

$$\cos x = \sqrt{1-\sin^2 x}, \qquad \cos y = \sqrt{1-\sin^2 y},$$

and

$$\begin{aligned}\gamma &= \sin(x+y)\\ &= \sin x\cos y + \sin y \cos x\\ &= \sin x\sqrt{1-\sin^2 y} + \sin y\sqrt{1-\sin^2 x}\\ &= \alpha\sqrt{1-\beta^2} + \beta\sqrt{1-\alpha^2}.\end{aligned}$$

□

Ex. 15.2.12 *Show that the substitution $t = \sin\theta$ transforms (15.20) into (15.21), and use this to prove carefully that $\varphi(u) = \sin\mathrm{am}(u)$ when the modulus is $k = i$.*

Proof. Consider the integral

$$I = \int_\gamma^\delta \frac{1}{\sqrt{1-k^2\sin^2\theta}}\mathrm{d}\theta,$$

where γ, δ are such that $[\gamma,\delta] \subset]0,\pi[$ and $\theta \mapsto f(\theta) = \frac{1}{\sqrt{1-k^2\sin^2\theta}}$ is defined (and continuous) on $[\gamma,\delta]$:

if the modulus k is real and positive, this requires $[\gamma,\delta] \subset]-\arcsin\left(\frac{1}{k}\right), \arcsin\left(\frac{1}{k}\right)[$.

Write $\alpha = \sin(\gamma), \beta = \sin(\delta)$, and consider $\psi = \arcsin : [-1,1] \to [0,\pi]$ (so that $t = \sin\theta \iff \theta = \psi(t)$ if $-1 < t < 1$ and $\theta \in [0,\pi]$)).

Then ψ is continuously differentiable, and is strictly increasing, thus $\psi([\alpha,\beta]) = [\psi(\alpha),\psi(\beta)]$, and ψ induces a bijection $[\alpha,\beta] \to [\psi(\alpha),\psi(\beta)] = [\gamma,\delta]$. The Theorem of Integration by Substitution gives

$$\int_\alpha^\beta f(\psi(t))\psi'(t)\mathrm{d}t = \int_{\psi(\alpha)}^{\psi(\beta)} f(\theta)\mathrm{d}\theta,$$

where

$$\begin{aligned}f(\psi(t)) &= \frac{1}{\sqrt{1-k^2t^2}},\\ \psi'(t) &= \frac{1}{\sqrt{1-t^2}}.\end{aligned}$$

Therefore, if $\int_\gamma^\delta \frac{1}{\sqrt{1-k^2\sin^2\theta}}\mathrm{d}\theta$ make sense,

$$\int_{\sin\gamma}^{\sin\delta} \frac{1}{\sqrt{(1-t^2)(1-k^2t^2)}}\mathrm{d}t = \int_\gamma^\delta \frac{1}{\sqrt{1-k^2\sin^2\theta}}\mathrm{d}\theta, \qquad (\gamma,\delta\in[0,\pi]).$$

Suppose now that $k=i$. Then, for all $r\in]-1,1[$,

$$\int_0^r \frac{1}{\sqrt{1-t^4}}\mathrm{d}t = \int_0^{\arcsin(r)} \frac{1}{\sqrt{1+\sin^2\theta}}\mathrm{d}\theta.$$

Therefore, for all $r\in]-1,1[$, and for all $s\in]-\frac{\varpi}{2},\frac{\varpi}{2}[$,

$$\begin{aligned} r=\varphi(s) &\iff s=\int_0^r \frac{1}{\sqrt{1-t^4}}\mathrm{d}t\\ &\iff s=\int_0^{\arcsin(r)} \frac{1}{\sqrt{1+\sin^2\theta}}\mathrm{d}\theta\\ &\iff \arcsin(r)=\mathrm{am}(s)\Rightarrow r=\sin\mathrm{am}(s)\end{aligned}$$

Therefore, for all $s\in]-\frac{\varpi}{2},\frac{\varpi}{2}[$, $\varphi(s)=\sin\mathrm{am}(s)=\mathrm{sn}(s)$, for the modulus $k=i$. By continuity, this is also true for $s=\pm\frac{\varpi}{2}$:

$$\varphi(s)=\mathrm{sn}(s), \qquad -\frac{\varpi}{2}\le s\le\frac{\varpi}{2}.$$

If we know the properties of symmetry (15.9) and periodicity of sn, we can conclude $\varphi=\mathrm{sn}$ for the modulus $k=i$. $\square$

15.3 THE COMPLEX LEMNISCATIC FUNCTION

Ex. 15.3.1 *Suppose that $g(z)$ is an analytic function satisfying $g(iz)=ig(z)$. Prove that $g'(iz)=g'(z)$.*

Proof. By the Chain Rule, $g(iz)=ig(z)$ implies $ig'(iz)=ig'(z)$, thus $g'(iz)=g'(z)$. $\square$

Ex. 15.3.2 *This exercise is concerned with the proof of Proposition 15.3.1.*

(a) Prove that $\varphi(x+iy)$, as defined by (15.22), satisfies the Cauchy-Riemann equations.

(b) Prove (15.23), (15.24), (15.25) and (15.26).

Proof.

(a) By the definition of φ on $\Omega=\{z\in\mathbb{C}\mid z\ne(m+in)\frac{\varpi}{2}, m\equiv n\equiv 1 \pmod 2\}$, for all $z=x+iy\in\Omega$,

$$\varphi(x+iy)=\frac{\varphi(x)\varphi'(y)+i\varphi(y)\varphi'(x)}{1-\varphi^2(x)\varphi^2(y)}=u(x,y)+iv(x,y),$$

where

$$u(x,y)=\frac{\varphi(x)\varphi'(y)}{1-\varphi^2(x)\varphi^2(y)}, \qquad v(x,y)=\frac{\varphi(y)\varphi'(x)}{1-\varphi^2(x)\varphi^2(y)}(=u(y,x)).$$

If we write $d = 1 - \varphi^2(x)\varphi^2(y)$ the denominator, then $d \neq 0$ on Ω.

Using $\varphi''(x) = -2\varphi^3(x)$ (see Exercise 15.2.3), and $\varphi'^2(x) = 1 - \varphi^4(x)$, we obtain

$$\begin{aligned}
d^2 \cdot \frac{\partial u}{\partial x}(x,y) &= \varphi'(x)\varphi'(y)\left(1 - \varphi^2(x)\varphi^2(y)\right) + 2\varphi'(x)\varphi'(y)\varphi^2(x)\varphi^2(y) \\
&= \varphi'(x)\varphi'(y)\left(1 + \varphi^2(x)\varphi^2(y)\right), \\
d^2 \cdot \frac{\partial u}{\partial y}(x,y) &= \varphi(x)\varphi''(y)\left(1 - \varphi^2(x)\varphi^2(y)\right) + 2\varphi^3(x)\varphi(y)\varphi'(y)^2 \\
&= -2\varphi(x)\varphi^3(y)\left(1 - \varphi^2(x)\varphi^2(y)\right) + 2\varphi^3(x)\varphi(y)\left(1 - \varphi^4(y)\right) \\
&= -2\varphi(x)\varphi^3(y) + 2\varphi^3(x)\varphi^5(y) + 2\varphi^3(x)\varphi(y) - 2\varphi^3(x)\varphi^5(y) \\
&= 2\varphi(x)\varphi(y)(\varphi^2(x) - \varphi^2(y)),
\end{aligned}$$

and, using $v(x,y) = u(y,x)$,

$$\begin{aligned}
d^2 \cdot \frac{\partial v}{\partial x}(x,y) &= 2\varphi(y)\varphi(x)(\varphi^2(y) - \varphi^2(x)) \\
d^2 \cdot \frac{\partial v}{\partial y}(x,y) &= \varphi'(y)\varphi'(x)\left(1 + \varphi^2(y)\varphi^2(x)\right).
\end{aligned}$$

Therefore, using $d \neq 0$ on Ω,

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \qquad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x},$$

so that φ satisfies the Cauchy-Riemann equations on Ω. Thus φ is analytic on Ω.

(b) For $s \in [0, \frac{\varpi}{2}]$, and $r \in [0,1]$,

$$r = \varphi(s) \iff s = \int_0^r \frac{1}{\sqrt{1-t^4}} \mathrm{d}t.$$

Since $0 = \int_0^r \frac{1}{\sqrt{1-t^4}}\mathrm{d}t$, $\varphi(0) = 0$, and since $\frac{\varpi}{2} = \int_0^1 \frac{1}{\sqrt{1-t^4}}\mathrm{d}t$, $\varphi\left(\frac{\varpi}{2}\right) = 1$. Using $\phi'(x) = \sqrt{1 - \varphi^4(x)}$ for $0 \le x \le \frac{\varpi}{2}$ (see Section 15.2), we obtain $\varphi'(0) = 1, \varphi'\left(\frac{\varpi}{2}\right) = 0$.

By (15.9), for all real s, $\varphi(\varpi - s) = \varphi(s)$, which gives $-\varphi'(\varpi - s) = \varphi'(s)$, thus $\varphi(\varpi) = 0$, and $\varphi'(\varpi) = -\varphi'(0) = -1$.

Moreover φ is odd, thus $\varphi\left(-\frac{\varpi}{2}\right) = -1, \varphi'\left(\frac{\varpi}{2}\right) = 0$. Since φ has period 2ϖ, $\varphi\left(\frac{3\varpi}{2}\right) = -1, \varphi'\left(\frac{3\varpi}{2}\right) = 0$.

We have proved (15.23):

x	$\varphi(x)$	$\varphi'(x)$
$\frac{\varpi}{2}$	1	0
ϖ	0	-1
$\frac{3\varpi}{2}$	-1	0
0	0	1

By definition of φ on $\Omega \subset \mathbb{C}$, for all $z = x + iy \in \Omega$,

$$\varphi(x + iy) = \frac{\varphi(x)\varphi'(y) + i\varphi(y)\varphi'(x)}{1 - \varphi^2(x)\varphi^2(y)}.$$

Therefore, since φ is odd and φ' is even,

$$\begin{aligned}
\varphi(iz) &= \varphi(-y+ix)\\
&= \frac{\varphi(-y)\varphi'(x)+i\varphi(x)\varphi'(-y)}{1-\varphi^2(-y)\varphi^2(x)}\\
&= \frac{-\varphi(y)\varphi'(x)+i\varphi(x)\varphi'(y)}{1-\varphi^2(x)\varphi^2(y)}\\
&= i\frac{\varphi(x)\varphi'(y)+i\varphi(y)\varphi'(x)}{1-\varphi^2(x)\varphi^2(y)}\\
&= i\varphi(z).
\end{aligned}$$

Using the Chain Rule (see Exercise 1), $i\varphi'(iz) = i\varphi'(z)$, thus $\varphi'(iz) = \varphi'(z)$, for all $z \in \Omega$. This proves (15.24):

$$\begin{aligned}
\varphi(iz) &= i\varphi(z),\\
\varphi'(iz) &= \varphi'(z) \qquad (z \in \Omega).
\end{aligned}$$

Since φ and φ' have period 2ω on $\mathbb{R}$,if $k \in \mathbb{Z}$, $\varphi(2k\varpi) = \varphi(0) = 0$, and $\varphi((2k+1)\varpi) = \varphi(\varpi) = 0$. Similarly, $\varphi'(2k\varpi) = \varphi(0) = 1, \varphi'((2k+1)\varpi) = \varphi'(\varpi) = -1$. Using (15.24), $\varphi(m\varpi i) = i\varphi(m\varpi), \varphi'(m\varpi i) = \varphi'(m\ \varpi)$.This shows (15.25):

$$\begin{aligned}
\varphi(m\varpi) &= \varphi(m\varpi i) = 0,\\
\varphi'(m\varpi) &= \varphi'(m\varpi i) = (-1)^m \qquad (m \in \mathbb{Z}).
\end{aligned}$$

Using the Addition Law, for all $z \in \Omega$ (then $z + m\varpi + n\varpi i \in \Omega$ for $m, n \in \mathbb{Z}$),

$$\begin{aligned}
\varphi(z+m\varpi) &= \frac{\varphi(z)\varphi'(m\varpi)+\varphi(m\varpi)\varphi'(z)}{1+\varphi^2(z)\varphi^2(m\varpi)}\\
&= (-1)^m\varphi(z),\\
\varphi(z+n\varpi i) &= \frac{\varphi(z)\varphi'(n\varpi i)+\varphi(n\varpi i)\varphi'(z)}{1+\varphi^2(z)\varphi^2(n\varpi)i}\\
&= (-1)^n\varphi(z),
\end{aligned}$$

This proves (15.26), and

$$\varphi(z+m\varpi+n\varpi i) = (-1)^{m+n}\varphi(z) \qquad (z \in \Omega).$$

$\square$

Ex. 15.3.3 *Prove the formula for $\varphi\left(z \pm \frac{\varpi}{2} i\right)$ stated in the proof of Theorem 15.3.2.*

Proof. By (15.24) and (15.23),

$$\varphi\left(\frac{\varpi}{2}i\right) = i\varphi\left(\frac{\varpi}{2}\right) = i, \qquad \varphi'\left(\frac{\varpi}{2}i\right) = \varphi'\left(\frac{\varpi}{2}\right) = 0,$$

and

$$\varphi\left(-\frac{\varpi}{2}i\right) = i\varphi\left(-\frac{\varpi}{2}\right) = -i, \qquad \varphi'\left(-\frac{\varpi}{2}i\right) = \varphi'\left(-\frac{\varpi}{2}\right) = 0.$$

Using the addition law (Proposition 15.3.1(b)), we see that

$$\begin{aligned}\varphi\left(z+\frac{\varpi}{2}i\right) &= \frac{\varphi(z)\varphi'\left(\frac{\varpi}{2}i\right)+\varphi\left(\frac{\varpi}{2}i\right)\varphi'(z)}{1+\varphi^2(z)\varphi^2\left(\frac{\varpi}{2}i\right)}\\ &= \frac{i\varphi'(z)}{1-\varphi^2(z)},\end{aligned}$$

and similarly,

$$\begin{aligned}\varphi\left(z-\frac{\varpi}{2}i\right) &= \frac{\varphi(z)\varphi'\left(-\frac{\varpi}{2}i\right)+\varphi\left(-\frac{\varpi}{2}i\right)\varphi'(z)}{1+\varphi^2(z)\varphi^2\left(-\frac{\varpi}{2}i\right)}\\ &= \frac{-i\varphi'(z)}{1-\varphi^2(z)}.\end{aligned}$$

We have proved

$$\varphi\left(z\pm\frac{\varpi}{2}i\right)=\pm\frac{i\varphi'(z)}{1-\varphi^2(z)}.$$

$\square$

Ex. 15.3.4 *Prove that $\varphi'(z)$ vanishes at all points of form $(m+in)\frac{\varpi}{2}$, $m+n$ odd.*

Proof. Note that, since $\varphi(z+k\varpi+l\varpi i)=(-1)^{k+l}\varphi(z)$, we obtain by differentiation

$$\varphi'(z+k\varpi+l\varpi i)=(-1)^{k+l}\varphi'(z),\qquad (z\in\Omega,\ k,l\in\mathbb{Z}).$$

Suppose that $m+n$ is odd, where $m,n\in\mathbb{Z}$.

- If m is odd, and n even, then $m=2k+1, n=2l$, where k,l are integers. Then

$$\begin{aligned}\varphi'\left((m+in)\frac{\varpi}{2}\right) &= \varphi'\left(\frac{\varpi}{2}+k\varpi+l\varpi\right)\\ &= (-1)^{k+l}\varphi'\left(\frac{\varpi}{2}\right)=0.\end{aligned}$$

- If m is even , and n odd, then $m=2k, n=2l+1$, where k,l are integers. Then, using (15.24),

$$\begin{aligned}\varphi'\left((m+in)\frac{\varpi}{2}\right) &= \varphi'\left(\frac{\varpi}{2}i+k\varpi+l\varpi\right)\\ &= (-1)^{k+l}\varphi'\left(\frac{\varpi}{2}i\right)\\ &= (-1)^{k+l}\varphi'\left(\frac{\varpi}{2}\right)=0.\end{aligned}$$

Thus $\varphi'(z)$ vanishes at all points of form $(m+in)\frac{\varpi}{2}$, $m+n$ odd.

But are these points the only zeros of $\varphi'(z)$? In Exercise 6, we need also the converse, which will prove now.

Suppose that $\varphi'(z)=0$. As in the proof of Theorem 15.3.2, for all $z\in\Omega$ such that $\varphi(z)\neq\pm i$,

$$\varphi\left(z+\frac{\varpi}{2}\right)=\frac{\varphi(z)\varphi'\left(\frac{\varpi}{2}\right)+\varphi\left(\frac{\varpi}{2}\right)\varphi'(z)}{1+\varphi^2(z)\varphi^2\left(\frac{\varpi}{2}\right)}=\frac{\varphi'(z)}{1+\varphi^2(z)},$$

thus

$$\varphi'(z)=(1+\varphi^2(z))\varphi\left(z+\frac{\varpi}{2}\right).$$

By the Principle of Analytic Continuation (see Exercise 5), since both members are analytic, this formula, which is true for all $z \in \mathbb{R}$, is true for all $z \in \Omega$ such that $z + \frac{\varpi}{2}$ is not a pole of φ.

Therefore, for all $z \in \omega$

$$\varphi'(z) = 0 \Rightarrow \varphi\left(z + \frac{\varpi}{2}\right) = 0, \text{ or } \varphi(z) = \pm i, \text{ or } z + \frac{\varpi}{2} \text{ is a pole.}$$

- If $\varphi\left(z + \frac{\varpi}{2}\right) = 0$, by Proposition 15.3.2,

$$z + \frac{\varpi}{2} = (p + iq)\varpi, \qquad p, q \in \mathbb{Z},$$

thus $z = (2p - 1 + i2q)\frac{\varpi}{2} = (m + in)\frac{\varpi}{2}$, where $m = 2p - 1, n = 2q$, and $m + n$ is odd.

- If $\varphi(z) = -i$, then $\varphi(iz) = 1 = \varphi\left(\frac{\varpi}{2}\right)$, thus, using $\varphi'(iz) = \varphi'(z)$, and the addition formula,

$$\varphi\left(iz - \frac{\varpi}{2}\right) = \frac{\varphi(iz)\varphi'\left(\frac{\varpi}{2}\right) - \varphi\left(\frac{\varpi}{2}\right)\varphi'(iz)}{1 + \varphi^2(iz)\varphi^2\left(\frac{\varpi}{2}\right)} = -\frac{\varphi'(iz)}{2} = -\frac{\varphi'(z)}{2} = 0.$$

Therefore, by Proposition 15.3.2(a),

$$iz - \frac{\varpi}{2} = (p + iq)\varpi, \qquad p, q \in \mathbb{Z},$$

thus, multiplying by $-i$,

$$z + i\frac{\varpi}{2} = (-ip + q)\varpi,$$

and

$$z = [2q + (-2p - 1)i]\,\frac{\varpi}{2} = (m + ni)\frac{\varpi}{2}, \text{where } m = 2q, n = -2p - 1 \in \mathbb{Z},\ m + n \text{ odd.}$$

- If $\varphi(z) = i$, then $\varphi(iz) = -1 = \varphi\left(-\frac{\varpi}{2}\right)$, thus

$$\varphi\left(iz + \frac{\varpi}{2}\right) = \frac{\varphi(iz)\varphi'\left(\frac{\varpi}{2}\right) + \varphi\left(\frac{\varpi}{2}\right)\varphi'(iz)}{1 + \varphi^2(iz)\varphi^2\left(\frac{\varpi}{2}\right)} = \frac{\varphi'(iz)}{2} = \frac{\varphi'(z)}{2} = 0.$$

Therefore

$$iz + \frac{\varpi}{2} = (p + iq)\varpi, \qquad p, q \in \mathbb{Z},$$

thus

$$z = i\frac{\varpi}{2} + (-ip + q)\varpi,$$

and

$$z = [2q + (-2p + 1)i]\,\frac{\varpi}{2} = (m + ni)\frac{\varpi}{2}, \text{where } m = 2q, n = -2p + 1 \in \mathbb{Z},\ m + n \text{ odd.}$$

- If $z + \frac{\varpi}{2}$ is a pole of φ, then

$$z + \frac{\varpi}{2} = (p + iq)\frac{\varpi}{2}, \qquad p \equiv q \equiv 1 \pmod 2,$$

thus

$$\begin{aligned} z &= (p - 1 + iq)\frac{\varpi}{2} \\ &= (m + in)\frac{\varpi}{2}, \qquad \text{where } m = p - 1, n = q, \text{and } m + n = p + q - 1 \equiv 1 \pmod 2. \end{aligned}$$

(This case gives the same solutions that $\varphi(z) = i$, so that these two cases are equivalent.)

In all cases, $z = (m + ni)\frac{\varpi}{2}$, where $m + n$ is odd, thus all zeros of φ' are our known zeros. $\square$

Ex. 15.3.5 *A useful observation is that an identity for φ proved over $\mathbb{R}$ automatically becomes an identity over $\mathbb{C}$.*

(a) Prove this carefully, using results from complex analysis such as [13,6.1.1]

(b) Explain why $\varphi'^2(z) = 1 - \varphi^4(z)$ holds for all $z \in \Omega$.

Proof.

(a) We recall the Principle of Analytic Continuation (or Identity Theorem), given in [13,6.1.1] in some larger context:

" Let f, g be analytic in a region (connected open set) $\Omega \subset \mathbb{C}$. Suppose that there is some $a \in \Omega$, and a sequence $(z_n)_{n\in\mathbb{N}} \in (\Omega \setminus \{a\})^{\mathbb{N}}$ of points of Ω distinct of a converging to $a \in \Omega$, such that $f(z_n) = g(z_n)$ for all $n \in \mathbb{N} = \{0, 1, 2, \cdots\}$. Then $f(z) = g(z)$ for all $z \in \Omega$."

Here $\Omega = \{z \in \mathbb{C} \mid z \neq (m + in)\frac{\varpi}{2}, m \equiv n \equiv 1 \pmod 2\}$. Then $\Omega \supset \mathbb{R}$ is open, and path-connected, thus is connected. Suppose that f, g are analytic on Ω, and $f(x) = g(x)$ for all $x \in \mathbb{R}$. Since any point a of $\mathbb{R}$ is a limit of some sequence $(z_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ (for instance $z_n = a + \frac{1}{n+1}$, $n \in \mathbb{N} = \{0, 1, 2, \cdots\}$), where $z_n \neq a$ for all $n \in \mathbb{N}$. Since $z_n \in \mathbb{R}$ for all n, $f(z_n) = g(z_n)$. The Principle of Analytic Continuation shows that $f(z) = g(z)$ for all $z \in \Omega$.

(b) If we define $f, g : \Omega \to \mathbb{C}$ by $f(z) = \varphi'^2(z), g(z) = 1 - \varphi^4(z)$ for all $z \in \Omega$, then f, g are analytic and $f(x) = g(x)$ for all $x \in \mathbb{R}$ by Section 15.2. Then part (b) shows that $f(z) = g(z)$ for all $z \in \Omega$, thus

$$\varphi'^2(z) = 1 - \varphi^4(z), \qquad z \in \Omega.$$

$\square$

Ex. 15.3.6 *By Theorem 15.3.3, $\varphi(z) = \varphi(z_0)$ if and only if $z = (-1)^{m+n}z_0 + (m+in)\varpi$. Following Abel, prove this using (15.13).*

Proof. If $z = (-1)^{m+n}z_0 + (m + in)\varpi$, then the periodicity and odd parity of φ shows that

$$\varphi(z) = \varphi\left((-1)^{m+n}z_0 + (m + in)\varpi\right) = (-1)^{m+n}\varphi\left((-1)^{m+n}z_0\right) = \varphi(z_0).$$

Conversely, suppose that $\varphi(z) = \varphi(z_0)$ (where z, z_0 are not poles of φ). By Proposition 13.3.1, the addition law gives, for all $x, y \in \mathbb{C}$ such that both members are defined,

$$\varphi(x + y) = \frac{\varphi(x)\varphi'(y) + \varphi'(x)\varphi(y)}{1 + \varphi^2(x)\varphi^2(y)}, \qquad \varphi(x - y) = \frac{\varphi(x)\varphi'(y) - \varphi'(x)\varphi(y)}{1 + \varphi^2(x)\varphi^2(y)},$$

thus, by subtraction,

$$\varphi(x + y) - \varphi(x - y) = \frac{\varphi'(x)\varphi(y)}{1 + \varphi^2(x)\varphi^2(y)}.$$

Take $x = \frac{z+z_0}{2}, y = \frac{z-z_0}{2}$ in this formula. We obtain

$$\varphi(z) - \varphi(z_0) = \frac{\varphi'\left(\frac{z+z_0}{2}\right)\varphi\left(\frac{z-z_0}{2}\right)}{1 + \varphi^2\left(\frac{z+z_0}{2}\right)\varphi^2\left(\frac{z-z_0}{2}\right)}.$$

(This formula is analogous to the trigonometric formula $\sin p - \sin q = 2\cos\frac{p+q}{2}\sin\frac{p-q}{2}$.) Therefore,

$$(\varphi(z)-\varphi(z_0))\left(1+\varphi^2\left(\frac{z+z_0}{2}\right)\varphi^2\left(\frac{z-z_0}{2}\right)\right)=\varphi'\left(\frac{z+z_0}{2}\right)\varphi\left(\frac{z-z_0}{2}\right).$$

By the Principle of Analytic Continuation (as in the proof of Proposition 15.3.1), this formula is true for all z such that both members are defined, including the points such that $1+\varphi^2\left(\frac{z+z_0}{2}\right)=0$. In others words, this is true for all $z\in\Omega$ such that $\frac{z-z_0}{2}, \frac{z+z_0}{2}$ are not poles of φ.

Thus $\varphi(z)=\varphi(z_0)$ implies that

$$\varphi\left(\frac{z-z_0}{2}\right)=0,\ \text{or}\ \varphi'\left(\frac{z+z_0}{2}\right)=0,\ \text{or}\ \frac{z-z_0}{2}\not\in\Omega,\ \text{or}\ \frac{z+z_0}{2}\not\in\Omega.$$

- Suppose that $\varphi\left(\frac{z-z_0}{2}\right)=0$.

  By Proposition 15.3.2, the zeros of φ are $z=(p+iq)\varpi,\ p,q\in\mathbb{Z}$, thus

$$\begin{aligned}\varphi\left(\frac{z-z_0}{2}\right)=0 &\iff \frac{z-z_0}{2}=(p+qi)\varpi, \qquad p,q\in\mathbb{Z}\\ &\iff z=z_0+2p\varpi+2q\varpi i, \qquad p,q\in\mathbb{Z}.\end{aligned}$$

  This shows that

$$z=(-1)^{m+n}z_0+(m+in)\varpi, \qquad \text{where } m=2p, n=2q\in\mathbb{Z}.$$

- Suppose that $\varphi'\left(\frac{z+z_0}{2}\right)=0$.

  By Exercise 4, we know that the points $(m+in)\frac{\varpi}{2}$, $m+n$ odd, are zeros of φ', and we showed that they are the only zeros of φ' (without using Theorem 15.3.3). Therefore,

$$\begin{aligned}\varphi'\left(\frac{z+z_0}{2}\right)=0 &\iff \frac{z+z_0}{2}=(m+in)\frac{\varpi}{2},\ m+n\equiv 1 \pmod 2\\ &\iff z=-z_0+(m+in)\varpi,\ m+n\equiv 1 \pmod 2\end{aligned}$$

  This shows that

$$z=(-1)^{m+n}z_0+(m+in)\varpi, \qquad m,n\in\mathbb{Z}.$$

- Suppose that $\frac{z-z_0}{2}\not\in\Omega$. Then $\frac{z-z_0}{2}$ is a pole. By Theorem 15.3.2,

$$\frac{z-z_0}{2}=(m+in)\frac{\varpi}{2}, \qquad m\equiv n\equiv 1 \pmod 2,$$

  thus

$$z=z_0+(m+in)\varpi, \qquad m\equiv n\equiv 1 \pmod 2,$$

  so that

$$z=(-1)^{m+n}z_0+(m+in)\varpi.$$

- Suppose at last that $\frac{z+z_0}{2} \notin \Omega$ (this case is more tricky). Then

$$\frac{z+z_0}{2} = (m+in)\frac{\varpi}{2}, \qquad m \equiv n \equiv 1 \pmod 2,$$

thus

$$z = -z_0 + (m+in)\varpi, \qquad m \equiv n \equiv 1 \pmod 2,$$

where the sign (-1) before z_0 is not equal to $(-1)^{m+n}$!?!

But fortunately, in this case, by Proposition 15.3.1,

$$\varphi(z) = \varphi(-z_0 + (m+in)\varpi) = (-1)^{m+n}\varphi(-z_0) = \varphi(-z_0) = -\varphi(z_0).$$

Since by hypothesis $\varphi(z) = \varphi(z_0)$, we obtain $\varphi(z_0) = -\varphi(z_0)$, thus $\varphi(z_0) = 0$, and $\varphi(z) = \varphi(z_0)$ is equivalent to $\varphi(z) = 0$.

By Proposition 15.3.2, $z_0 = (p+iq)\varpi, z = (r+is)\varpi$, where p, q, r, s are integers. Thus

$$z = z_0 + (r-p+i(s-q))\varpi = z_0 + (m'+in')\varpi, \text{ where } m' = r-p, n' = s-q \in \mathbb{Z},$$

and

$$z = -z_0 + (r+p+i(s+q)\varpi = -z_0 + (m''+in''), \text{ where } m'' = r+p, n'' = s+q \in \mathbb{Z}.$$

Note that $m'+n' \equiv m''+n'' \pmod 2$. If $m'+n'$ is even then $z = (-1)^{m'+n'}z_0 + (m'+in')\varpi$, and if $m'+n'$ is odd, then $z = (-1)^{m''+n''}z_0 + (m''+in'')\varpi$.

In all cases $z = (-1)^{m+n}z_0 + (m+in)\varpi$, for some $m, n \in \mathbb{Z}$. □

15.4 COMPLEX MULTIPLICATION

Ex. 15.4.1 *Prove (15.36).*

$$\varphi((1+i)z) = \frac{(1+i)\varphi(z)\varphi'(z)}{1-\varphi^4(z)},$$
$$\varphi((1-i)z) = \frac{(1-i)\varphi(z)\varphi'(z)}{1-\varphi^4(z)}.$$

Proof. Using the addition law together with (15.24):

$$\varphi(iz) = i\varphi(z), \qquad \varphi'(iz) = \varphi'(z),$$

we obtain

$$\begin{aligned}\varphi((1+i)z) &= \varphi(z+iz)\\ &= \frac{\varphi(z)\varphi'(iz) + \varphi'(z)\varphi(iz)}{1+\varphi^2(z)\varphi^2(iz)}\\ &= \frac{\varphi(z)\varphi'(z) + i\varphi'(z)\varphi(z)}{1-\varphi^4(z)}\\ &= \frac{(1+i)\varphi(z)\varphi'(z)}{1-\varphi^4(z)}.\end{aligned}$$

Similarly, using $\varphi(-z) = -\varphi(z), \varphi'(-z) = \varphi'(z)$, we have

$$\begin{aligned}
\varphi((1+i)z) &= \varphi(z - iz)\\
&= \frac{\varphi(z)\varphi'(iz) - \varphi'(z)\varphi(iz)}{1 + \varphi^2(z)\varphi^2(iz)}\\
&= \frac{\varphi(z)\varphi'(z) - i\varphi'(z)\varphi(z)}{1 - \varphi^4(z)}\\
&= \frac{(1-i)\varphi(z)\varphi'(z)}{1 - \varphi^4(z)}.
\end{aligned}$$

□

Ex. 15.4.2 *Let $\alpha \in \mathbb{Z}[i]$ be nonzero. The goal of this exercise is to prove part (a) of Lemma 15.4.2, which asserts that $|\mathbb{Z}[i]/\alpha\mathbb{Z}[i]| = N(\alpha)$. The idea is to forget multiplication and think of $\mathbb{Z}[i]$ and $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$ as groups under addition. let m be the greatest common divisor of the real and imaginary parts of α, so that $\alpha = m(a+bi)$, where* $\gcd(a,b) = 1$. *Then pick $c, d \in \mathbb{Z}$ such that $ad - bc = 1$.*

(a) Show that the map $\mathbb{Z}[i] \to \mathbb{Z} \oplus \mathbb{Z}$ defined by

$$\mu + \nu i \mapsto \mu(d, -b) + \nu(-c, a) = (\mu d - \nu c, -\mu b + \nu a)$$

is a group isomorphism under addition.

(b) Show that the map of part (a) takes α and $i\alpha$ to $(m, 0)$ and $-(m(ac+bd), m(a^2+b^2))$, respectively. Then use this to show that the map takes $\alpha\mathbb{Z}[i] \subset \mathbb{Z}[i]$ to the subgroup

$$m\mathbb{Z} \oplus m(a^2+b^2)\mathbb{Z} \subset \mathbb{Z} \oplus \mathbb{Z}.$$

(c) Use part (b) to conclude that $|\mathbb{Z}[i]/\alpha\mathbb{Z}[i]| = N(\alpha)$.

Proof.

(a) Consider

$$\psi \left\{ \begin{array}{ccl} \mathbb{Z}[i] & \to & \mathbb{Z} \oplus \mathbb{Z} \\ \mu + \nu i & \mapsto & \mu(d, -b) + \nu(-c, a) = (\mu d - \nu c, -\mu b + \nu a). \end{array} \right.$$

We verify that φ is a group homomorphism: if $z = \mu + \nu i, z' = \mu' + \nu' i \in \mathbb{Z}[i]$, then

$$\begin{aligned}
\psi(z + z') &= \psi((\mu + \mu') + i(\nu + \nu'))\\
&= (\mu + \mu')(d, -b) + (\nu + \nu')(-c, a)\\
&= [\mu(d, -b) + \nu(-c, a)] + [\mu'(d, -b) + \nu'(-c, a)]\\
&= \psi(z) + \psi(z').
\end{aligned}$$

Let (u, v) be any element of $\mathbb{Z} \oplus \mathbb{Z}$. For all $\mu + i\nu \in \mathbb{Z}[i]$, since $ad - bc = 1$,

$$\begin{aligned}
(u, v) = \psi(\mu + i\nu) &\iff \left\{ \begin{array}{rl} \mu d - \nu c &= u, \\ -\mu b + \nu a &= v, \end{array} \right.\\
&\Rightarrow \left\{ \begin{array}{l} \mu(ad - bc) = au + cv, \\ \nu(ad - bc) = bu + dv, \end{array} \right.\\
&\Rightarrow \left\{ \begin{array}{l} \mu = au + cv, \\ \nu = bu + dv. \end{array} \right.
\end{aligned}$$

Conversely, if $\mu = au + cv, \nu = bu + dv$, then

$$\left\{\begin{array}{rcl} \mu d - \nu c &=& (au+cv)d - (bu+dv)c = u(ad-bc) = u,\\ -\mu b + \nu a &=& -(au+cv)b + (bu+dv)a = v(ad-bc) = v. \end{array}\right.$$

We have proved, for all $z \in \mathbb{Z}[i]$, for all $(u,v) \in \mathbb{Z}\times\mathbb{Z}$, that

$$(u,v) = \psi(z) \iff z = (au+cv) + i(bu+dv)$$

This shows that ψ is bijective, and for all $(u,v) \in \mathbb{Z}\oplus\mathbb{Z}$,

$$\psi^{-1}(u,v) = (au+cv) + i(bu+dv) = (a+ib)u + (c+id)v.$$

To conclude, ψ is a group isomorphism.

(b) We compute the images of α and $i\alpha$ by the homomorphism ψ:

$$\begin{aligned} \psi(\alpha) &= \psi(ma + mbi)\\ &= ma(d,-b) + mb(-c,a)\\ &= (m(ad-bc),0)\\ &= (m,0),\\ \psi(i\alpha) &= \psi(-mb, ma)\\ &= -mb(d,-b) + ma(-c,a)\\ &= (-m(ac+bd), m(a^2+b^2)). \end{aligned}$$

$(\alpha, i\alpha)$ is a $\mathbb{Z}$-basis of $\alpha\mathbb{Z}[i]$, i.e. every element of $\alpha\mathbb{Z}[i]$ writes uniquely as a linear combination of $\alpha, i\alpha$ with integer coefficients. Moreover $\psi(\alpha) = (m,0) \in m\mathbb{Z}\times m(a^2+b^2)\mathbb{Z}$, and $\psi(i\alpha) = (-m(ac+bd), m(a^2+b^2)) \in m\mathbb{Z}\times(a^2+b^2)\mathbb{Z} = m\mathbb{Z}\oplus(a^2+b^2)\mathbb{Z}$, therefore

$$\psi(\alpha\mathbb{Z}[i]) \subset m\mathbb{Z}\oplus(a^2+b^2)\mathbb{Z}.$$

Conversely, let (u,v) be any element of $m\mathbb{Z}\times(a^2+b^2)\mathbb{Z}$. There are some $\lambda,\mu \in \mathbb{Z}$ such that

$$\begin{aligned} u &= \lambda m,\\ v &= \mu(a^2+b^2). \end{aligned}$$

Using the formula which gives $\psi^{-1}(u,v)$ in part (a), we obtain

$$\begin{aligned} \psi^{-1}(u,v) &= (a+ib)\lambda m + (c+id)\mu(a^2+b^2)\\ &= (a+ib)\left[\lambda m + \mu(c+id)(a-ib)\right], \end{aligned}$$

thus $\psi^{-1}(u,v) \in \alpha\mathbb{Z}[i]$, and $(u,v) \in \psi(\alpha\mathbb{Z}[i])$. This proves $m\mathbb{Z}\oplus(a^2+b^2)\mathbb{Z} \subset \psi(\alpha\mathbb{Z}[i])$, thus

$$\psi(\alpha\mathbb{Z}[i]) = m\mathbb{Z}\oplus(a^2+b^2)\mathbb{Z}.$$

(c) If A, B are Abelian groups, and I, J are subgroups of A, B respectively, the surjective homomorphism

$$\begin{array}{rl} A\times B & \to A/I \times B/J\\ (a,b) & \mapsto A/I\times B/J \end{array}$$

has kernel $I \times J$, so that

$$(A \times B)/(I \times J) \simeq A/I \times B/J.$$

This general property gives here

$$(\mathbb{Z} \oplus \mathbb{Z})/(m\mathbb{Z} \oplus (a^2 + b^2)\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/(a^2 + b^2)\mathbb{Z}.$$

Since the isomorphism ψ maps $\mathbb{Z}[i]$ on $\mathbb{Z} \oplus \mathbb{Z}$, and $\alpha\mathbb{Z}[i]$ on $m\mathbb{Z} \oplus (a^2 + b^2)\mathbb{Z}$, this implies

$$\mathbb{Z}[i]/\alpha\mathbb{Z}[i] \simeq (\mathbb{Z} \oplus \mathbb{Z})/(m\mathbb{Z} \oplus (a^2 + b^2)\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/(a^2 + b^2)\mathbb{Z}.$$

Therefore

$$|\mathbb{Z}[i]/\alpha\mathbb{Z}[i]| = |\mathbb{Z}/m\mathbb{Z}| \cdot |\mathbb{Z}/(a^2 + b^2)\mathbb{Z}| = m(a^2 + b^2) = N(\alpha).$$

□

Ex. 15.4.3 *Prove part (b) of Lemma 15.4.2.*

Proof. We prove that, assuming α is a prime in $\mathbb{Z}[i]$, that $\mathbb{Z}/\alpha\mathbb{Z}[i]$ is a field.

Since $\mathbb{Z}/\alpha\mathbb{Z}[i]$ is a ring, it is sufficient to prove that any nonzero $\overline{\beta} = \beta + \alpha\mathbb{Z}[i]$ has an inverse.

$\overline{\beta} \ne \overline{0}$ is equivalent to $\beta \notin \alpha\mathbb{Z}[i]$, so that α doesn't divide β in $\mathbb{Z}[i]$.

Since α is a prime in the principal ideal domain $\mathbb{Z}[i]$, α is relatively prime to β: if γ divides α and β, then γ is associate to 1 or α, but if γ is associate to α, then α divides β, and this contradicts the hypothesis, therefore γ is associate to 1. This proves that α is relatively prime to β.

Since $\mathbb{Z}[i]$ is a PID, this shows that there are some $\lambda, \mu \in \mathbb{Z}[i]$ such that

$$1 = \lambda\beta + \mu\alpha,$$

thus, using $\overline{\alpha} = \alpha + \alpha\mathbb{Z}[I] = \alpha\mathbb{Z}[i] = \overline{0}$,

$$\overline{1} = \overline{\lambda}\,\overline{\beta} + \overline{\mu}\,\overline{\alpha} = \overline{\lambda}\,\overline{\beta}.$$

This proves that $\overline{\beta} = \beta + \alpha\mathbb{Z}[i]$ has inverse $\overline{\lambda} = \lambda + \alpha\mathbb{Z}[i]$ in $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$.

If α is a prime in $\mathbb{Z}[i]$, then $\mathbb{Z}/\alpha\mathbb{Z}[i]$ is a field.

Moreover, by Exercise 2, $|\mathbb{Z}/\alpha\mathbb{Z}[i]| = N(\alpha)$, so that

$$\mathbb{Z}[i]/\alpha\mathbb{Z}[i] \simeq \mathbb{F}_{N(\alpha)}.$$

□

Ex. 15.4.4 *Prove (15.38).*

(a) $\alpha\beta$ *is odd* $\iff$ α *and* β *are odd.*

(b) $\alpha + \beta$ *is even* $\iff$ α, β *are both even or both odd.*

(c) α *is even* $\iff$ $1 + i$ *divides* α.

Proof. We say that a Gaussian integer $a + bi \in \mathbb{Z}[i]$ is *odd* if $a + b$ is odd ($b \equiv a + 1 \pmod 2$)and *even* if $a + b$ is even ($b \equiv a \pmod 2$).

(a) If $\alpha = a + bi$ and $\beta = c + di$ are odd, then $b \equiv a + 1, d \equiv c + 1 \pmod 2$, and $\alpha\beta = (a+bi)(c+di) = ac - bd + i(bc + ad) = A + Bi$, where

$$\begin{aligned} A + B &= ac - bd + bc + ad \\ &\equiv ac - (a+1)(c+1) + (a+1)c + a(c+1) \\ &\equiv 1 \pmod 2, \end{aligned}$$

thus $\alpha\beta$ is odd.

If α is even, then $b \equiv a \pmod 2$, thus

$$\begin{aligned} A + B &= ac - bd + bc + ad \\ &\equiv ac - a(c+1) + ac + a(c+1) \\ &\equiv 0 \pmod 2, \end{aligned}$$

thus $\alpha\beta$ is even, and symmetrically the same is true if β is even.

This proves

$$\alpha\beta \text{ is odd } \iff \alpha \text{ and } \beta \text{ are odd.}$$

(b) Now $\alpha + \beta = (a + c) + (b + d)i = C + Di$. If α, β are both even, then

$$\begin{aligned} C + D &= a + c + b + d \\ &\equiv a + c + a + c \equiv 0 \pmod 2. \end{aligned}$$

If $\alpha + \beta$ are both odd, then

$$\begin{aligned} C + D &= a + c + b + d \\ &\equiv a + c + a + 1 + c + 1 \equiv 0 \pmod 2. \end{aligned}$$

If α is odd, and β is even, or symmetrically, if α is even and β odd,

$$\begin{aligned} C + D &= a + c + b + d \\ &\equiv a + c + a + c + 1 \equiv 0 \pmod 2. \end{aligned}$$

This proves the equivalence

$$\alpha + \beta \text{ is even } \iff \alpha, \beta \text{ are both even or both odd.}$$

(c) If α is even, then $b \equiv a \pmod 2$, and $1 + i \mid 2 = (1+i)(1-i)$, therefore $b \equiv a \pmod{1+i}$, thus

$$\alpha = a + ib \equiv (1+i)a \equiv 0 \pmod{1+i},$$

thus $1 + i \mid \alpha$.

Conversely, if $1 + i \mid \alpha$, then $\alpha = \lambda(1+i)$ for some $\lambda \in \mathbb{Z}[i]$. Therefore $N(\alpha) = N(\lambda)N(1+i)$, so that $a^2 + b^2 = \alpha\overline{\alpha} = 2N(\lambda)$. Thus $a^2 + b^2 \equiv 0 \pmod 2$, which proves that a, b have same parity, thus $\alpha = a + bi$ is even. This shows the equivalence

$$\alpha \text{ is even } \iff 1 + i \text{ divides } \alpha.$$

$\square$

Note: The equivalence of part (c) gives a shorter proof of parts (a),(b). Since $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i] \simeq \mathbb{F}_2$ by Exercise 2, for every $\alpha \in \mathbb{Z}[i]$,

$$\alpha \equiv 0 \pmod{1+i} \quad \text{or} \quad \alpha \equiv 1 \pmod{1+i}.$$

Therefore,

$$\begin{aligned} \alpha \text{ is even} &\iff \alpha \equiv 0 \ (\mathrm{mod}\ 1+i), \\ \alpha \text{ is odd} &\iff \alpha \equiv 1 \ (\mathrm{mod}\ 1+i). \end{aligned}$$

Then

$$\begin{aligned} \alpha\beta \text{ is odd} &\iff \alpha\beta \equiv 1 \pmod{1+i} \\ &\iff \alpha \equiv 1 \text{ and } \beta \equiv 1 \pmod{1+i} \\ &\iff \alpha \text{ is odd and } \beta \text{ is odd.} \end{aligned}$$

and similarly,

$$\begin{aligned} \alpha + \beta \text{ is even} &\iff \alpha + \beta \equiv 0 \pmod{1+i} \\ &\iff \alpha \equiv \beta \equiv 0 \text{ or } \alpha \equiv \beta \equiv 1 \pmod{1+i} \\ &\iff \alpha, \beta \text{ are both even or both odd.} \end{aligned}$$