CHAPTER 17

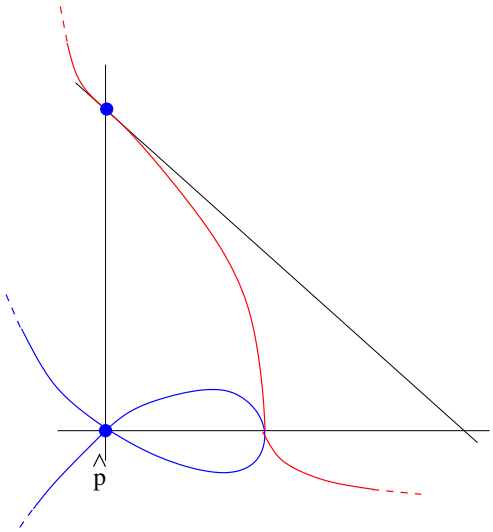
The singular cubic

Recall that a singular cubic curve[1] $D \subset \mathbb{P}^2$ is normalized via stereographic projection through its singular point $\hat{p}$; that is, we get a normalization morphism

$$\sigma : \mathbb{P}^1 \to \mathbb{P}^2$$

with image D. In particular, all singular cubics have normalization of genus zero. Moreover, they are all projectively equivalent to one of two examples.

The nodal cubic. Recall that a "node" is just an ordinary double point. Let $D = \{Y^2Z = X^2(Z - X)\}$; the affine equation is $y^2 = x^2(1 - x)$ and a schematic picture is



where I have denoted points with real coordinates in blue and points with only x-coordinate real in red. (How these sit inside the full set of

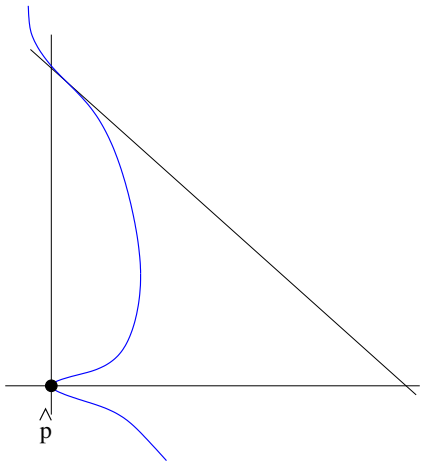
[1] D is for "degenerate"!

complex points will be pictured below; the dotted stuff will connect up.) By Exercise 5 of Chapter 3, this is parametrized by

$$\begin{aligned} \varphi : \mathbb{P}^1/\{0,\infty\} &\xrightarrow{\cong} D \\ t &\longmapsto \left(\frac{-4t}{(1-t)^2}, \frac{-t(1+t)}{(1-t)^3} \right) =: (x(t), y(t)). \end{aligned}$$

The "$\mathbb{P}^1/\{0,\infty\}$" means the Riemann sphere with the top and bottom points identified.[2]

The cuspidal cubic. Take $D = \{Y^2Z = X^3\}$, with affine equation $y^2 = x^3$, and schematic picture



where I have only drawn real points. To do stereographic projection through the cusp $(0,0)$, write $y = \frac{1}{t}x$ and substitute to get $\frac{1}{t^2}x^2 = x^3 \implies x = \frac{1}{t^2}$. Hence we get a normalization

$$\varphi : \mathbb{P}^1 \to D$$

defined by

$$t \mapsto \left[1 : \frac{1}{t^2} : \frac{1}{t^3}\right].$$

[2]Sending $[T_0 : T_1] \longmapsto [(T_0 - T_1)^3 : -4T_1T_0(T_0 - T_1) : -T_1T_0(T_0 + T_1)]$ homogenizes the formula for φ, and then it is clear that $\varphi(1) = \varphi([1:1]) = [0:0:1]$.

One of our overarching themes in the next few chapters will be the study of algebro-geometrically defined group laws on cubics. In this chapter, we focus on the above two singular examples, as the smooth case is more difficult. For the nodal cubic, the law will turn out to be equivalent (via φ) to multiplication on $\mathbb{C}^* = \mathbb{P}^1\backslash\{0,\infty\}$; while in the cuspidal case, it identifies with addition on $\mathbb{C} = \mathbb{P}^1\backslash\{\infty\}$. In both cases, these sets are the preimages under normalization of the smooth points of D, which is where the group laws will be defined.

In the course of studying such laws as well as "addition theorems" on these curves, we will pull back rational functions on $\mathbb{P}^2$ (quotients of homogeneous polynomials of equal degree, or equivalently elements of $\mathbb{C}(x,y)$) to get meromorphic functions on $\mathbb{P}^1$ (the normalization of our curve). So in illustrating the simplicity of the group law, hence

Principle 1: *Singularities make curves of a given degree more trivial and easier to study,*

we will be seeing a concrete example of the following

Principle 2: *Given $C \subset \mathbb{P}^2$ an* irreducible *algebraic curve with normalization $\sigma : \tilde{C} \to \mathbb{P}^2$, every $f \in \mathcal{K}(\tilde{C})$ is of the form $\sigma^* F$, $F \in \mathbb{C}(x,y)$.*

In other words, writing $C_0 := C \cap (\mathbb{P}^2\backslash\{Z = 0\})$ for the affine part of C and $g_{C_0}(x,y)$ for its defining equation, if we define

$$\mathbb{C}[C_0] := \frac{\mathbb{C}[x,y]}{(g_{C_0})}, \qquad \begin{aligned} \mathbb{C}(C) &:= \text{ fraction field of } \mathbb{C}[C_0] \\ &\cong \left\{ \sigma^* F \;\middle|\; \begin{array}{l} F \in \mathbb{C}(x,y) \\ F \not\equiv \infty \text{ on } C \end{array} \right\}, \end{aligned}$$

then Principle 2 says that

$$\begin{array}{ccc} \mathcal{K}(\tilde{C}) & \cong & \mathbb{C}(C). \\ \text{analytic} & & \text{algebraic} \end{array}$$

Since C was projective, $\tilde{C}$ is compact, and that turns out to be of fundamental importance: e.g., $\mathbb{C}[C_0]$ is only a subring of, rather than

equal to, the ring of holomorphic functions on (the desingularization of) C_0. But the holomorphic functions *not* in $\mathbb{C}[C_0]$ have essential singularities at infinity so aren't in $\mathcal{K}(\tilde{C})$.

Before continuing on, we should address one point: why should the only possible singularities of an irreducible cubic C be an ordinary double point (node) or cusp, and why must it have only one? First of all, if it had two singular points, then we could take a line L through those two points. Both intersection multiplicities (of C with L at these two points) would have to be ≥ 2, and so $(C \cdot L) \geq 4$ in violation of Bézout. (See what a useful theorem this is?) So C can only have one singular point, and as its equation is of degree 3 that point can only be of order 2 or 3. If it is of order 3, then by Exercise 5 of Chapter 6, C is a union of 3 lines, contradicting irreducibility.

Finally, the local equation about a *non*-ordinary double point of C can only be of the form $x^2 + f_3(x, y) = 0$, with f_3 homogeneous of degree 3. An explicit local analytic transformation puts this in the form $(\tilde{x})^2 + (\tilde{y})^3 = 0$. So it is a cusp. Alternately, anything which looks like $x^2 + y^n = 0$ has intersection multiplicity n with the line $x = 0$, again violating Bézout (in the context of our cubic curve) if $n > 3$.

17.1. Warm-up: Functions on a nonsingular conic

Our smooth conic is named C. Any $F \in \mathcal{K}(C)$ can be viewed as a map $C \to \mathbb{P}^1$. Composing this with the stereographically produced normalization $\sigma : \mathbb{P}^1 \xrightarrow{\cong} C$, yields

$$\mathbb{P}^1 \xrightarrow[\sigma]{\cong} C \xrightarrow[F]{} \mathbb{P}^1, \qquad \sigma^* F$$

that is, a meromorphic function on $\mathbb{P}^1$. Since $\mathcal{K}(\mathbb{P}^1) = \mathbb{C}(t)$ (with $t := T_1/T_0$), $\sigma^* F$ must be of the form

$$\frac{g(t)}{h(t)} = \frac{G(T_0, T_1)}{H(T_0, T_1)}$$

where g, h, G, H are polynomials and G, H are homogeneous of the same degree. By the fundamental theorem of algebra, we can write this as

$$\gamma \cdot T_0^N \frac{\prod_i (T_1 - \alpha_i T_0)^{m_i}}{\prod_j (T_1 - \beta_j T_0)^{n_j}},$$

for some $\gamma, \alpha_i, \beta_j \in \mathbb{C}$. As $\deg G = \deg H \implies N + \sum m_i - \sum n_j = 0$, the expression simplifies to

$$\gamma \frac{\prod (t - \alpha_i)^{m_i}}{\prod (t - \beta_j)^{n_j}} \ (= \ (\sigma^* F)(t)).$$

Note that

$$(\sigma^* F)(\infty) \neq 0, \infty \quad \iff \quad \sum m_i = \sum n_j. \tag{17.1.1}$$

17.2. Functions on a singular cubic (nodal case)

Let $F : D \to \mathbb{P}^1$ be

$$\begin{gathered} \text{the restriction to } D \text{ of a rational function on } \mathbb{P}^2 \\ \text{which is well-defined and } \neq 0, \infty \\ \text{at the singular point } \hat{p} \in D. \end{gathered} \tag{17.2.1}$$

Since the normalization $\mathbb{P}^1 \to D$ sends $0, \infty \mapsto \hat{p}$ but is otherwise 1-to-1, we get

$$\left(\mathbb{P}^1 / \{0, \infty\}\right) \xrightarrow[\cong]{\varphi} D \xrightarrow{F} \mathbb{P}^1, \qquad \varphi^* F : \left(\mathbb{P}^1 / \{0, \infty\}\right) \to \mathbb{P}^1$$

with $F(0) = F(\infty) \in \mathbb{C}^*$. Henceforth we shall, by abuse of notation, refer to this composition as F.

Thinking of F as a meromorphic function on $\mathbb{P}^1$, (17.1.1) applies and we get

$$F(t) = \gamma \frac{\prod (t - \alpha_i)^{m_i}}{\prod (t - \beta_j)^{n_j}} \quad \text{with } \sum m_i = \sum n_j.$$

Furthermore,

$$\gamma = F(\infty) = F(0) = \gamma \frac{\prod \alpha_i^{m_i}}{\prod \beta_j^{n_j}}$$

so that

$$\prod \alpha_i^{m_i} = \prod \beta_j^{n_j}, \tag{17.2.2}$$

relating the t-coordinates of the zeroes and poles of F.

Now introduce the multivalued function

$$u := \int_1^* \frac{dt}{t} = \log(t)$$

on $\mathbb{P}^1$, which takes well-defined values in $\mathbb{C}/2\pi\sqrt{-1}\mathbb{Z}$. We can restate (17.2.2) in terms of u: viz.,

$$\sum_{p \in D} \nu_p(F) \cdot u(p) \equiv 0 \mod 2\pi\sqrt{-1}\mathbb{Z}.$$

This leads to *Abel's theorem for the singular cubic*. To state it, recall that divisors on a complex 1-manifold are formal sums of points with integer coefficients; a divisor is *effective* if none of those coefficients are negative.

17.2.3. PROPOSITION. *Given $\mathcal{P}, \mathcal{Z} \in Div(D \backslash \hat{p})$ effective divisors of the same degree,*

$$\int_{\mathcal{P}}^{\mathcal{Z}} \frac{dt}{t} \equiv 0 \mod 2\pi\sqrt{-1}\mathbb{Z} \iff \left.\begin{array}{c} \mathcal{P} = poles \\ \mathcal{Z} = zeroes \end{array}\right\} \text{ of some } F \text{ as in } (17.2.1).$$

Explicitly, if $\mathcal{P} = \sum n_j[\beta_j]$ and $\mathcal{Z} = \sum m_i[\alpha_i]$ are of the same degree ($d = \sum n_j = \sum m_i$), then we may write

$$\mathcal{Z} - \mathcal{P} = \sum_{k=1}^{d} ([z_k] - [p_k]),$$

and then $\int_{\mathcal{P}}^{\mathcal{Z}} := \sum \int_{p_k}^{z_k}$ for some choice of paths from p_k to z_k. Also, in the statement "poles" and "zeroes" are as usual meant with multiplicity. This is a first "baby" case of a general statement for algebraic curves (Abel's theorem) connecting integrals of 1-forms to the question of when a divisor is the divisor of a meromorphic function.

17.3. Group law on the nodal cubic

Fix a normalization[3]

$$\begin{aligned}\varphi : \left(\mathbb{P}^1/\{0,\infty\}\right) &\xrightarrow{\cong} D \\ t &\longmapsto (x(t), y(t)) \\ 1 &\longmapsto \varphi(1) =: \mathbf{e}.\end{aligned}$$

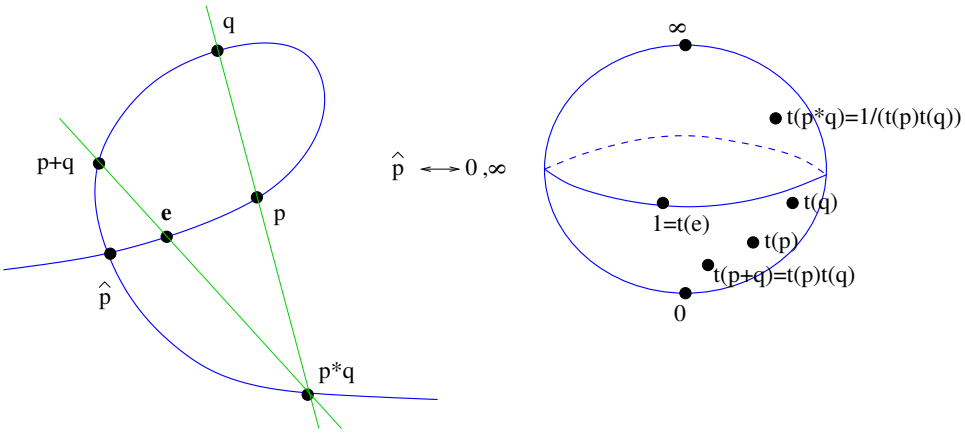
Let $p, q \in D$ be arbitrary nonsingular points, and L_{pq} be the line through p and q. (If they are the same, then take L to be the tangent line T_pD.) By Bézout, $(L_{pq} \cdot D) = 3$ and so L_{pq} meets D in a third point which we call $p * q$. More precisely, everything is counted with multiplicity ($p * q$ need not be distinct from p or q) so we really mean

$$[p * q] := L_{pq} \cdot D - [p] - [q].$$

Now let L' be the line through $p * q$ and $\mathbf{e}$ (or $T_{\mathbf{e}}D$ if they coincide), and put

$$[p + q] := L' \cdot D - [p * q] - [\mathbf{e}].$$

That is, $p + q$ is the "extra" intersection point of this line with D guaranteed by Bézout. Here's a useful picture of the construction:



Now writing f_L for the equation of a line L, observe that

$$F := \left.\frac{f_{L_{pq}}}{f_{L'}}\right|_D : D \longrightarrow \mathbb{P}^1$$

[3] In homogeneous coordinates, we will write $\varphi(t) = [Z(t) : X(t) : Y(t)]$.

satisfies (17.2.1). In terms of the t-coordinate on $\mathbb{P}^1$, i.e. pulling F back along φ, we must have:

$$F(t) = \gamma \frac{(t-t(p))(t-t(q))(t-t(p*q))}{(t-t(p+q))(t-1)(t-t(p*q))} = \gamma \frac{(t-t(p))(t-t(q))}{(t-t(p+q))(t-1)}.$$

But since $F(0) = F(\infty)$, by (17.2.2)

$$\prod\{\text{locations of zeroes}\} = \prod\{\text{locations of poles}\}$$
$$\implies \quad t(p)\cdot t(q) = t(p+q)\cdot \underbrace{t(\mathbf{e})}_{1} = t(p+q).$$

This identifies the group law (multiplication) on $\mathbb{C}^* = \mathbb{P}^1\backslash\{0,\infty\}$ with the one just defined on $D\backslash\hat{p}$. Alternately, taking log gives

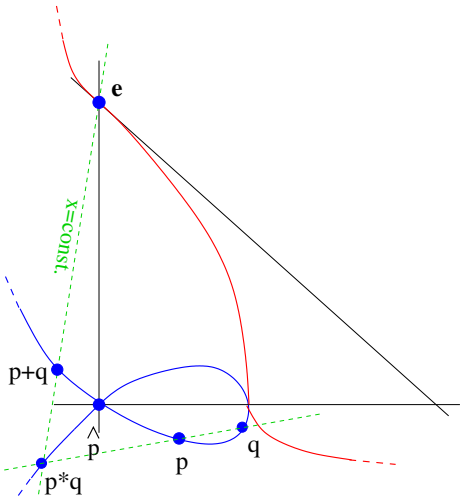
$$u(p)+u(q) \equiv u(p+q) \mod 2\pi\sqrt{-1}\mathbb{Z},$$

identifying addition on $D\backslash\hat{p}$ with addition in $\mathbb{C}/2\pi\sqrt{-1}\mathbb{Z}$. This may be rewritten

$$\int_1^{t(p)} \frac{dt}{t} + \int_1^{t(q)} \frac{dt}{t} \equiv \int_1^{t(p+q)} \frac{dt}{t} \mod 2\pi\sqrt{-1}\mathbb{Z}. \tag{17.3.1}$$

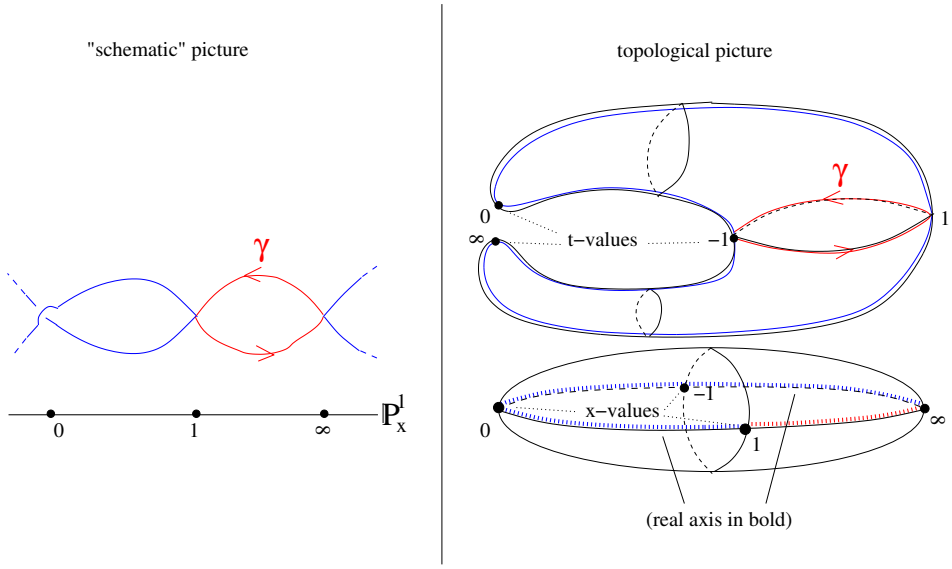
17.4. Addition theorems for the nodal cubic

Let's unwind the "equivalence of group laws" in the nodal cubic example from the beginning of the chapter. Noting that $\mathbf{e} := \varphi(1) = [0:0:1]$, here is a picture of how the group law works:



In particular, the x-coordinates of $p+q$ and $p*q$ are the same, while the y-coordinates are $\pm$ of each other.

Just to clarify the topology of the situation, here is what the projection of the normalization of D onto the x-axis looks like:



It is a 2-sheeted cover with 2 branch points, with the closed path γ indicating the "equator" (or unit circle $|t|=1$) on the upper $\mathbb{P}^1$ (i.e. $\tilde{D}$).

Now we get to work. Start by "inverting" the equivalence $t(p)\cdot t(q)=t(p+q)$:

$$\underbrace{\varphi(t_1)}_{p}+\underbrace{\varphi(t_2)}_{q}=\underbrace{\varphi(t_1\cdot t_2)}_{p+q}.$$

Since p, q, and $p*q$ are collinear by construction,

$$0=\det\begin{pmatrix} Z(p) & Z(q) & Z(p*q)\\ X(p) & X(q) & X(p*q)\\ Y(p) & Y(q) & Y(p*q)\end{pmatrix}.$$

Assuming none of them is **e**, $Z(p)Z(q)Z(p*q)\neq 0$ and we get the

1st addition theorem:

$$0 = \det \begin{pmatrix} 1 & 1 & 1 \\ x(t_1) & x(t_2) & x(t_1 \cdot t_2) \\ y(t_1) & y(t_2) & -y(t_1 \cdot t_2) \end{pmatrix}.$$

This allows you to compute $x(t_1 \cdot t_2)$ from $x(t_1)$ and $x(t_2)$, using the equation of D to write $y(t) = \pm x(t)\sqrt{1 - x(t)}$.

Next,

$$\varphi^* \left(\frac{dx}{y}\Big|_D \right) = \frac{d(x(t))}{y(t)} = \cdots [\text{use Exercise 4 from Ch. 13}] \cdots = \frac{dt}{t},$$

while $\frac{dx}{y}\Big|_D = \frac{dx}{\pm x\sqrt{1-x}}$; so (17.3.1) may be expressed

$$\int_{x(\mathbf{e})(=\infty)}^{x(p)} \frac{dx}{x\sqrt{1-x}} + \int_{x(\mathbf{e})}^{x(q)} \frac{dx}{x\sqrt{1-x}} \equiv \int_{x(\mathbf{e})}^{x(p+q)} \frac{dx}{x\sqrt{1-x}}.$$

(Note that $2\pi\sqrt{-1} = \oint_{|t|=1} \frac{dt}{t} = \int_\gamma \frac{dx}{y}$. Going modulo its integer multiples, which is what "$\equiv$" means here, is necessary not to have the equation's correctness depend upon the choice of paths from ∞ to $x(p)$, to $x(q)$, and to $x(p+q)$.) Solving

$$\det \begin{pmatrix} 1 & 1 & 1 \\ x(p) & x(q) & x(p+q) \\ x(p)\sqrt{1-x(p)} & x(q)\sqrt{1-x(q)} & -x(p+q)\sqrt{1-x(p+q)} \end{pmatrix} = 0$$

for $x(p+q)$ yields

$$x(p+q) = \frac{-x(p)x(q)}{\left(\sqrt{1-x(p)} + \sqrt{1-x(q)}\right)^2}.$$

Forgetting the association with $p, q, p+q \in D$ we get the

2nd addition theorem: Modulo $2\pi\sqrt{-1}\mathbb{Z}$,

$$\int_\infty^{x_1} \frac{dx}{x\sqrt{1-x}} + \int_\infty^{x_2} \frac{dx}{x\sqrt{1-x}} \equiv \int_\infty^{\frac{-x_1x_2}{(\sqrt{1-x_1}+\sqrt{1-x_2})^2}} \frac{dx}{x\sqrt{1-x}}.$$

Note that $\int_\infty^x \frac{dx}{x\sqrt{1-x}} = \log\left(\frac{\sqrt{1-x}-1}{\sqrt{1-x}+1}\right)$ by explicit computation of the integral. (One way to view this function is $\log(t)\,(= u)$ viewed as

a multivalued function of x.) So we have discovered a functional equation for $\log\left(\frac{\sqrt{1-x}-1}{\sqrt{1-x}+1}\right)$, which is ugly to check by hand.

One aspect of the game we have just played here is: start with a "natural" choice of differential 1-form on the curve (if possible, one which is smooth away from any singularities of the curve). In the above, this was $\frac{dx}{y}|_D$. You can think of this as a multivalued 1-form on the x-axis, and then D is the "existence domain of the 1-form" over $\mathbb{P}^1_x$. Then you integrate this 1-form, which gives a transcendental function which is multivalued even on D (you have to go to its universal cover to make it well-defined), and try to produce a functional equation for it (as a function of x). In the last section we'll summarize this story for a couple of other curves.

17.5. Other addition theorems (conic, cuspidal cubic)

Consider the example $C = \{y^2 + x^2 = 1\}$, parametrized by $\mathbb{P}^1$ via

$$t \overset{\varphi}{\longmapsto} \left(\frac{-2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$$

as in §3.3. We compute

$$\varphi^*\left(\left.\frac{dx}{y}\right|_C\right) = \frac{2dt}{t^2+1} = 2d(\arctan(t)),$$

$$\left.\frac{dx}{y}\right|_C = \frac{dx}{\sqrt{1-x^2}} = d(\arcsin(x)).$$

On the universal cover of $\mathbb{P}^1_x \backslash \{\pm 1\}$ let $\theta = \arcsin(x)$ (starting at $x = 0 \leftrightarrow t = 0 \leftrightarrow \theta = 0$).[4] Its role is similar to that of $u = \log t$ above, as the integral of our chosen differential 1-form on the curve; θ takes well-defined values in $\mathbb{C}/2\pi\mathbb{Z}$. Writing $x(\theta_1) =: x_1$, $x(\theta_2) =: x_2$,

[4]Note: $t \mapsto \frac{-2t}{t^2+1} = x$ is a degree-2 map (from C to the x-axis) with ramification points $t = \pm 1$ over $x = \pm 1$. On the complements of these points, we have a 2-to-1 map $\mathbb{C}^* \to \mathbb{C}^*$. The universal cover of $\mathbb{C}^*$ is $\mathbb{C}$, and so we have maps $\mathbb{C} \to \mathbb{C}^*_t \to \mathbb{C}^*_x$ sending θ to t to x. So our setup encodes the relation $\frac{-2\tan\frac{\theta}{2}}{(\tan\frac{\theta}{2})^2+1} = x(t(\theta)) = x(\theta) = \sin(\theta)$.

$x(\theta_1+\theta_2) =: x_{12}$, the standard trigonometry relations give

$$x_{12} = x_1\sqrt{1-x_2^2} + x_2\sqrt{1-x_1^2}.$$

The "second addition formula" for the conic then reads

$$\int_0^{x_1} \frac{dx}{\sqrt{1-x^2}} + \int_0^{x_2} \frac{dx}{\sqrt{1-x^2}} \equiv \int_0^{x_{12}} \frac{dx}{\sqrt{1-x^2}} \mod 2\pi\mathbb{Z},$$

which is a functional equation for *arcsin*. More simply put, it is just the inverse of the trigonometric identity.

Next, look back to the cuspidal example from the beginning of the chapter. We have

$$\varphi^*\left(\left.\frac{dx}{y}\right|_D\right) = \frac{d(x(t))}{y(t)} = \frac{d\left(\frac{1}{t^2}\right)}{\frac{1}{t^3}} = -2dt,$$

while

$$\left.\frac{dx}{y}\right|_D = \frac{dx}{x^{\frac{3}{2}}}.$$

(Note that this time, the integral of $\frac{dx}{y}|_D$ is just $-2t$ and is *not* multi-valued on D.) Clearly if $t_{12} = t_1 + t_2$, then

$$\int_0^{t_1} dt + \int_0^{t_2} dt = \int_0^{t_{12}} dt$$

$$\Longrightarrow \quad \int_\infty^{\frac{1}{t_1^2}(=x(t_1))} \frac{dx}{x^{\frac{3}{2}}} + \int_\infty^{\frac{1}{t_2^2}(=x(t_2))} \frac{dx}{x^{\frac{3}{2}}} = \int_\infty^{\frac{1}{t_{12}^2}(=x(t_1+t_2))} \frac{dx}{x^{\frac{3}{2}}}.$$

So we get a functional equation for $\frac{1}{\sqrt{x}}$, which is unfortunately rather stupid: it says

$$\frac{1}{\left(\frac{1}{t_1^2}\right)^{\frac{1}{2}}} + \frac{1}{\left(\frac{1}{t_2^2}\right)^{\frac{1}{2}}} = \frac{1}{\left(\frac{1}{(t_1+t_2)^2}\right)^{\frac{1}{2}}}.$$

In an exercise below, you will show a less trivial addition theorem for the cuspidal cubic, to the effect that

$$P, Q, R \in (D\backslash\hat{p}) \text{ are collinear} \iff t(P) + t(Q) + t(R) = 0.$$

Exercises

(1) Consider the cuspidal cubic curve $D = \{Y^2Z = X^3\} \subseteq \mathbb{P}^2$ and normalize it as above, with $\varphi : \mathbb{P}^1 \to D$ given by $t \mapsto [1 : \frac{1}{t^2} : \frac{1}{t^3}] = [Z : X : Y]$. (The singular point is $\hat{p} = [1 : 0 : 0]$.) Prove directly that the group law given by addition on $(\mathbb{P}^1 \backslash \{\infty\}) \cong \mathbb{C}$ (namely, $t_1, t_2 \mapsto t_1 + t_2$) corresponds to the following process on $(D \backslash \{\hat{p}\})$: take the line L through $\varphi(t_1)$ and $\varphi(t_2)$, then a line L' through the third intersection point $\varphi(t_1) * \varphi(t_2)$ (of L with D) and the "neutral" point $[0 : 0 : 1]$, and finally locate the third intersection point of this L' with D to get "$\varphi(t_1) + \varphi(t_2)$" (also as above, for the nodal cubic). Do this simply *by showing that* $P, Q, R \in (D \backslash \{\hat{p}\})$ *are collinear if and only if* $t(P) + t(Q) + t(R) = 0$. (Here P, Q, R are distinct.) [Hint: use the determinant of the matrix

$$\begin{pmatrix} a^3 & a & 1 \\ b^3 & b & 1 \\ c^3 & c & 1 \end{pmatrix},$$

and rewrite $[1 : \frac{1}{t^2} : \frac{1}{t^3}] = [t^3 : t : 1]$.]

(2) Geometrically define a "group law" on the conic $C = \{x^2 + y^2 = 1\}$ minus two points (which ones?) that matches addition in θ (as in the beginning of §17.5). [Hint: add a line (which line?) and treat it as a cubic.]

(3) Let d be a squarefree positive integer. The units $\mathbb{Z}[\sqrt{d}]^* \subset \mathbb{Z}[\sqrt{d}]$ are the elements $a + b\sqrt{d}$ with norm $a^2 - db^2 = \pm 1$. (Assume for simplicity that -1 does not occur, e.g. $d = 3, 6, 7, 11, \ldots$.) By adding the line at infinity to

$$C = \{x^2 - dy^2 = 1\},$$

and taking $\mathbf{e} := (1, 0)$, define a group law on this affine curve. Show that the map $\mathbb{Z}[\sqrt{d}]^* \to C(\mathbb{Z})$ (integer points) defined by $a + b\sqrt{d} \mapsto (a, b)$ is an isomorphism of groups.[5]

[5] It turns out that the group $\mathbb{Z}[\sqrt{d}]^*$ always is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$, with elements of the form $\pm u^\ell$ for some "fundamental unit" u. By calculating u, you can thus find all integer points on the curve – that is, all integer solutions to *Pell's equation*.

(4) Show that the integer points on the curves $x^2 - 5y^2 = 4$ and $x^2 - 5y^2 = -4$ have y-coordinates the Fibonacci numbers (up to sign). You may assume that $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]^* = \{\pm u^\ell \mid \ell \in \mathbb{Z}\}$ with $u = \frac{1+\sqrt{5}}{2}$, and sending $\frac{a+b\sqrt{5}}{2} \mapsto (a, b)$ covers all integer points of both curves. [Hint: writing $u^\ell = \frac{x_\ell + y_\ell\sqrt{5}}{2}$, what is $y_{\ell-2} + y_{\ell-1}$?]

(5) (a) Check explicitly that $\mathbf{e}$ is the identity of the group law on $D \setminus \hat{p}$ in §17.3. [Note: here $\mathbf{e} \in D \setminus \hat{p}$ is arbitrary.] (b) Verify that, with $D\,(= \{Y^2Z = X^2(Z - X)\})$ and $\mathbf{e}\,(= [0{:}0{:}1])$ as in §17.4, $p * q$ is the inverse of $p + q$ in the group law.

(6) Check the computation of $x(p + q)$ just before the 2nd addition theorem in §17.4.

(7) Let C be a quartic with three nodes p_0, p_1, p_2. (a) Geometrically define a group law on $C \setminus \{p_0\}$ (or rather, its normalization). [Hint: use conics, not lines.] (b) In Example 14.4.1, replace t by a different coordinate on $\mathbb{P}^1$ to make your law correspond to multiplication (in $\mathbb{C}^*$).