

1 Addition Law

1.1 Definitions and Notation

Definition 1: Let K be a field with $\text{char}(K) \neq 2, 3, 5$ and \overline{K} its algebraic closure. Define the hyperelliptic curve of genus two $H_0(K)$ as the set of solutions in K^2 to the equation $y^2 = C(x)$ where

$$C(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e$$

is a polynomial over K . Similarly, the set of solutions in the closure would be denoted $H_0(\overline{K})$. Define $H(K)$ as $H_0(\overline{K}) \cup \{\infty\}$.

Note that we could obtain a more reduced form of $C(x)$, eliminating a by shifting x to $x - a/5$. However, since this would rob us of the possibility of $\text{char}(K) = 5$ without simplifying our coming calculations in any significant manner, we shall be reluctant towards using this trick.

For the purpose of clarity, let points on the hyperelliptic curve — in the sense of solutions to $y^2 = C(x)$ — be designated by the calligraphic letter $\mathcal{Q} = (x, y) \in H_0(\overline{K})$. The point opposite to \mathcal{Q} will be written $\overline{\mathcal{Q}} = (x, -y)$ and by symmetry of the curve in y also belongs to $H_0(\overline{K})$. In the case where $\mathcal{Q} = \infty$, define $\overline{\mathcal{Q}} = \infty$.

We want to consider the set of all pairs $(\mathcal{Q}_1, \mathcal{Q}_2)$ and tame it with an equivalence relation with the goal of obtaining an additive group:

Definition 2: Define \mathbf{J} to be the set \mathcal{J}/\sim where $\mathcal{J} = H(\overline{K}) \times H(\overline{K})$. It is called the “Jacobian” and the equivalence relation is defined by

$$\begin{aligned} (\mathcal{Q}_1, \mathcal{Q}_2) &\sim (\mathcal{Q}_2, \mathcal{Q}_1) \\ \text{and } (\mathcal{Q}, \overline{\mathcal{Q}}) &\sim (\infty, \infty). \end{aligned}$$

Write $\{\mathcal{Q}_1, \mathcal{Q}_2\}$ from now on and let bold letters denote points on the curve in the sense of classes of unordered pairs $\mathbf{P} = \{\mathcal{Q}_1, \mathcal{Q}_2\} \in \mathbf{J}$. The point $\{\overline{\mathcal{Q}}_1, \overline{\mathcal{Q}}_2\}$ will be called $\overline{\mathbf{P}}$ for now but can already tentatively be thought of as $-\mathbf{P}$. Call $\{\infty, \infty\}$ the zero of our set. Call \mathcal{Q}_i a point-component.

A point $\mathcal{Q} = (x_0, y_0)$ is called singular if it fulfills both $y_0 = 0$ and $C'(x_0) = 0$. A curve is called singular if and only if it has a singular point. We consider only non-singular hyperelliptics from here on; this amounts to $C(x)$ having no repeated factors over \overline{K} (“squarefree”).

1.2 The General Case

Let's start with $\mathbf{P}_1 = \{\mathcal{Q}_1, \mathcal{Q}_2\}$, $\mathbf{P}_2 = \{\mathcal{Q}_3, \mathcal{Q}_4\}$ with $\mathcal{Q}_i = (x_i, y_i) \in H_0(K)$ or $\mathcal{Q}_i = \infty$. To define $\mathbf{P}_3 = \mathbf{P}_1 + \mathbf{P}_2$ we distinguish between one general case and a number of special cases and first derive the results of the former before enumerating the latter ones.

CASE 1, FOUR DISTINCT POINT-COMPONENTS: Let $\mathcal{Q}_i \in H_0(K)$ and \mathbf{P}_i be defined as above with $x_i \neq x_j$ whenever $i \neq j$.

The overarching idea is to obtain a fifth and sixth x -coordinate and the corresponding y -coordinates by passing a polynomial of degree three through the four points \mathcal{Q}_i . Ideally this should give us two additional intersections with the curve which we then use as the components of our point $\mathbf{P}_1 + \mathbf{P}_2$.

STEP 1: It is known that the Vandermonde matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}$$

has determinant $\prod_{i < j} (x_i - x_j)$ which is conveniently non-zero if and only if the x_i are pairwise distinct. Let $p(x) = p_3x^3 + p_2x^2 + p_1x + p_0 \in \overline{K}[x]$ be the polynomial in unknown coefficients that we are looking for. With $\mathbf{y} = (y_1 \ y_2 \ y_3 \ y_4)^t$ and $\mathbf{p} = (p_0 \ p_1 \ p_2 \ p_3)^t$, the problem of determining $p(x)$ can be rewritten as

$$V \cdot \mathbf{p} = \mathbf{y}$$

which by invertibility of V has a unique solution for \mathbf{p} with $p_i \in K$.

Note that the leading coefficient of $p(x)$ is

$$p_3 = \frac{1}{\det(V)} \begin{vmatrix} 1 & x_1 & x_1^2 & y_1 \\ 1 & x_2 & x_2^2 & y_2 \\ 1 & x_3 & x_3^2 & y_3 \\ 1 & x_4 & x_4^2 & y_4 \end{vmatrix}$$

and the next step will depend on whether $p(x)$ is truly of degree 3 or not.

Define	$D(x) = C(x) - (p(x))^2.$	(*)
--------	---------------------------	-----

STEP 2A: Knowing the coefficients p_i we first assume $p_3 \neq 0$ so we can proceed to look for the additional solutions of the sextic equation $D(x) = 0$. Observe that this vanishes at x_1, x_2, x_3 and x_4 , so write the lefthand side as

$$D(x) = -p_3^2(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)(x - x_6) \quad (*_1)$$

for x_5 and x_6 unknowns in \overline{K} . Comparing the coefficients at x^4 and x^5 yields

$$\sum_{\substack{i,j=1 \\ i < j}}^6 x_i x_j = T_4$$

and

$$\sum_{i=1}^6 x_i = T_5$$

where $T_4 = \frac{p_2^2 + 2p_1 p_3 - a}{p_3^2}$ and $T_5 = \frac{1 - 2p_2 p_3}{p_3^2}$. The first expression gives

$$x_6 \sum_{i=1}^5 x_i + \sum_{\substack{i,j=1 \\ i < j}}^5 x_i x_j = T_4.$$

Replacing x_6 by $T_4 - \sum_{\substack{i,j=1 \\ i < j}}^5 x_i x_j$ gives the tidy quadratic equation

$$x^2 - \left(T_5 - \sum_{i=1}^4 x_i \right) \cdot x + \left(T_4 - T_5 \sum_{i=1}^4 x_i + \sum_{\substack{i,j=1 \\ i \leq j}}^4 x_i x_j \right) = 0 \quad (\dagger)$$

of which x_5 is one solution and — by symmetry of the above steps — x_6 the other one. Compute $y_i = p(x_i)$ for $i = 5, 6$ to obtain $\mathcal{Q}_5 = \{x_5, y_5\}$ and $\mathcal{Q}_6 = \{x_6, y_6\}$, at which point it becomes clear that the worst-case scenario for our field extension to accommodate the new coordinates is to be quadratic. Finally we define $\mathbf{P}_1 + \mathbf{P}_2$ to be equal to $\mathbf{P}_3 = \{\overline{\mathcal{Q}}_5, \overline{\mathcal{Q}}_6\}$.

STEP 2B: If p_3 were zero, the equation $(*)$ would be quintic instead. We may therefore write the lefthand side factorized, so we get a different $D(x)$,

$$D(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5), \quad (*)$$

again for x_5 somewhere in \overline{K} . We used the tag $(*)_1$ twice to refer to both equations. Defining $T_{4\infty} = p_2^2 - a$ and comparing the coefficients at x^4 gives

$$x_5 = T_{4\infty} - \sum_{i=1}^4 x_i \quad (\ddagger)$$

and we may rejoice in the implication of x_5 staying in K .

Compute $y_5 = p(x_5)$ and define $\mathbf{P}_1 + \mathbf{P}_2$ to be the point $\mathbf{P}_3 = \{(x_5, -y_5), \infty\}$.

STEP 1': To extend our construction from $H_0(K)$ to $H(K)$ we now consider $\mathcal{Q}_4 = \infty$ with the other $\mathcal{Q}_i = (x_i, y_i)$ as before. This can be seen as the x_i still being pairwise distinct, only that one of them is allowed to be ∞ here.

There is no coordinate x_4 this time, so we pass a quadratic polynomial $p(x)$ through the remaining three points (x_i, y_i) . This means that we solve the linear system $\tilde{V} \cdot \mathbf{p} = \tilde{\mathbf{y}}$ where \tilde{V} is the Vandermonde matrix for $x_i, i = 1, \dots, 3$,

$$\tilde{V} = \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix}$$

As before, the leading coefficient of $p(x)$ might or might not be zero, but $(*)$ will be quintic in either case, so we only have to worry about one step 2.

STEP 2': Doing a coefficient comparison at x^3 and at x^4 in $(*)$ through

$$D(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_5)(x - x_6), \quad (*'_1)$$

gives
$$\sum_{\substack{i,j=1 \\ i < j}}^3 x_i x_j + x_5 \sum_{i=1}^3 x_i + x_6 \sum_{i=1}^3 x_i + x_5 x_6 = b - 2p_1 p_2$$

and
$$\sum_{i=1}^3 x_i + x_5 + x_6 = p_2^2 - a.$$

Call the righthand terms $T_{3\infty}$ and $T_{4\infty}$, combine both equations and obtain

$$x^2 - \left(T_{4\infty} - \sum_{i=1}^3 x_i \right) \cdot x + \left(T_{3\infty} - T_{4\infty} \sum_{i=1}^3 x_i + \sum_{\substack{i,j=1 \\ i \leq j}}^3 x_i x_j \right) \quad (\dagger')$$

Solve, call the two solutions x_5 and x_6 , compute y_5 and y_6 through $p(x_5)$ and $p(x_6)$ and define $\mathbf{P}_1 + \mathbf{P}_2$ to be $\mathbf{P}_3 = \{(x_5, -y_5), (x_6, -y_6)\} = \{\overline{\mathcal{Q}}_5, \overline{\mathcal{Q}}_6\}$.

Remark 1: Up to this point, we have given the general-case rule only for elements in $H(K) \times H(K)$. Extending to $\mathcal{J} = H(\overline{K}) \times H(\overline{K})$ is trivial as we can simply choose \overline{K} as the new K . The final step is to note that everything until now is well-defined on \mathbf{J} . The equivalence relation from Definition 2 corresponds to interchanging \mathcal{Q}_1 and \mathcal{Q}_2 or \mathcal{Q}_3 and \mathcal{Q}_4 or both. To this end we can check that interchanging (x_i, y_i) and (x_j, y_j) does nothing to the resulting \mathcal{Q}_5 and \mathcal{Q}_6 . This is the case because $p(x)$ depends only on the solution of the linear system $V \cdot \mathbf{p} = \mathbf{y}$ on which the aforementioned permutation has no effect. With p invariant, the subsequent steps remain unchanged as well.

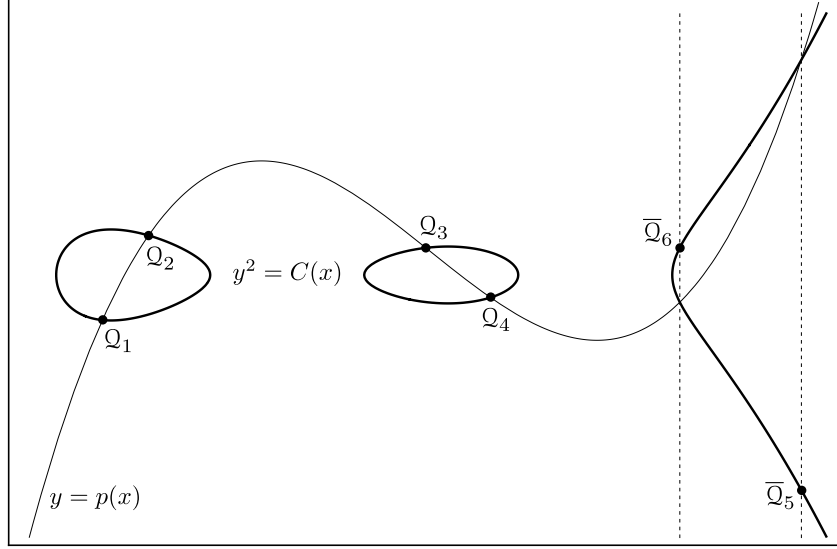
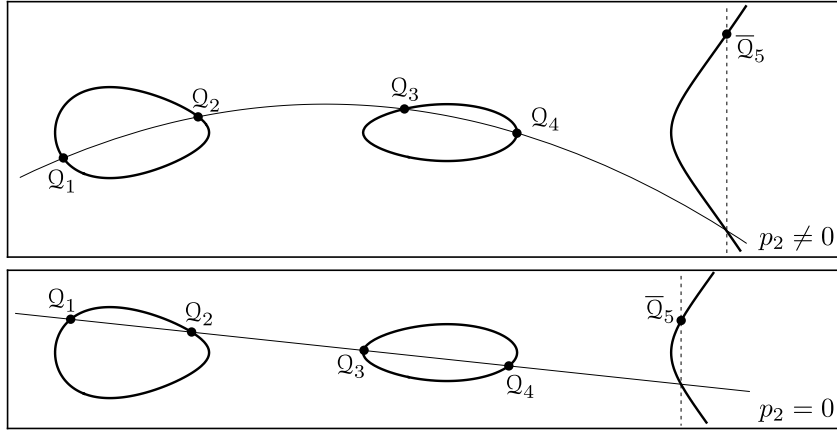


FIGURE 1A: The general case for the addition law in \mathbb{R}^2 where $p_3 \neq 0$.



FIGURES 1B and 1C: If $p_3 = 0$ we have at most five intersections.

Finally, the restriction to K instead of \overline{K} was to showcase the degree of the required field extension, a feat we will now leave aside by always using \overline{K} .

Before we begin listing the special cases, we impose the following property: The sum of any $\mathbf{P}_1 = \{Q_1, Q_2\}$ and $\mathbf{P}_2 = \{Q_3, Q_4\}$ in \mathbf{J} fulfills the equality

$$\mathbf{P}_1 + \mathbf{P}_2 = \{Q_3, Q_2\} + \{Q_1, Q_4\}. \quad (\diamond)$$

Note that the general-case addition we just defined already fulfills this, as we noted before that interchanging any of the (x_i, y_i) does not impact the solution \mathbf{p} of the linear system nor any of the dagger equations.

Remark 2: The property (\diamond) corresponds to the permutation $(1\ 3)$ on the point-components \mathcal{Q}_i . With Definition 2 allowing the permutations $(1\ 2)$ and $(3\ 4)$ this naturally leads to the observation that in fact all permutations of point-components must now leave the sum unchanged. In fact it is easy to check that the three transpositions generate all of S_4 and the remark above already provides compatibility with the construction of the general case.

A substantial bonus of this is the fact that commutativity corresponds to the permutation $(1\ 3)(2\ 4)$ which by the above we now obtained for free.

1.3 Complete List of Cases

We may now impose conditions on the relations between the \mathcal{Q}_i without mentioning whether they belong to \mathbf{P}_1 or \mathbf{P}_2 . As a result, the list of special cases can be written in a significantly more concise manner.

As we strive to define $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\}$, for any $\mathcal{Q}_i = (x_i, y_i) \in H_0(\overline{K})$ or $\mathcal{Q}_i = \infty \in H(\overline{K})$ we observe that the following simplification takes place:

Let $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Whenever $\mathcal{Q}_i = \overline{\mathcal{Q}}_j$ for $i \neq j$ we have

$$\begin{aligned} \{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\} &= \{\mathcal{Q}_i, \mathcal{Q}_j\} + \{\mathcal{Q}_k, \mathcal{Q}_l\} \\ &= \{\mathcal{Q}_k, \mathcal{Q}_l\} + \{\mathcal{Q}_j, \overline{\mathcal{Q}}_j\} \\ &= \{\mathcal{Q}_k, \mathcal{Q}_l\} + \{\infty, \infty\} = \{\mathcal{Q}_k, \mathcal{Q}_l\} \end{aligned} \quad (0)$$

The justification for this follows directly from Remark 2 and Definition 2. It is easily checked that this sum remains well defined if the choice of i and j is not unique. This allows us to treat the above as a separate case in order to characterize the other cases solely through the x -coordinates of the \mathcal{Q}_i , so we may assume

$$x_i = x_j \iff \mathcal{Q}_i = \mathcal{Q}_j$$

for any $\mathcal{Q}_i, \mathcal{Q}_j \in H(\overline{K})$, provided we assign $\mathcal{Q}_i = \infty$ the x -coordinate $x_i = \infty$. There is a possibility for ambiguity of “ ∞ ” here, which we will however avoid later on by making it obvious which infinity we are working with.

We may now write the distinction between the remaining cases as follows:

1. The general case where x_1, x_2, x_3, x_4 are pairwise distinct.
2. The case where exactly two of x_1, x_2, x_3, x_4 are equal.
3. The case where x_1, x_2, x_3, x_4 are equal in pairs.
4. The case where exactly three of x_1, x_2, x_3, x_4 are equal.
5. The case where where all of x_1, x_2, x_3, x_4 are equal.

Since we are allowed to permute point-components anyway, we may fix which of the \mathcal{Q}_i are equal and write everything out for the complete and final list.

Given the addition $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\}$, distinguish between the following:

0. The addition with zero, i.e. $\mathcal{Q}_1 = \overline{\mathcal{Q}}_2$ with $\mathcal{Q}_i \in H(\overline{K})$ for $i = 1, \dots, 4$.
 1. The general case where $\mathcal{Q}_i \neq \mathcal{Q}_j$ and $\mathcal{Q}_i \neq \overline{\mathcal{Q}}_j$ for $i \neq j$.
 2. The single tangential case where all \mathcal{Q}_i as in case 1 with the exception of $\mathcal{Q}_1 = \mathcal{Q}_2 \in H_0(\overline{K})$ with $y_1 \neq 0$.
 3. The double tangential case where all \mathcal{Q}_i as in case 1 with the exception of $\mathcal{Q}_1 = \mathcal{Q}_2 \in H_0(\overline{K})$ with $y_1 \neq 0$ and $\mathcal{Q}_3 = \mathcal{Q}_4 \in H_0(\overline{K})$ with $y_3 \neq 0$.
 4. The triple point case wherein $\mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3 \in H_0(\overline{K})$ with $y_1 \neq 0$ and $\mathcal{Q}_4 \in H(\overline{K})$ differs from both \mathcal{Q}_1 and $\overline{\mathcal{Q}}_1$.
 5. The quadruple point case where all $\mathcal{Q}_i \in H_0(\overline{K})$ are equal with $y_1 \neq 0$.
-

Remark 3:

- (i) In both lists, the cases do not overlap.
- (ii) For the list to be complete, we must allow for $\mathcal{Q}_i = \infty$ for some i . Note that one is sufficient, since if two or more \mathcal{Q}_i were to be ∞ , we would be back at the case 0 by virtue of (\diamond) , bringing the two infinities together in one point. As we did for case 1, we consider $\mathcal{Q}_i \in H_0(\overline{K})$ and $\mathcal{Q}_i \in H(\overline{K})$ in two separate cases and postpone handling the latter.
- (iii) As for the first case, the constructions will a priori only be made on \mathcal{J} . It remains to check that this makes indeed for a well-defined addition on \mathbf{J} by being invariant under interchanges of \mathcal{Q}_i and \mathcal{Q}_j for any i, j .

1.4 Addition Law for the Special Cases

Before we handle the next construction steps we need an intermediate result.

Lemma 1: If the derivatives $D(\tau) = D'(\tau) = \dots = D^{(k-1)}(\tau) = 0$ for a polynomial D over a field of characteristic 0 or $p \geq k$ then

$$(t - \tau)^k \mid D(t).$$

Proof. Assume $\tau = 0$ by shifting t to $t + \tau$. With $D(t) = \sum_{i=0}^d a_i t^i$ we have

$$a_i = \frac{1}{i!} D^{(i)}(0) = 0 \quad i = 0, \dots, k-1$$

so t^k divides $D(t)$. □

We will now use this property on $D(x) = C(x) - (p(x))^2$ when factoring $(*)$.

CASE 0, ADDITION WITH ZERO: As anticipated, (0) gives $\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_1$ for every $\mathbf{P}_1 \in \mathbf{J}$ if $\mathbf{P}_2 = \{\mathcal{Q}, \overline{\mathcal{Q}}\} = 0$. Similarly $\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_2$ if $\mathbf{P}_1 = 0$.

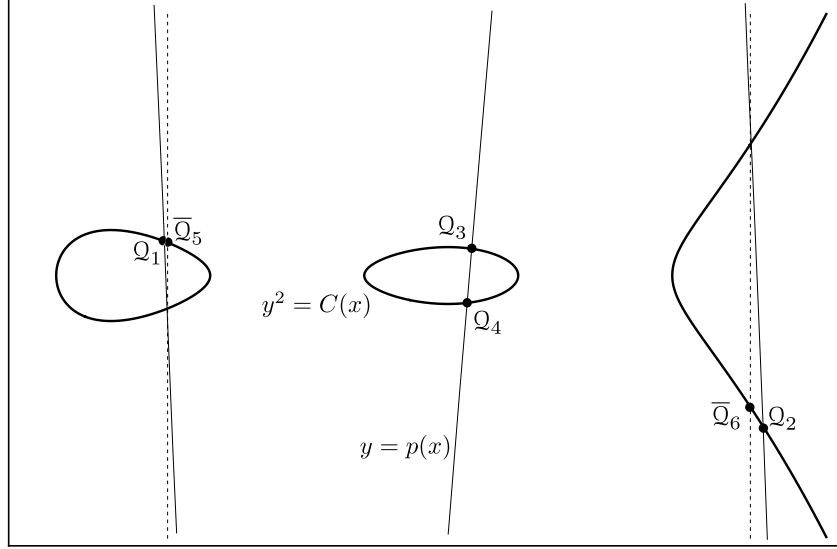


FIGURE 0A: Illustrating a limit argument where \mathcal{Q}_3 is very close to $\overline{\mathcal{Q}}_4$.

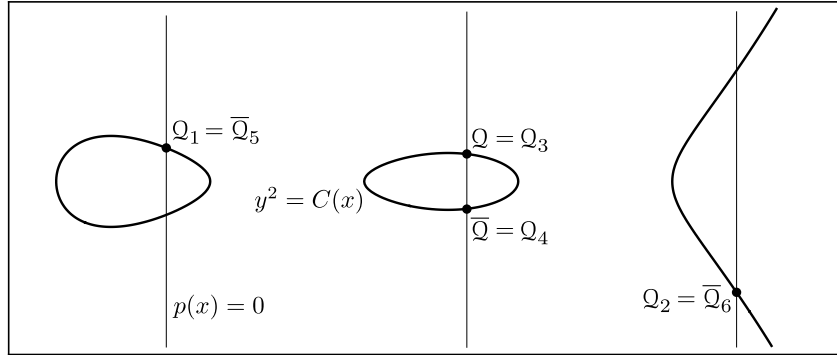


FIGURE 0B The addition with zero and justifying $\{\mathcal{Q}, \overline{\mathcal{Q}}\} \sim 0$.

CASE 2, TANGENTIAL: Let $\mathcal{Q}_i \in H_0(\overline{K})$, $\mathcal{Q}_1 = \mathcal{Q}_2$, $y_1 \neq 0$ but x_1 , x_3 and x_4 are pairwise distinct. We cannot use the Vandermonde matrix in this case because it won't possess maximal rank, consequently being non-invertible. We can however obtain an additional equation by demanding that our poly-

nomial $p(x)$ be tangential to the curve at Q_1 . This gives

$$2y \frac{dy}{dx} = 5x^4 + 4ax^3 + 3bx^2 + 2cx + d$$

and

$$\frac{dy}{dx} = 3p_3x^2 + 2p_2x + p_1$$

meaning that the system to solve for \mathbf{p} is now $V_1 \cdot \mathbf{p} = \mathbf{y}_1$ with

$$V_1 = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 0 & 1 & 2x_1 & 3x_1^2 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}.$$

The subscript indicates at which points the intersections have higher order. Here \mathbf{y}_1 is defined as \mathbf{y} with y_2 replaced by $y'_2 = \frac{C'(x_1)}{2y_1}$ where $C'(x)$ is the derivative of C and $2y_1 \neq 0$ because $\text{char}(\bar{K}) \neq 2$ and $y_1 \neq 0$. Since $\det(V_1) = (x_4 - x_1)^2(x_3 - x_1)^2(x_4 - x_3)$ this fits neatly into our constraints by being non-zero exactly in the case where x_1, x_3 and x_4 are pairwise distinct.

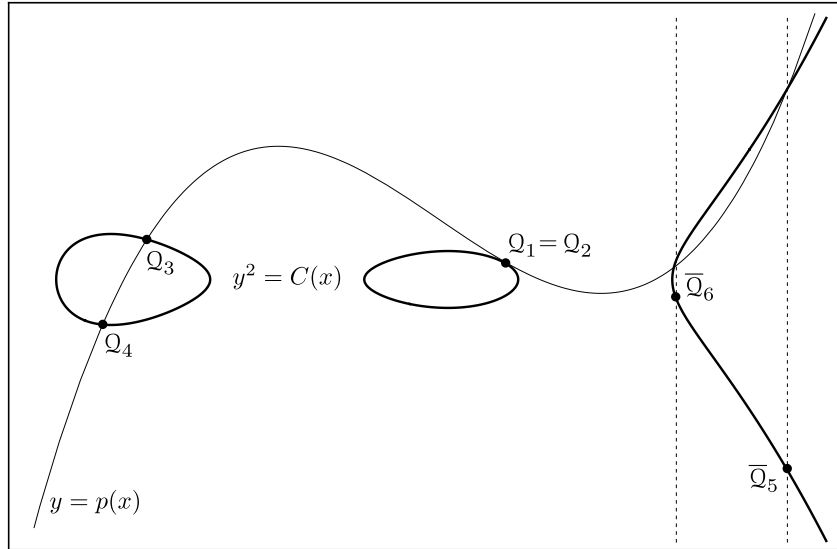


FIGURE 2: The case of a tangential intersection at Q_1 .

Once the polynomial is determined, we note that the $p^2(x)$ shares a tangent with $C(x)$ at x_1 on purpose, specifically

$$\begin{aligned} D'(x_1) &= C'(x_1) - 2p(x_1)p'(x_1) \\ &= C'(x_1) - 2y_1y'_2 = 0 \end{aligned}$$

so we use Lemma 1 to see that the lefthand side of $(*)$ either factors as

$$D(x) = -p_3^2(x - x_1)^2 \prod_{i=3}^6 (x - x_i) \quad (*_2)$$

or

$$D(x) = (x - x_1)^2 \prod_{i=3}^5 (x - x_i).$$

Now step two will be entirely identical to that of the general case and we can again solve (\ddagger) or (\dagger) for x_5 or x_5 and x_6 .

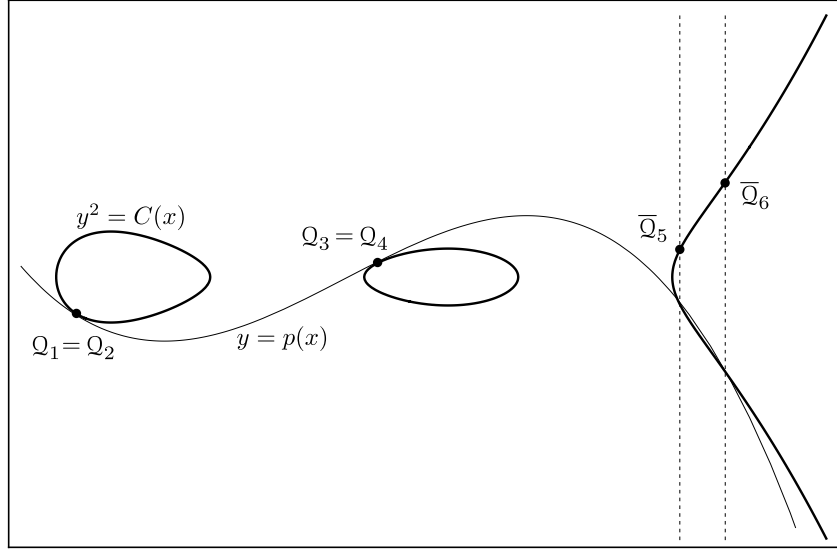


FIGURE 3: Two tangential intersection at Q_1 and Q_3 respectively.

CASE 3, DOUBLE TANGENTIAL: Let $Q_i \in H_0(\bar{K})$, $Q_1 = Q_2$ and $Q_3 = Q_4$ but $x_1 \neq x_3$ and $Q_i \neq \bar{Q}_i$ meaning that neither y_1 nor y_3 will be zero. As before, we lack equations for our linear system, requiring the use of a second tangential constraint. Replace the fourth row of V_1 and \mathbf{y}_1 exactly like we did for the second one: $y'_4 = \frac{C'(x_3)}{2y_3}$ and

$$V_{13} = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 0 & 1 & 2x_1 & 3x_1^2 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 0 & 1 & 2x_3 & 3x_3^2 \end{pmatrix}.$$

Now $\det(V_{13}) = (x_3 - x_1)^4$ and this is again different from zero precisely whenever $x_3 \neq x_1$, so as before solve $V_{13} \cdot \mathbf{p} = \mathbf{y}_{13}$ for \mathbf{p} , then note that

$D(x)$ has double zeroes at x_1 and x_3 by the same argument as in case 2. By Lemma 1 we know that $(*)$ has a factor $(x - x_1)^2(x - x_3)^2$ so we use

$$D(x) = -p_3^2(x - x_1)^2(x - x_3)^2(x - x_5)(x - x_6) \quad (*_3)$$

or $D(x) = (x - x_1)^2(x - x_3)^2(x - x_5).$

and the procedure of case 1 with $x_2 = x_1$ and $x_4 = x_3$ to solve (\dagger) or (\ddagger) .

CASE 4, TRIPLE POINT: Let $\mathcal{Q}_i \in H_0(\overline{K})$, $\mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3$ but $x_1 \neq x_4$ and $y_1 \neq 0$. We can thus see this as a third-order intersection and demand that the curve and the polynomial share a second-order derivative at \mathcal{Q}_1 :

$$V_{11} = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 0 & 1 & 2x_1 & 3x_1^2 \\ 0 & 0 & 2 & 6x_1 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}.$$

Here $\det(V_{11}) = 2(x_4 - x_1)^3$ and with this, define \mathbf{y}_{11} by taking \mathbf{y}_1 and replacing the third coordinate by $y_3'' = \frac{C''(x_1)}{2y_1} - \frac{(C'(x_1))^2}{4y_1^3}$ where $C''(x)$ is the second-order derivative of C .

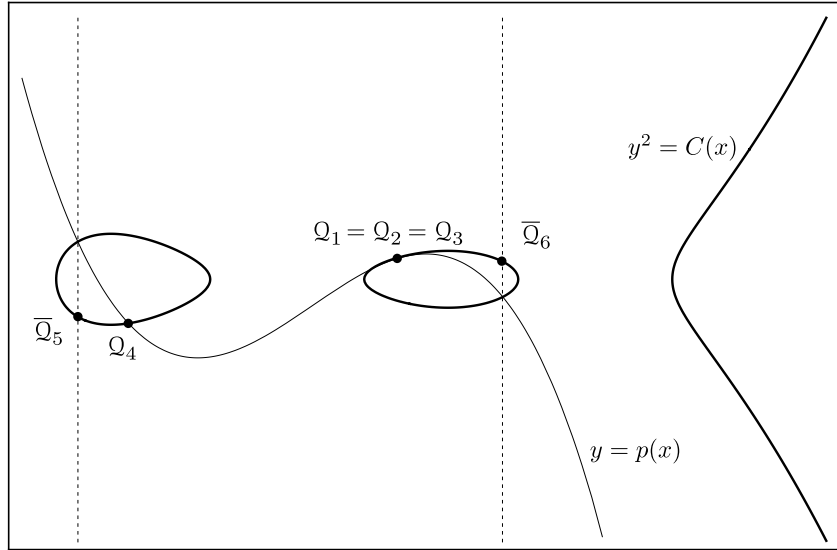


FIGURE 4: An intersection of order three at \mathcal{Q}_1 .

Apply Lemma 1 as in case 2, only this time we also have

$$\begin{aligned} D''(x_1) &= C'''(x_1) - 2p(x_1)p''(x_1) - 2(p'(x_1))^2 \\ &= C'''(x_1) - 2y_1y_3'' - 2(y_2')^2 = 0 \end{aligned}$$

as can be checked by glancing at the definition of y_3'' . With $(*)$ factoring as

$$D(x) = -p_3^2(x - x_1)^3 \prod_{i=4}^6 (x - x_i) \quad (*_4)$$

or

$$D(x) = (x - x_1)^3 \prod_{i=4}^5 (x - x_i),$$

this allows us to continue with one of the second steps of case 1 to find \mathbf{P}_3 .

CASE 5, QUADRUPLE POINT: Given the situation where $\mathcal{Q}_i = \mathcal{Q}_1 \in H_0(\overline{K})$ for every i with $y_1 \neq 0$, we use

$$V_{111} = \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 0 & 1 & 2x_1 & 3x_1^2 \\ 0 & 0 & 2 & 6x_1 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

which is invertible in all fields but those of characteristic 2 and 3.

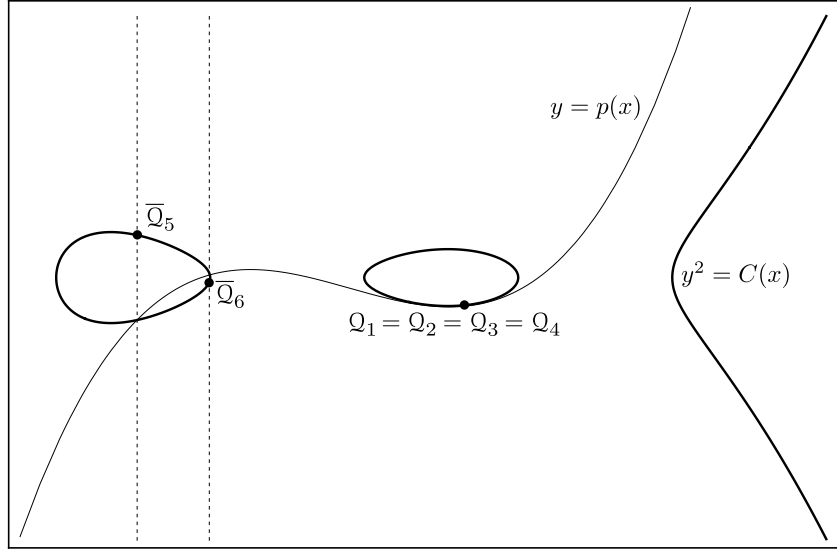


FIGURE 5: An intersection of order four at \mathcal{Q}_1 .

Here \mathbf{y}_{111} is the same as \mathbf{y}_{11} except for the last coordinate which should read

$$y_4''' = \frac{C'''(x_1)}{2y_1} - \frac{3C'(x_1)C''(x_1)}{4y_1^3} + \frac{3(C'(x_1))^3}{8y_1^5}$$

where $C'''(x)$ is the third-order derivative of C . Once more, we solve the linear system $V_{111} \cdot \mathbf{p} = \mathbf{y}_{111}$. In addition to $D^{(i)}(x_1) = 0, i = 0, \dots, 2$ we have

$$D'''(x_1) = C'''(x_1) - 2y_1y_4''' - 6y_2'y_3'' = 0$$

$$\begin{aligned} \text{so either} \quad & D(x) = -p_3^2(x - x_1)^4(x - x_5)(x - x_6) \\ \text{or} \quad & D(x) = (x - x_1)^4(x - x_5) \end{aligned} \tag{*5}$$

which we subsequently use to solve (\dagger) or (\ddagger) and we're done.

~

Finally, as noted in Remark 3, (ii) we have yet to extend our definition from $H_0(\overline{K})$ to $H(\overline{K})$. Observe that this is only relevant for cases number two and four where we now consider $\mathcal{Q}_4 = \infty$ as we did in STEP 1' of the general case. As an analogue to this, the relevant matrices \tilde{V}_1 and \tilde{V}_{11} will be the upper-left 3×3 sub-matrices of their $H_0(\overline{K})$ -counterparts V_1 and V_{11} .

In both cases we obtain a linear system of the form $\tilde{V}_* \cdot \mathbf{p} = \tilde{\mathbf{y}}_*$ for a three-element vector \mathbf{p} and the vectors $\tilde{\mathbf{y}}_1$ and $\tilde{\mathbf{y}}_{11}$ are defined like their 4-element counterparts \mathbf{y}_1 and \mathbf{y}_{11} with the last coordinate omitted.

Both matrices \tilde{V}_* are invertible and we therefore get a unique polynomial $p(x)$ which we use to solve (\dagger') , obtaining $x_5, x_6, y_5 = p(x_5)$ and $y_6 = p(x_6)$ in \overline{K} and we define $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \infty\} = \{\overline{\mathcal{Q}}_5, \overline{\mathcal{Q}}_6\} = \{(x_5, -y_5), (x_6, -y_6)\}$.

The counterparts to $(*_2)$ and $(*_4)$ in these cases are

$$D(x) = (x - x_1)^2(x - x_3)(x - x_5)(x - x_6) \tag{(*'_2)}$$

$$\text{and} \quad D(x) = (x - x_1)^3(x - x_5)(x - x_6) \tag{(*'_4)}$$

1.5 Well-Definedness of the Addition Law

To check whether our addition is well defined on \mathbf{J} in each of the cases, we have to consider the permutation of point-components \mathcal{Q}_i under the equivalence relation from Definition 2. Furthermore, to claim that all possible cases are all covered, it is necessary to check the permutations under (\diamond) . Both cases can be combined into a single one by the following statement:

Lemma 2: In each given definition of “+”, the result is invariant under the interchange of \mathcal{Q}_i and \mathcal{Q}_j .

Proof. Simultaneously interchanging $x_i \rightleftharpoons x_j$ and $y_i \rightleftharpoons y_j$ in our linear systems $V_* \cdot \mathbf{p} = \mathbf{y}_*$ has the effect of permuting the rows of V_* and \mathbf{y}_* and relabeling (x_k, y_k) whenever \mathcal{Q}_k was equal to \mathcal{Q}_i or \mathcal{Q}_j .

Consequently the resulting $p(x)$ doesn't change, so neither do any of the terms T_* . The three dagger equations remain unchanged as well, as can easily be checked at (\dagger) , (\ddagger) and (\dagger') which are invariant under $x_i \rightleftharpoons x_j$.

Finally, the version of Step 2 we fall into remains the same, since it is only imposed by the distinction of p_3 being zero or not. \square

2 Rational Functions on Hyperelliptics

The goal of this chapter is to look at rational functions on the hyperelliptic curve $y^2 = C(x)$ and to define a notion of the order of a function in a point on the curve. We then give some basic properties for this order function before we introduce divisors and proceed to look at functions with a specified number of poles at ∞ as a preparation for the proof of associativity on **J**.

2.1 Function Field and Order of Rational Functions

Definition 3: Define the ring of rational functions on the curve as

$$\mathcal{F} = K(x)[y] / (y^2 - C(x)).$$

As $y^2 - C(x)$ is irreducible in $K(x)[y]$, \mathcal{F} is a field and $\mathcal{F} = K(x) + K(x)y$, so write elements $f \in \mathcal{F}$ as $f = g + hy$ where $g, h \in K(x)$. Define $\bar{f} = g - hy$.

We will occasionally write things like $K[x, y] \subset \mathcal{F}$ but this is always implicitly understood to be in conjunction with $y^2 = C(x)$.

Reminders: A formal Laurent series written $\tau = \gamma t^e(1 + \dots) \in K((t))$ with $\gamma \in K^*$, $e \in \mathbb{Z}$ has a unique inverse $\tau^{-1} = \gamma^{-1}t^{-e}(1 + \dots) \in K((t))$.

From now on we will use an ellipsis to denote any terms of ascending order everywhere where we are not interested in the specifics.

If $\text{char}(K) \neq 2$ and τ is a series of the form $\tau = 1 + \sum_{i=1}^{\infty} a_i t^i$ then it has a unique square root of the form $\sigma = 1 + \sum_{i=1}^{\infty} b_i t^i$ in $\bar{K}((t))$ meaning $\sigma^2 = \tau$. Write $\sigma = \sqrt{\tau} = 1 + \dots$.

~

In order to define the order of a function f in a point \mathcal{Q} , $\text{ord}_{\mathcal{Q}}(f) \in \mathbb{Z}$ for $f \in \mathcal{F}^*$ and $\mathcal{Q} \in H(\bar{K})$ we first construct a K -homomorphism

$$\lambda_{\mathcal{Q}} : \mathcal{F} \rightarrow \bar{K}((t))$$

Because $C(\lambda_{\mathcal{Q}}(x)) = (\lambda_{\mathcal{Q}}(y))^2$ has to be fulfilled, we decide on $\lambda_{\mathcal{Q}}(x)$ and deduce $\lambda_{\mathcal{Q}}(y)$. For this, we distinguish between three cases for $\mathcal{Q} \in H(\bar{K})$.

Definition 4: 1. Let $\mathcal{Q} = (x_0, y_0) \in H_0(\overline{K})$ with $y_0 \neq 0$ and consequently $C(x_0) \neq 0$.

Define $\lambda_{\mathcal{Q}}(x) = x_0 + t$. Now

$$\begin{aligned} C(\lambda_{\mathcal{Q}}(x)) &= C(x_0 + t) \\ &= C(x_0) + \cdots + t^5 \\ &= C(x_0)(1 + \cdots) \\ &= y_0^2 \tau_1 \quad \text{with } \tau_1 \in K((t)). \end{aligned}$$

Define $\lambda_{\mathcal{Q}}(y) = y_0 \sqrt{\tau_1}$.

2. Let $\mathcal{Q} = (x_0, y_0) \in H_0(\overline{K})$ with $y_0 = 0$. Points with this property are called “Weierstrass Points” and as $C(x_0) = 0$ there are at most five of them. Write $C(x) = \prod_{i=1}^5 (x - \alpha_i)$ for $\alpha_i \in \overline{K}$ and for instance $\alpha_1 = x_0$.

Define $\lambda_{\mathcal{Q}}(x) = x_0 + t^2$. Now

$$\begin{aligned} C(\lambda_{\mathcal{Q}}(x)) &= t^2 \prod_{i=2}^5 (x_0 - \alpha_i + t^2) \\ &= \mu t^2 (1 + \cdots) \end{aligned}$$

with $\mu \in \overline{K}$ being $\mu = \prod_{i=2}^5 (x_0 - \alpha_i) = C'(x_0)$ which is non-zero because our curve is non-singular. Write therefore $C(\lambda_{\mathcal{Q}}(x)) = \mu t^2 \tau_2$ with τ_2 of the form $1 + \cdots$ and define $\lambda_{\mathcal{Q}}(y) = \nu t \sqrt{\tau_2}$ with $\nu^2 = \mu$, $\nu \in \overline{K}$.

Note that we may choose one out of two square roots for ν so whichever we take we demand that we stay consistent in our choice for now. It will however turn out that this choice bears no effect on definition 5.

3. Let $\mathcal{Q} = \infty$. Define $\lambda_{\mathcal{Q}}(x) = t^{-2}$. It follows that

$$\begin{aligned} C(\lambda_{\mathcal{Q}}(x)) &= t^{-10} + at^{-8} + bt^{-6} + ct^{-4} + dt^{-2} + e \\ &= t^{-10} \sqrt{\tau_3} \end{aligned}$$

so define $\lambda_{\mathcal{Q}}(y) = t^{-5} \sqrt{\tau_3}$.

Definition 5: For $\mathcal{Q} \in H(\overline{K})$ and $f \in \mathcal{F}^*$ define $\text{ord}_{\mathcal{Q}}(f) = \text{ord } \lambda_{\mathcal{Q}}(f)$.

Lemma 3: Let $f \in K[x, y] \subset \mathcal{F}$, $f \neq 0$ and $\mathcal{Q} \in H_0(\overline{K})$, $\mathcal{Q} = (x_0, y_0)$. Then

- (a) $\text{ord}_{\mathcal{Q}} f \geq 0$ and
- (b) if $f(\mathcal{Q}) = 0$ then $\text{ord}_{\mathcal{Q}} f \geq 1$.

Proof.

- (a) Because $\mathcal{Q} \in H_0(\overline{K})$ we have $\lambda_{\mathcal{Q}}(x), \lambda_{\mathcal{Q}}(y) \in \overline{K}[[t]]$ so with $f \in K[x, y]$ we have $\text{ord}_{\mathcal{Q}}(f) \in \mathbb{N} \cup \{0\}$.
- (b) Write $f = A(x, y)$, $A(X, Y) \in K[X, Y]$. First, let $y_0 \neq 0$.

$$\begin{aligned}\text{ord}_{\mathcal{Q}} f &= \text{ord} A(\lambda_{\mathcal{Q}}(x), \lambda_{\mathcal{Q}}(y)) \\ &= \text{ord} A(x_0 + t, y_0 \sqrt{\tau_1}).\end{aligned}$$

But $A(x_0 + t, y_0 \sqrt{\tau_1}) = \sum_{i=0}^{\infty} a_i t^i$ so with $t = 0$ we get $A(x_0, y_0) = a_0$ but the former is $f(\mathcal{Q})$ which is 0, so $a_0 = 0$ and the claim follows.

If $y_0 = 0$ we would have $\text{ord}_{\mathcal{Q}} f = \text{ord} A(x_0 + t^2, \nu t \sqrt{\tau_2})$ instead. But like before, this means $0 = f(\mathcal{Q}) = A(x_0, 0) = a_0$ so again $\text{ord}_{\mathcal{Q}}(f) \geq 1$.

□

Lemma 4: Let $f \in K(x) \subset \mathcal{F}$, $f \neq 0$, $\mathcal{Q} \in H(\overline{K})$. Then

- (a) $\text{ord}_{\mathcal{Q}}(f) = \text{ord}_{x=x_0} f(x)$ if $\mathcal{Q} = (x_0, y_0) \in H_0(\overline{K})$ with $y_0 \neq 0$.
- (b) $\text{ord}_{\mathcal{Q}}(f) = 2\text{ord}_{x=x_0} f(x)$ if $\mathcal{Q} = (x_0, 0) \in H_0(\overline{K})$.
- (c) $\text{ord}_{\infty}(f) = 2\text{ord}_{x=\infty} f(x) = 2\text{ord}_{x=0} f(\frac{1}{x})$.

Note that the right-hand sides of the equalities refer to the usual definition of the order of a rational function in a point $x_0 \in \overline{K} \cup \{\infty\}$.

Proof. Take $f \in K[x]$ and define $e = \text{ord}_{x=x_0} f \in \mathbb{N}$ so $f(x) = (x - x_0)^e g(x)$ with $g \in \overline{K}[x]$ and $g(x_0) \neq 0$.

- (a) If $\mathcal{Q} = (x_0, y_0)$, $y_0 \neq 0$ then $\lambda_{\mathcal{Q}}(f) = f(x_0 + t) = t^e g(x_0 + t)$ and so $\text{ord} \lambda_{\mathcal{Q}}(f) = e$ because $g(x_0 + t) = g(x_0) + \dots$ with $g(x_0) \neq 0$.
- (b) Here $\lambda_{\mathcal{Q}}(f) = f(x_0 + t^2) = t^{2e} g(x_0 + t^2)$ and again $g(x_0 + t^2) = g(x_0) + \dots$ so $\text{ord} \lambda_{\mathcal{Q}}(f) = 2e$.
- (c) For $\mathcal{Q} = \infty$ we have $\lambda_{\mathcal{Q}}(f) = f(t^{-2}) = \kappa t^{-2d} + \dots$ with $\kappa \neq 0$ if $d = \deg f$ so $\text{ord}_{x=0} f(\frac{1}{x}) = -d$ and so $\text{ord} \lambda_{\mathcal{Q}}(f) = 2\text{ord}_{x=0} f(\frac{1}{x})$.

Generally, if $f \in K(x)$ we can write $f = \frac{r}{q}$ for $r, q \in K[x]$ and apply $\text{ord}_{x=x_0} f = \text{ord}_{x=x_0} r - \text{ord}_{x=x_0} q$ in order to use the above on r and q . □

Lemma 5: For $f \in \mathcal{F}^*$ and $\mathcal{Q} \in H(\overline{K})$ the order satisfies $\text{ord}_{\mathcal{Q}}(\bar{f}) = \text{ord}_{\mathcal{Q}}(f)$

Proof. Split into three possible cases:

1. For $\mathcal{Q} \in H_0(\overline{K})$ with $y_0 \neq 0$ we've got $\lambda_{\mathcal{Q}}(x) = x_0 + t$ and $\lambda_{\mathcal{Q}}(y) = y_0 \sqrt{\tau_1}$.

Therefore $\lambda_{\overline{\mathcal{Q}}}(x) = x_0 + t = \lambda_{\mathcal{Q}}(\overline{x})$ and $\lambda_{\overline{\mathcal{Q}}}(y) = -y_0\sqrt{\tau_1} = \lambda_{\mathcal{Q}}(\overline{y})$ so

$$\begin{aligned}\lambda_{\overline{\mathcal{Q}}}(f(x, y)) &= f(\lambda_{\overline{\mathcal{Q}}}(x), \lambda_{\overline{\mathcal{Q}}}(y)) \\ &= \lambda_{\mathcal{Q}}(f(\overline{x}, \overline{y})) \\ &= \lambda_{\mathcal{Q}}(\overline{f}(x, y)).\end{aligned}$$

2. If $\mathcal{Q} \in H_0(\overline{K})$ with $y_0 = 0$ then $\overline{\mathcal{Q}} = \mathcal{Q}$. Write $f(x) = g(x) + h(x)y$, so

$$\lambda_{\mathcal{Q}}(\overline{f}) = g(x_0 + t^2) - h(x_0 + t^2)\nu t\sqrt{\tau_2}.$$

Calling this $l(t) = \lambda_{\mathcal{Q}}(\overline{f})$ and looking at the construction of $\lambda_{\mathcal{Q}}$ we see that τ_2 sports only even powers of t so we see above that $l(-t) = \lambda_{\mathcal{Q}}(f)$. As interchanging t with $-t$ doesn't change the order, we're done.

3. For $\mathcal{Q} = \infty$, $\tau_3 = 1 + at^2 + bt^4 + ct^6 + dt^8 + et^{10}$ features only even powers as well, so again $l(-t) = \lambda_{\mathcal{Q}}(f)$ for $l(t) = \lambda_{\mathcal{Q}}(\overline{f}) = g(t^{-2}) - h(t^{-2})t^{-5}\sqrt{\tau_3}$. Finally, $\lambda_{\mathcal{Q}}(f)$ is equal to $\lambda_{\overline{\mathcal{Q}}}(f)$ since $\infty = \overline{\infty}$. Again $\text{ord} l(t) = \text{ord} l(-t)$.

□

Remark 4: We now see why the choice of the square root in definition 4 has no effect on $\text{ord}_{\mathcal{Q}} f$. If $\lambda'_{\mathcal{Q}}$ were to correspond to the other choice, we would have $\lambda'_{\mathcal{Q}}(x) = \lambda_{\mathcal{Q}}(x)$ and $\lambda'_{\mathcal{Q}}(y) = -\lambda_{\mathcal{Q}}(y)$, so $\lambda'_{\mathcal{Q}}(f) = \lambda_{\mathcal{Q}}(\overline{f})$. As this was under item 2 where $y_0 = 0$, meaning $\overline{\mathcal{Q}} = \mathcal{Q}$, we have $\text{ord} \lambda_{\mathcal{Q}}(\overline{f}) = \text{ord} \lambda_{\mathcal{Q}}(f)$.

Lemma 6: If $f \in \mathcal{F}^*$ then the set $\{\mathcal{Q} \in H(\overline{K}) \mid \text{ord}_{\mathcal{Q}} f \neq 0\}$ is finite and

$$\sum_{\mathcal{Q} \in H(\overline{K})} \text{ord}_{\mathcal{Q}} f = 0.$$

Proof. First take $f \in K[x, y]$, $f \neq 0$ and let $\mathcal{Q} = (x_0, y_0) \in H_0(\overline{K})$, $y_0 \neq 0$, with $\text{ord}_{\mathcal{Q}} f \neq 0$. By Lemma 3 (a) we know that $\text{ord}_{\mathcal{Q}} f \geq 1$. It follows that $\text{ord}_{\mathcal{Q}}(f\overline{f}) = \text{ord}_{\mathcal{Q}} f + \text{ord}_{\mathcal{Q}} \overline{f} \geq 1$. Now since $f = g + hy$, $f\overline{f} = g^2 - h^2C(x)$ which lies in $K[x]$, so by Lemma 4 we have $\text{ord}_{x=x_0}(f\overline{f}) = \text{ord}_{\mathcal{Q}}(f\overline{f}) \geq 1$. But there are only finitely many such x_0 and so only finitely many such $y_0 = \pm\sqrt{C(x_0)}$.

If $f \in K(x, y)$, $f = \frac{r}{q}$, $r, q \in K[x, y]$ then $\text{ord}_{x=x_0} f = \text{ord}_{x=x_0} r - \text{ord}_{x=x_0} q$, and again only finitely many x_0 exist for which this differs from zero.

For the second claim, give our sum the name

$$s(f) = \sum_{\mathcal{Q} \in H(\overline{K})} \text{ord}_{\mathcal{Q}} f$$

and note that $s(f) = s(\bar{f})$ due to Lemma 5 and the fact that we take the sum over all \mathcal{Q} . Because $\text{ord}_{\mathcal{Q}}(f\bar{f}) = \text{ord}_{\mathcal{Q}}(f) + \text{ord}_{\mathcal{Q}}(\bar{f})$ we can see that

$$s(f\bar{f}) = s(f) + s(\bar{f}) = 2s(f).$$

But because $f\bar{f} \in K(x)$ we can use Lemma 4 to write this out as

$$\begin{aligned} 2s(f) &= \sum_{\mathcal{Q} \in H(\bar{K})} \text{ord}_{\mathcal{Q}} f\bar{f} \\ &= 2 \sum_{\substack{x_0 \neq \infty \\ C(x_0) \neq 0}} \text{ord}_{x=x_0} f\bar{f} + 2 \sum_{\substack{x_0 \neq \infty \\ C(x_0)=0}} \text{ord}_{x=x_0} f\bar{f} + 2 \sum_{x_0=\infty} \text{ord}_{x=x_0} f\bar{f} \\ &= 2 \sum_{x_0 \in \bar{K} \cup \{\infty\}} \text{ord}_{x=x_0} f\bar{f}. \end{aligned}$$

Here α_i are the points on which $C(x)$ vanishes and since

$$\sum_{x_0 \in \bar{K} \cup \{\infty\}} \text{ord}_{x=x_0} g = 0$$

for any $g \in K(x)$ we have $s(f) = 0$ in \mathbb{Z} . □

2.2 Divisors and Lemmas

Definition 6: The divisor of a function $f \in \mathcal{F}^*$ is the formal sum

$$(f) = \sum_{\mathcal{Q} \in H(\bar{K})} \text{ord}_{\mathcal{Q}} f \cdot \mathcal{Q}$$

Thanks to Lemma 6 the sum is finite and the sum of all coefficients is 0.

Points $\mathcal{Q} \in H(\bar{K})$ with a positive coefficient in (f) are called zeroes of f while those with a negative coefficient are called poles.

Lemma 7: If $f \in \mathcal{F}^*$ has no poles on $H(\bar{K})$, i.e. if $\text{ord}_{\mathcal{Q}} f \geq 0$ for all \mathcal{Q} , then f is constant.

Proof. With $f = g + hy$, $\text{ord}_{\mathcal{Q}} f \geq 0$ for every $\mathcal{Q} \in H(\bar{K})$ we take a look at $f + \bar{f} = 2g \in K(x)$ and $f\bar{f} = g^2 - h^2C \in K(x)$ and observe that by well-known properties of orders

$$\begin{aligned} \text{ord}_{\mathcal{Q}}(f + \bar{f}) &\geq \min\{\text{ord}_{\mathcal{Q}} f, \text{ord}_{\mathcal{Q}} \bar{f}\} \\ &= \min\{\text{ord}_{\mathcal{Q}} f, \text{ord}_{\bar{\mathcal{Q}}} f\} \geq 0. \end{aligned}$$

with Lemma 5 and similarly

$$\text{ord}_Q(f\bar{f}) = \text{ord}_Q f + \text{ord}_{\bar{Q}} f \geq 0.$$

With the help of Lemma 4 we conclude that $\text{ord}_{x=x_0}(f + \bar{f}) \geq 0$ and $\text{ord}_{x=x_0}(f\bar{f}) \geq 0$ respectively.

But in $\bar{K}(x)$, a function q with $\text{ord}_{x=x_0} q \geq 0$ for every $x_0 \in \bar{K} \cup \{\infty\}$ must be constant, so both $f + \bar{f}$ and $f\bar{f}$ are constant functions. Since f is a root of $(T - f)(T - \bar{f}) = T^2 - (f + \bar{f})T + f\bar{f} \in \bar{K}[T]$, f lies in \bar{K} . \square

Theorem 1: Let K be a field and $x, y \in K(t)$ rational functions such that $y^2 = C(x)$. Then x and y are actually constants, i.e. $x, y \in K$.

Lemma 8: Suppose $f \in \mathcal{F}^*$ has a pole of order at most one at ∞ i.e. $\text{ord}_\infty f \geq -1$ and no pole at any other $Q \in H_0(\bar{K})$. Then f is a constant.

Proof. By Lemma 7 we can assume $\text{ord}_\infty f = -1$ and $\text{ord}_Q f \geq 0$ for every $Q \in H_0(\bar{K})$. Now $f = g + hy$ and $\lambda_\infty(f) = \kappa t^{-1} + \dots$ with $\kappa \neq 0$ in \bar{K} . Since we are only interested in the order, replace f with $\kappa^{-1}f$ so $\lambda_\infty(f) = t^{-1} + \dots$.

Now remember that $\lambda_\infty(x) = t^{-2}$ so $\lambda_\infty(x - f^2) = \alpha t^{-1} + \dots$, $\alpha \in \bar{K}$ and finally we have a regular power series $\lambda_\infty(x - f^2 - \alpha f)$ so

$$\text{ord}_\infty(x - f^2 - \alpha f) \geq 0.$$

Also for any other $Q \in H_0(\bar{K})$ we have

$$\text{ord}_Q(x - f^2 - \alpha f) \geq \min\{\text{ord}_Q(x), \text{ord}_Q(f^2), \text{ord}_Q f\}$$

which is non-negative by virtue of the prerequisite on f and $\lambda_Q(x) = x_0 + \dots$. The previous Lemma now implies $x - f^2 - \alpha f \in \bar{K}$ so we see $x = f^2 + \alpha f + \beta$ as a polynomial $x = X(f)$ with $X(T) \in \bar{K}[T] \setminus \bar{K}$.

Do the same thing with $\lambda_\infty(y) = t^{-5}\sqrt{\tau_3} = t^{-5} + \dots$

so $\lambda_\infty(y - f^5) = \beta_4 t^{-4} + \dots$

and $\lambda_\infty(y - f^5 - \beta_4 f^4) = \beta_3 t^{-3} + \dots$

and so on, so $\lambda_\infty(y - f^5 - \beta_4 f^4 - \beta_3 f^3 - \beta_2 f^2 - \beta_1 f)$ is a power series as well. Again $y = f^5 + \beta_4 f^4 + \beta_3 f^3 + \beta_2 f^2 + \beta_1 f + \beta_0 = Y(f)$ with $Y(T) \in \bar{K}[T] \setminus \bar{K}$.

Combined we have the polynomial equation $Y(f)^2 - C(X(f)) = 0$ over \bar{K} whose algebraic closure dictates either $f \in \bar{K}$ or $Y(T)^2 = C(X(T))$. The latter can't be true by Theorem 1 and the former is in contradiction to $\text{ord}_\infty f = -1$. \square

Lemma 9: If $f \in \mathcal{F}^*$ has a pole of order at most two at ∞ and $\text{ord}_{\mathcal{Q}} f \geq 0$ for every $\mathcal{Q} \in H_0(\overline{K})$ then f is of the form $f = \alpha + \beta x$ with $\alpha, \beta \in K$.

Proof. Because $\lambda_{\infty}(f) = \beta t^{-2} + \dots$ where $\beta \in \overline{K}$ we have $\lambda_{\infty}(f - \beta x) = \gamma t^{-1} + \dots$ and thanks to Lemma 8 we know this to imply $f - \beta x = \alpha$. \square

Note that it is easy to see that in this case $(f) = \mathcal{A} + \overline{\mathcal{A}} - 2\infty$ for $\mathcal{A} = (-\frac{\alpha}{\beta}, *)$

Lemma 10: If $f \in \mathcal{F}^*$ has a pole of order at most three at ∞ and $\text{ord}_{\mathcal{Q}} f \geq 0$ for every $\mathcal{Q} \in H_0(\overline{K})$ then f is of the form $f = \alpha + \beta x$ with $\alpha, \beta \in K$.

Proof. From $\lambda_{\infty}(f) = \gamma t^{-3} + \dots$ and $f + \overline{f} \in K(x)$ we get that the order of the latter must be even by Lemma 4 (c), so $\text{ord}_{\infty}(f + \overline{f}) \geq -2$. Like f , $f + \overline{f}$, has no poles on $H_0(\overline{K})$ so Lemma 9 implies $f + \overline{f} = \alpha + \beta x$. Writing $f = g + hy$ we therefore see that $g = \frac{\alpha + \beta x}{2}$ and $f - g = hy$. The latter also has a pole of order three at ∞ and none on $H_0(\overline{K})$ so we are effectively reduced to studying functions f of the form $f = hy$ for $h \in K(x)$, $h \neq 0$.

With $f = hy$ we have $-3 = \text{ord}_{\infty} f = \text{ord}_{\infty} h + \text{ord}_{\infty} y = \text{ord}_{\infty} h - 5$ so $\text{ord}_{\infty} h = 2$. Writing $h = \frac{r}{q}$ for $r, q \in K[x]$ coprime, this means that q cannot be constant. Use this to pick a $\xi \in \overline{K}$ with $q(\xi) = 0$, implying $r(\xi) \neq 0$ by coprimality.

Pick a point $\mathcal{R} = (\xi, \eta)$ in $H_0(\overline{K})$. If $\xi \neq \alpha_i$ then $\text{ord}_{\mathcal{R}} y = 0$ and $\text{ord}_{\mathcal{R}} q \geq 1$ from which we follow $\text{ord}_{\mathcal{R}} f = \text{ord}_{\mathcal{R}} \frac{y}{q} \leq -1$, a contradiction. In case ξ is a Weierstrass Point, $\xi = \alpha_i$ then $\text{ord}_{\mathcal{R}} y = 1$ and $\text{ord}_{\mathcal{R}} q \geq 2$ and so we get the same contradiction. This finishes the proof. \square

Lemma 11: If $f \in \mathcal{F}^*$ has a pole of order at most four at ∞ then f is of the form $f = \alpha + \beta x + \gamma x^2$ with $\alpha, \beta, \gamma \in K$.

Proof. With $\lambda_{\infty}(f) = \gamma t^{-4} + \dots$ we know that $\lambda_{\infty}(f - \gamma x^2) = \delta t^{-3} + \dots$ and we use the previous Lemma to see that $f - \gamma x^2 = \alpha + \beta x$. \square

3 Associativity

Lemma 12: Suppose we have $\mathcal{Q}_i = (x_i, y_i)$, $\mathcal{Q}_i \in H(\overline{K})$, that fulfill

$$\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\} = \{\overline{\mathcal{Q}}_5, \overline{\mathcal{Q}}_6\}$$

with $\mathcal{Q}_j = \infty$ for at most one $j \in \{1, \dots, 6\}$. This means that we are in one of the cases 1–5 of the addition law which involved passing a polynomial p through all $\mathcal{Q}_i \neq \infty$. Now remember that we defined $D(x) = C(x) - (p(x))^2$.

If exactly e_i of the \mathcal{Q}_i are equal, say to some \mathcal{Q}_k for a $k \in \{1, \dots, 6\}$, then

$$D(x) = (x - x_k)^e g(x)$$

with $g(x_k) \neq 0$ and $e = e_i = e_k$. This is of course equivalent to stating $\text{ord}_{x=x_k} D(x) = e_k$ and is nothing other than the order of the intersection of $p(x)$ and the curve at \mathcal{Q}_k . The choice of k obviously does not matter.

Proof. In all non-zero cases we know the expression for the various $D(x)$ as derived at the various $(*_i)$ and $(*_i')$ for cases 1–5, which all come down to

$$D(x) = -p_3^2 \prod_{i=1}^6 (x - x_i)$$

if $p_3 \neq 0$. If $p_3 = 0$ and therefore $\mathcal{Q}_j = \infty$ for exactly one $j \in \{1, \dots, 6\}$ then

$$D(x) = \prod_{\substack{i=1 \\ i \neq j}}^6 (x - x_i).$$

So by construction, \mathcal{Q}_i being equal to some \mathcal{Q}_k contributes a factor $x - x_k$. \square

Theorem 2: Let $\mathbf{P}_1 = \{\mathcal{Q}_1, \mathcal{Q}_2\}$, $\mathbf{P}_2 = \{\mathcal{Q}_3, \mathcal{Q}_4\}$, $\mathbf{P}_3 = \{\overline{\mathcal{Q}}_5, \overline{\mathcal{Q}}_6\}$ be in \mathbf{J} with

$$\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_3.$$

Then there exists an $f \in \mathcal{F}^*$ with divisor

$$(f) = \mathcal{Q}_1 + \mathcal{Q}_2 + \mathcal{Q}_3 + \mathcal{Q}_4 - \overline{\mathcal{Q}}_5 - \overline{\mathcal{Q}}_6 - 2\infty.$$

Remark 5: Looking back at the complete list of cases, we simplified things twofold. First, at (\diamond) we imposed that permutation between $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ and \mathcal{Q}_4 was permitted. Second, we isolated the zero case in order to state that in any other case the situation $\mathcal{Q}_i = \overline{\mathcal{Q}}_j$ for $i \neq j$, $i, j = 1, \dots, 4$ never occurs.

Now, by construction of the sum in all non-zero cases it is easy to check that the same properties hold for the whole set $\{\mathcal{Q}_i \mid i = 1, \dots, 6\}$ for a given sum.

The polynomial $p(x)$ passes through all those \mathcal{Q}_i that are in $H_0(\overline{K})$. This implies that if $\mathcal{Q}_i = \overline{\mathcal{Q}}_j$ we must have $-y_i = y_j = p(x_j) = p(x_i) = y_i$ so $y_i = 0$ in $\text{char}(K) \neq 2$ i.e. $\overline{\mathcal{Q}}_i = \mathcal{Q}_j = \mathcal{Q}_i$. This is helpful for the next proof.

Proof. First part

Begin with the observation that in case 0 we are looking for a function f with divisor $(f) = \mathcal{Q}_1 + \overline{\mathcal{Q}}_1 - 2\infty$. If $\mathcal{Q}_1 \neq \infty$, we may take $f = x - x_1$, otherwise $f = 1$ fills the criterion, so we are completely done with case 0.

Exclude the zero case from now on, so for the remaining cases we have the polynomial $p(x)$ at our disposal. As $y_i = p(x_i)$ whenever $\mathcal{Q}_i \neq \infty$, we define

$$q = y - p(x) \in K[x, y] \subset \mathcal{F}^*$$

with the intention of showing that $(q) = \mathcal{Q}_1 + \mathcal{Q}_2 + \mathcal{Q}_3 + \mathcal{Q}_4 + \mathcal{Q}_5 + \mathcal{Q}_6 - 6\infty$.

By Lemma 3 (b) we know that $\text{ord}_{\mathcal{Q}_i} q \geq 1$ for those \mathcal{Q}_i that are not ∞ .

Let's first assume that all $\mathcal{Q}_i \in H_0(\overline{K})$. This means that we are in the case where $p(x)$ is of degree 3, so as $\lambda_\infty(x) = t^{-2}$ we see that $\text{ord}_\infty q = -6$.

Use Lemma 12 in conjunction with Lemma 4 to see that for each of the \mathcal{Q}_i

$$\begin{aligned} \text{ord}_{\mathcal{Q}_i} q + \text{ord}_{\mathcal{Q}_i} \overline{q} &= \text{ord}_{\mathcal{Q}_i} q\overline{q} \\ &= \text{ord}_{x=x_i} D(x) \\ &= e_i. \end{aligned}$$

As in Lemma 12, e_i denotes the exact number of occurrences of \mathcal{Q}_i . Also note $\text{ord}_{\mathcal{Q}_i} \overline{q} = 0$, otherwise $q - \overline{q} = 2y$ would imply $y_i = 0$ which we excluded.

Since $q \in K[x, y]$ implies the only negative order may be at ∞ and $\sum e_i = 6$, $\text{ord}_\infty q = -6$, we have $\text{ord}_{\mathcal{Q}} q = 0$ for all $\mathcal{Q} \in H_0(\overline{K})$ that are not some \mathcal{Q}_i .

In the case where $y_i = 0$, the same lemmas imply

$$\text{ord}_{\mathcal{Q}_i} q + \text{ord}_{\mathcal{Q}_i} \overline{q} = 2e_i$$

and since $\overline{\mathcal{Q}}_i = \mathcal{Q}_i$, Lemma 5 gives $\text{ord}_{\mathcal{Q}_i} \overline{q} = \text{ord}_{\mathcal{Q}_i} q$ so again $\text{ord}_{\mathcal{Q}_i} q = e_i$.

So in both cases, if \mathcal{Q}_i appears e_i times in the sum $\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_3$ then it appears the same number of times in (q) and all in all

$$(q) = \sum_{\{\mathcal{Q}_i\}} e_i \mathcal{Q}_i - 6\infty = \sum_{i=1}^6 \mathcal{Q}_i - 6\infty.$$

Now consider the case where $\mathcal{Q}_k = \infty$ for some k . Because $p(x)$ is now of degree two or less and $\lambda_\infty(y) = t^{-5}\sqrt{\tau}$ we have $\text{ord}_\infty q = -5$. This leads to

$$(q) = \sum_{\substack{i=1 \\ i \neq k}}^6 \mathcal{Q}_i - 5\infty = \sum_{i=1}^6 \mathcal{Q}_i - 6\infty$$

completing the first part of our proof, as no more than one \mathcal{Q}_k may be ∞ .

Second Part

The divisor of $x - x_i$ is $(x - x_i) = \mathcal{Q}_i + \overline{\mathcal{Q}}_i - 2\infty$ both for $\mathcal{Q}_i = \overline{\mathcal{Q}}_i$ and $\mathcal{Q}_i \neq \overline{\mathcal{Q}}_i$.

Without loss of generality let $\mathcal{Q}_5 \neq \infty$ and distinguish between $\mathcal{Q}_6 \neq \infty$ and $\mathcal{Q}_6 = \infty$. In the first case it is easy to check that for $f = q(x - x_5)^{-1}(x - x_6)^{-1}$

$$\begin{aligned} (f) &= \sum_{i=1}^6 \mathcal{Q}_i - 6\infty - \mathcal{Q}_5 - \overline{\mathcal{Q}}_5 - \mathcal{Q}_6 - \overline{\mathcal{Q}}_6 + 4\infty \\ &= \sum_{i=1}^4 \mathcal{Q}_i - \overline{\mathcal{Q}}_5 - \overline{\mathcal{Q}}_6 - 2\infty \end{aligned}$$

which corresponds precisely to the statement we aim to prove. If $\mathcal{Q}_6 = \infty$, we can define $f = q(x - x_5)^{-1}$ and check that

$$\begin{aligned} (f) &= \sum_{i=1}^5 \mathcal{Q}_i - 5\infty - \mathcal{Q}_5 - \overline{\mathcal{Q}}_5 + 2\infty \\ &= \sum_{i=1}^4 \mathcal{Q}_i - \overline{\mathcal{Q}}_5 - \infty - 2\infty. \end{aligned}$$

So the function f that we were looking for is

$$f = \frac{y - p(x)}{(x - x_5)(x - x_6)}$$

if \mathcal{Q}_5 and \mathcal{Q}_6 are both different from ∞ and otherwise if $\mathcal{Q}_6 = \infty$ then

$$f = \frac{y - p(x)}{x - x_5}.$$

□

Theorem 3: *Associativity.* The sums

$$\begin{aligned} &\underbrace{(\mathbf{P} + \mathbf{Q})}_{=\mathbf{T}} + \mathbf{R} = \mathbf{S} \\ \text{and } &\mathbf{P} + \underbrace{(\mathbf{Q} + \mathbf{R})}_{=\mathbf{W}} = \mathbf{S}' \end{aligned}$$

give the same result, namely $\mathbf{S} = \mathbf{S}'$.

Proof. We will use the following notation:

$$\begin{aligned} \mathbf{P} &= \{\mathcal{P}_1, \mathcal{P}_2\}, \mathbf{Q} = \{\mathcal{Q}_1, \mathcal{Q}_2\}, \mathbf{R} = \{\mathcal{R}_1, \mathcal{R}_2\}, \mathbf{T} = \{\mathcal{T}_1, \mathcal{T}_2\}, \mathbf{W} = \{\mathcal{W}_1, \mathcal{W}_2\}, \\ \mathbf{S} &= \{\mathcal{A}, \mathcal{B}\}, \mathbf{S}' = \{\mathcal{U}, \mathcal{V}\}, \\ \mathcal{A} &= (a, *), \mathcal{B} = (b, *). \end{aligned}$$

Thanks to the previous theorem we have functions $f_{\mathbf{PQ}}$, $f_{\mathbf{TR}}$, $f_{\mathbf{PW}}$ and $f_{\mathbf{QR}}$ in \mathcal{F}^* such that the divisor of

$$f = \frac{f_{\mathbf{PQ}}f_{\mathbf{TR}}}{f_{\mathbf{PW}}f_{\mathbf{QR}}}$$

is

$$\begin{aligned} (f) &= \mathcal{P}_1 + \mathcal{P}_2 + \mathcal{Q}_1 + \mathcal{Q}_2 - \mathcal{T}_1 - \mathcal{T}_2 - 2\infty \\ &\quad + \mathcal{T}_1 + \mathcal{T}_2 + \mathcal{R}_1 + \mathcal{R}_2 - \mathcal{A} - \mathcal{B} - 2\infty \\ &\quad - \mathcal{P}_1 - \mathcal{P}_2 - \mathcal{W}_1 - \mathcal{W}_2 + \mathcal{U} + \mathcal{V} + 2\infty \\ &\quad - \mathcal{Q}_1 - \mathcal{Q}_2 - \mathcal{R}_1 - \mathcal{R}_2 + \mathcal{W}_1 + \mathcal{W}_2 + 2\infty \\ &= \mathcal{U} + \mathcal{V} - \mathcal{A} - \mathcal{B}. \end{aligned}$$

This leaves us with three cases: both \mathcal{A} and \mathcal{B} being ∞ , only \mathcal{B} being ∞ and neither being ∞ . In the first case Lemma 9 tells us $\mathcal{U} = \overline{\mathcal{V}}$ so $\mathbf{S}' = 0 = \mathbf{S}$.

In the second case, $a \neq \infty$ so we can look at $\tilde{f} = (x - a)f$ which now has divisor $(\tilde{f}) = \mathcal{U} + \mathcal{V} + \overline{\mathcal{B}} - 3\infty$ but only two real poles at ∞ according to Lemma 10. This means that either $\mathcal{U} = \infty$ or $\mathcal{V} = \infty$. Either way, the other one has to be equal to \mathcal{B} , again as can be seen in Lemma 9, and so $\mathbf{S} = \mathbf{S}'$

This leaves $\tilde{f} = (x - a)(x - b)f$ which has divisor $(\tilde{f}) = \overline{\mathcal{A}} + \overline{\mathcal{B}} + \mathcal{U} + \mathcal{V} - 4\infty$. By Lemma 11, \tilde{f} must be of the form $\kappa(x - \varrho)(x - \varsigma) \in \overline{K}[x]$, $\kappa \neq 0$ and so

$$f = \frac{\kappa(x - \varrho)(x - \varsigma)}{(x - a)(x - b)}.$$

But this has divisor of the form

$$(f) = \mathcal{M} + \overline{\mathcal{M}} + \mathcal{N} + \overline{\mathcal{N}} - \mathcal{A} - \overline{\mathcal{A}} - \mathcal{B} - \overline{\mathcal{B}}.$$

So, without loss of generality, either $\mathcal{A} = \mathcal{M}$ and $\mathcal{B} = \overline{\mathcal{M}}$ or $\mathcal{A} = \mathcal{M}$ and $\mathcal{B} = \mathcal{N}$. First case implies \mathbf{S} and \mathbf{S}' equals 0, second case implies that $(f) = \mathcal{A} + \mathcal{B} - \mathcal{A} - \mathcal{B}$ and in both cases we're done. \square

Remark 6: We can finally prove property (\diamond) we imposed on page 5 with the exact same technique of the theorem above. Let's have the two sums

$$\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\} = \{\mathcal{Q}_5, \mathcal{Q}_6\}$$

and

$$\{\mathcal{Q}_3, \mathcal{Q}_2\} + \{\mathcal{Q}_1, \mathcal{Q}_4\} = \{\mathcal{Q}'_5, \mathcal{Q}'_6\}.$$

Use Theorem 2 again to get two functions f_1 and f_2 corresponding to the two sums. Let's just look at the third case of the proof above. Defining the function $f = \frac{f_1}{f_2}$ we conclude that (f) must equal to both $\mathcal{Q}'_5 + \mathcal{Q}'_6 - \mathcal{Q}_5 - \mathcal{Q}_6$ and $\mathcal{M} + \overline{\mathcal{M}} + \mathcal{N} + \overline{\mathcal{N}} - \mathcal{Q}_5 - \overline{\mathcal{Q}}_5 - \mathcal{Q}_6 - \overline{\mathcal{Q}}_6$ for some $\mathcal{M}, \mathcal{N} \in H(\overline{K})$. As above, this means either $\mathcal{Q}'_5 = \mathcal{Q}_5$ and $\mathcal{Q}'_6 = \mathcal{Q}_6$ or the other way around.