1 Addition Law

1.1 Definitions and Notation

Definition 1: Let K be a field with $\text{char}(K) \neq 2, 3$ 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 $H_0(K) \cup \{\infty\}$.

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 allow ourselves to write $\pm\mathcal{Q}$ whenever we mean in fact 'either $\mathcal{Q}$ or $\overline{\mathcal{Q}}$'.

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 $\mathcal{J} = H(\overline{K}) \times H(\overline{K})$. $\mathbf{J}$ is called the 'Jacobian' and the equivalence relation fullfills

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

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. We will also permit ourselves the notation $\{\mathcal{Q}, \overline{\mathcal{Q}}\} = 0$ and we refrain from explicitly stating that $\mathbf{P}$ is in fact an equivalence class.

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.

1.2 The General Case

Let $\mathbf{P}_1 = \{\mathcal{Q}_1, \mathcal{Q}_2\}$, $\mathbf{P}_2 = \{\mathcal{Q}_3, \mathcal{Q}_4\}$ 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 Component-Points: Let first $\mathcal{Q}_i \in H_0(K)$ 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.

Step 2a: Knowing the coefficients p_i of $p(x)$ we first assume that $p_3 \neq 0$, so can proceed to look for the two additional solutions of the sextic equation

$$C(x) - (p(x))^2 = 0. \qquad (*)$$

Observe that this vanishes at x_1, x_2, x_3 and x_4, so write the lefthand side as $-p_3^2(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5)(x - x_6)$ for x_5 and x_6 in $\overline{K}$.

Comparing the coefficients of both expressions at x^4 and x^5 yields

$$\sum_{\substack{i,j=1\\i<j}}^{6} x_i x_j = T_4 \tag{4}$$

$$\text{and} \qquad \sum_{i=1}^{6} x_i = T_5 \tag{5}$$

where $T_5 = \frac{1-2p_2p_3}{p_3^2}$ and $T_4 = \frac{p_2^2+2p_1p_3-a}{p_3^2}$. The first expression gives

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

Doing this twice and replacing x_6 with the information from (5) gives the tidy quadratic equation

---

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

---

of which x_5 is one solution and — by symmetry of the above steps — x_6 the other one. Compute $y_i = p(x_i)$, $i = 5, 6$ 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 $\mathbf{P}_3 = \{\mathcal{Q}_5, \mathcal{Q}_6\}$.

Step 2b: If p_3 were zero, the equation $(*)$ would be quintic instead. We may therefore write the lefthand side as $(x-x_1)(x-x_2)(x-x_3)(x-x_4)(x-x_5)$, again for x_5 somewhere in $\overline{K}$. Defining $T_{4\infty} = p_2^2 - a$ and comparing the coefficients at x^4 gives

---

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

---

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 $\mathfrak{Q}_4 = \infty$ with the other $\mathfrak{Q}_i = (x_i, y_i)$ as before. We will later reason about why this is sufficient to cover the general case.

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 $\widetilde{V} \cdot \mathbf{p} = \widetilde{\mathbf{y}}$ where $\widetilde{V}$ is the Vandermonde matrix for x_i, $i = 1, .., 3$ which incidentally is the upper-left $3{\times}3$ sub-matrix of V. Here $\mathbf{p} = (p_0\ p_1\ p_2)^t$ and $\widetilde{\mathbf{y}} = (y_1\ y_2\ y_3)^t$ are defined as expected.

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 two.

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

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

$$\text{and} \qquad \sum_{i=1}^{3} x_i + x_5 + x_6 = p_2^2 - a. \tag{4′}$$

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

---

$$x^2 - T_{4\infty} \cdot x + \left(T_{3\infty} - \sum_{\substack{i,j=1\\ i<j}}^{3} x_i x_j \right) = 0. \tag{†′}$$

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 $\mathbf{P}_3 = \{(x_5, -y_5), (x_6, -y_6)\} = \{\mathfrak{Q}_5, \mathfrak{Q}_6\}$.

Remark 1: Note that an interesting consequence is — if the above does truly complete the general case — that at most one of the $\mathfrak{Q}_i$ for $i = 1, .., 6$ can be the point at infinity, provided that the $\mathfrak{Q}_i$ for $i = 1, .., 4$ are all pairwise distinct.

∼

Before we begin listing the special cases, we impose the following property on the addition of any two points:

The sum of any $\{\mathfrak{Q}_1, \mathfrak{Q}_2\}$ and $\{\mathfrak{Q}_3, \mathfrak{Q}_4\}$ in $\mathbf{J}$ fulfills the following equality:

$$\{\mathfrak{Q}_1, \mathfrak{Q}_2\} + \{\mathfrak{Q}_3, \mathfrak{Q}_4\} = \{\mathfrak{Q}_1, \mathfrak{Q}_3\} + \{\mathfrak{Q}_2, \mathfrak{Q}_4\}. \tag{$\Diamond$}$$

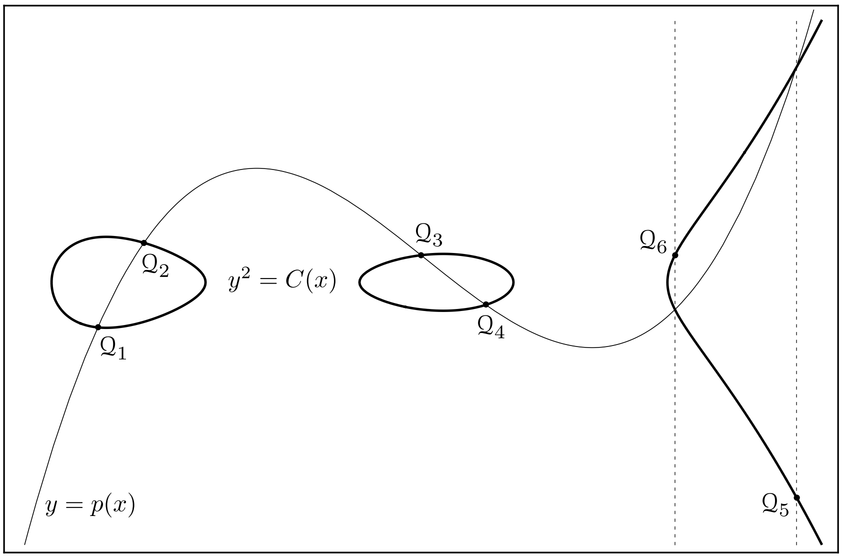
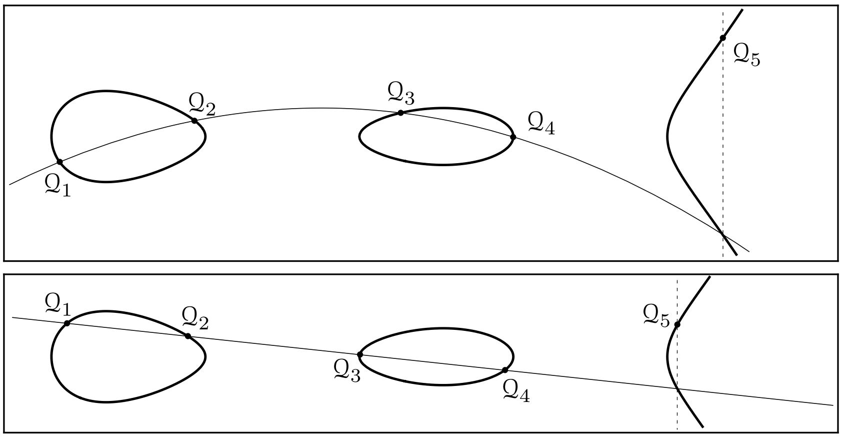


FIGURE 1A: The general case for the addition law in $\mathbb{R}^2$ where $p_3 \neq 0$.



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

Remark 2: We will use this property extensively from now on and it will be worth the additional trouble of having to check well-definedness because

(i) Since ($\diamondsuit$) implies that we can interchange *any* two point-components in a given sum, we may now impose conditions on the $\mathcal{Q}_i$ without mentioning whether they belong to $\mathbf{P}_1$ or $\mathbf{P}_2$.

(ii) As a result, the list of special cases can be written in a significantly more concise manner.

(iii) It is immediately clear now that if we have a well-defined addition, then $-\mathbf{P} = \overline{\mathbf{P}}$ because $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\overline{\mathcal{Q}}_1, \overline{\mathcal{Q}}_2\} = \{\mathcal{Q}_1, \overline{\mathcal{Q}}_1\} + \{\mathcal{Q}_2, \overline{\mathcal{Q}}_2\} = 0$.

(iv) The property even gives us commutativity for free.

1.3 List of Special Cases

Let's first list all configurations that can be taken by the $(x_i,\, y_i) \in H_0(K)$:

A. All x_i are pairwise distinct.

B. Exactly two of the x_i are equal, for instance $x_1 = x_2$ and
   - a. $y_1 = y_2 \neq 0$.
   - b. $y_1 = -y_2 \neq 0$. $\star$
   - c. $y_1 = y_2 = 0$. $\star$

C. Exactly three of the x_i are equal, e.g. $x_1 = x_2 = x_3$ and
   - a. All three y-coordinates are equal: $y_1 = y_2 = y_3 \neq 0$.
   - b. Only two y-coordinates are equal: $y_1 = y_2 \neq 0$ so $y_3 = -y_1$. $\star$
   - c. All three $y_1 = y_2 = y_3 = 0$. $\star$

D. All four x_i are equal and
   - a. All four y_i are equal but different from zero.
   - b. The y_i are equal two by two, e.g. $y_1 = y_2 \neq 0$ and $y_3 = y_4 = -y_1$. $\star$
   - c. Exactly three of the y_i are equal, e.g. $y_1 = y_2 = y_3 = -y_4 \neq 0$. $\star$
   - d. All four $y_i = 0$. $\star$

E. The x_i are equal two-by-two: $x_1 = x_2$ and $x_3 = x_4$ but $x_1 \neq x_3$ and
   - a. $y_1 = y_2 \neq 0$ and $y_3 = y_4 \neq 0$.
   - b. $y_1 = -y_2$ and $y_3 = y_4 \neq 0$. $\star$
   - c. $y_1 = -y_2$ and $y_3 = -y_4$. $\star$

Due to ($\diamondsuit$) and the property that $\{\mathcal{Q}_i, \mathcal{Q}_j\} \sim 0$ whenever $x_i = x_j$ and $y_i = -y_j$, every case marked with $\star$ comes down to the addition with 0. Considering the possibility of $\mathcal{Q}_i = \infty$ and reordering the above thus leads to the following condensed and complete list of cases for the addition law:

---

0. The addition with zero, i.e. $\mathbf{P} + \{\infty, \infty\}$ or in short $\mathbf{P} + 0$, $\mathbf{P} \in \mathbf{J}$.
1. The general case where all $\mathcal{Q}_i$ in $H(K)$ are pairwise distinct from $\pm\mathcal{Q}_j$.
2. The single tangential case where $\mathcal{Q}_1 = \mathcal{Q}_2 \in H_0(K)$ with $y_1 \neq 0$ and the remaining $\mathcal{Q}_3$, $\mathcal{Q}_4 \in H(K)$ are both distinct from each other as well as from $\pm\mathcal{Q}_1, \overline{\mathcal{Q}}_3$ and $\overline{\mathcal{Q}}_4$.
3. The double tangential case where $\mathcal{Q}_1 = \mathcal{Q}_2 \in H_0(K)$ with $y_1 \neq 0$ and $\mathcal{Q}_3 = \mathcal{Q}_4 \in H_0(K)$ with $y_3 \neq 0$ and $\mathcal{Q}_1 \neq \pm\mathcal{Q}_3$.
4. The triple-point tangential case wherein $\mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3 \in H_0(K)$ with $y_1 \neq 0$ and $\mathcal{Q}_4 \in H(K)$ differs from both $\pm\mathcal{Q}_1$.
5. The quadruple case where all $\mathcal{Q}_i \in H_0(K)$ are equal with $y_i \neq 0$.

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 zero case by virtue of $(\diamondsuit)$, bringing the two infinities together in one point. As for the first case, we consider $\mathcal{Q}_i \in H_0(K)$ and $\mathcal{Q}_i \in H(K)$ in two seperate 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 the permutations $\mathcal{Q}_1 \rightleftharpoons \mathcal{Q}_2$ and $\mathcal{Q}_3 \rightleftharpoons \mathcal{Q}_4$.

1.4 Addition Law for the Special Cases

Case 0, Addition with Zero: As one might have anticipated, if $\mathbf{P}_2 = 0$ we define $\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_1$ for every $\mathbf{P}_1 \in \mathbf{J}$.

Case 2, Tangential: Let $\mathcal{Q}_i \in H_0(K), \mathcal{Q}_1 = \mathcal{Q}_2$, $y_1 \neq 0$ 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 polynomial $p(x)$ be tangential to the curve at $\mathcal{Q}_1$. This gives

$$\begin{aligned} 2y\frac{dy}{dx} &= 5x^4 + 4ax^3 + 3bx^2 + 2cx + d \\ \text{and} \qquad \frac{dy}{dx} &= 3p_3x^2 + 2p_2x + p_1 \end{aligned}$$

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 $\operatorname{char}(K) \neq 2$ 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.

Once $p(x)$ is determined, step two will be entirely identical to the general case and we can again solve $(\ddagger)$ or $(\dagger)$ for x_5 or x_5 and x_6.

Case 3, Double Tangential: Let $\mathcal{Q}_i \in H_0(K)$, $\mathcal{Q}_1 = \mathcal{Q}_2$ and $\mathcal{Q}_3 = \mathcal{Q}_4$ but $x_1 \neq x_3$ and $\mathcal{Q}_i \neq \pm\mathcal{Q}_i$ 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 (†) or (‡).

Case 4, Second Order Tangential: Let $\mathcal{Q}_i \in H_0(K), \mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3$ 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. Again, apply the same procedure of the second steps of case 1 to find $\mathbf{P}_3$.

Case 5, Third Order Tangential: Given the quadruple situation where $\mathcal{Q}_i = \mathcal{Q}_1 \in H_0(K)$ 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.

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 $V_{111} \cdot \mathbf{p} = \mathbf{y}_{111}$ and subsequently (†) or (‡) and we're done.

∼

Finally, as noted in Remark 3, (ii) we have yet to extend our definition from $H_0(K)$ to $H(K)$. 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 $\widetilde{V}_1$ and $\widetilde{V}_{11}$ will be the upper-left 3×3 sub-matrices of their $H_0(K)$-counterparts V_1 and V_{11}.

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

Both matrices $\widetilde{V}_*$ are invertible and we therefore get a unique polynomial $p(x)$ wich 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 $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \infty\} = \{\mathcal{Q}_5, \mathcal{Q}_6\} = \{(x_5, -y_5), (x_6, -y_6)\}$.

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 $(\diamondsuit)$. Both cases can be combined into a single one by the following statement:

Lemma: In each given definition of '+', the result is invariant under the permutation $\mathcal{Q}_i \rightleftharpoons \mathcal{Q}_j$.

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. $\square$