1 Addition Law

1.1 Definitions and Notation

Definition 1: Let K be a field with $\mathrm{char}(K) \neq 2$ and $\overline{K}$ its algebraic closure. Define the hyperelliptic curve of genus two $H_{0,C}(K)$ 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. Write $H_0(K)$ whenever there is no ambiguity. 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 $\mathrm{char}(K) = 5$ without simplifying our coming calculations in any significant manner, we refrain from 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:

Define $\mathbf{J}$ to be the set ${\mathcal{J}}/{\sim}$ where $\mathcal{J} := \left\{(\mathcal{Q}_1, \mathcal{Q}_2) \;\middle|\; \mathcal{Q}_i \in H(\overline{K})\right\}$. $\mathbf{J}$ 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 Addition Law

Let $\mathbf{P}_1 = \{\mathcal{Q}_1, \mathcal{Q}_2\}$, $\mathbf{P}_2 = \{\mathcal{Q}_3, \mathcal{Q}_4\}$ with $\mathcal{Q}_i = (x_i, y_i) \in H(\overline{K})$. 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: 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 use as the components of our point $\mathbf{P}_1 + \mathbf{P}_2$.

Step 1: Let the $\mathcal{Q}_i$ and $\mathbf{P}_i$ be defined as above with $x_i \neq x_j$ whenever $i \neq j$. In addition to that, let us restrict ourselves to $\mathcal{Q}_i \in H_0(K)$. 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 $p(x) := p_3x^3 + p_2x^2 + p_1x + p_0 \in K[x]$ be the polynomial in unknown coefficients that we are looking for. With $\mathbf{y} = (y_i)_{i=1}^4$ and $\mathbf{p} = (p_i)_{i=0}^3$ the problem of determining $p(x)$ can be rewritten as

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

which by invertibility of V has of course a unique solution.

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

$$C(x) - (p(x))^2 = 0. \tag{$\star$}$$

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 some extension of the field K. Comparing the coefficients of both expressions at x^5 and x^4 yields

$$\sum_{i=1}^{6} x_i = \widetilde{T}_5 \tag{5}$$

$$\text{and} \quad \sum_{\substack{i,j=1 \\ i<j}}^{6} x_i x_j = \widetilde{T}_4 \tag{4}$$

where $\widetilde{T}_5 = \frac{1-2p_2p_3}{p_3^2}$ and $\widetilde{T}_4 = \frac{p_2^2+2p_1p_3-a}{p_3^2}$ The second expression gives

$$x_6 \sum_{i=1}^{5} x_i + \sum_{\substack{i,j=1 \\ i<j}}^{5} x_i x_j = \widetilde{T}_4.$$

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

$$\left(\widetilde{T}_5 - \sum_{i=1}^{4} x_i - x_5\right)\left(\sum_{i=1}^{4} x_i + x_5\right) + x_5 \sum_{i=1}^{4} x_i + \sum_{\substack{i,j=1 \\ i<j}}^{4} x_i x_j - \widetilde{T}_4 = 0.$$

Replacing $\widetilde{T}_5$ and $\widetilde{T}_4$ with the terms

$$T_5 := \widetilde{T}_5 - \sum_{i=1}^{4} x_i$$

$$\text{and} \quad T_4 := \widetilde{T}_4 - \sum_{\substack{i,j=1 \\ i<j}}^{4} x_i x_j$$

one obtains the tidy quadratic equation

$$x^2 - x \cdot T_5 + \left(T_4 - T_5 \sum_{i=1}^{4} x_i\right) = 0 \tag{†}$$

---

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 accomodate 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 $(\star)$ 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 $\overline{K}$. Comparing the coefficients at x^4 gives

---

$$x_5 = p_2^2 - a - \sum_{i=1}^{4} x_i \tag{††}$$

---

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 $\mathbf{P}_3 := \{(x_5, y_5), \infty\}$. Since this works just as well if $p_2 = 0$, we are done with the general case.

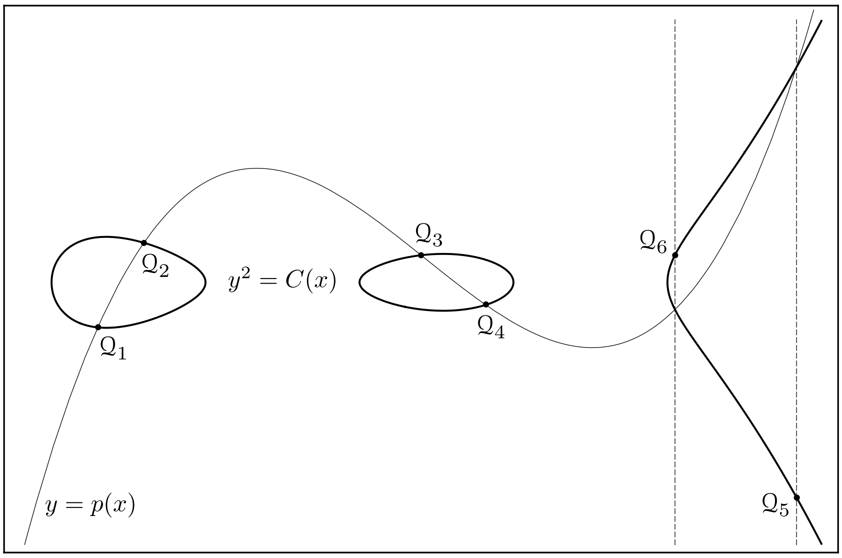

Figure 1: The general case for the addition law

Before we continue with the special cases, we want to give some consequences to the above approach.

Lemma: The the general case imposes $\overline{\mathbf{P}} + \mathbf{P} = 0$ for all $\mathbf{P} \in \mathbf{J}$, so we might want to use the notation $\overline{\mathbf{P}} = -\mathbf{P}$.

Proof. (i) Observe that if $\mathbf{P}_1 + \mathbf{P}_2 = \mathbf{P}_3 \in H_0(\overline{K})$ as in case 1, by symmetry the polynomial $-p(x)$ passes through the opposite points, meaning that

$$\{(x_5, -y_5), (x_6, -y_6)\} + \{(x_3, -y_3), (x_4, -y_4)\} = \{(x_1, y_1), (x_2, y_2)\}$$

or simply put, $\mathbf{P}_3 + \overline{\mathbf{P}}_2 = \mathbf{P}_1$. Since the choice of $\mathbf{P}_1$ and $\mathbf{P}_2$ was free, the statement must hold for any point $\mathbf{P} \in H_0(\overline{K})$. A similar argument can be made for the points in $H(\overline{K})$. $\square$

Remark 1:

(i) The Lemma implies that if $\mathbf{P} + \mathbf{P} = 0$ then $\overline{\mathbf{P}}$ equals $\mathbf{P}$, so the only candidates for points of order two are of the form $\{\mathcal{Q}, \overline{\mathcal{Q}}\}$ and those that can be written as $\{(x_1, 0), (x_2, 0)\}$ with $x_1 \neq x_2$, the latter being called 'special points'. As defined per our equivalence relation, the special points are therefore the only non-trivial points of order two.

(ii) Not only are we forced to accept the equivalence of $\{\mathcal{Q}_1, \mathcal{Q}_2\}$ and $\{\mathcal{Q}_2, \mathcal{Q}_1\}$ but if we want to construct the special cases as valid limit-cases of step 1 and 2, we must accept interchangeability between the point-components, meaning $\{\mathcal{Q}_1, \mathcal{Q}_2\} + \{\mathcal{Q}_3, \mathcal{Q}_4\}$ has to give the same result as $\{\mathcal{Q}_1, \mathcal{Q}_3\} + \{\mathcal{Q}_2, \mathcal{Q}_4\}$ and $\{\mathcal{Q}_1, \mathcal{Q}_4\} + \{\mathcal{Q}_2, \mathcal{Q}_3\}$. 1 hints at the necessity of this property.

(iii) As a bonus, this is already gives us commutativity on $\mathbf{J}$ for free.

We use property (ii) to make the coming case-distinctions more concise. Since we don't care which points in $\mathbf{J}$ the different $\mathcal{Q}_i$ belong to, we are allowed to impose conditions on the latter without any further specifications.

Let us first list all possible combinations that can be taken by the x_i and y_i provided they reside in $\overline{K}$:

A. All x_i are pairwise distinct.

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

C. Three x-coordinates overlap, e.g. $x_1 = x_2 = x_3$ and
   - a. All three y-coordinates are the same: $y_1 = y_2 = y_3 \neq 0$.
   - b. Only two y-coordinates are alike: $y_1 = y_2$ so $y_3 = -y_1$. $\star$

D. All four x_i are the same and
   - a. All four y_i equal as well but non-zero.
   - b. The y_i overlap two by two, e.g. $y_1 = y_2$ and $y_3 = y_4 = -y_1$. $\star$
   - c. Three of the y_i are alike, one isn't. $\star$

E. The x_i overlap two-by-two: $x_1 = x_2$ and $x_3 = x_4$ but $x_1 \neq x_3$ and
   - a. $y_1 = y_2$ plus $y_3 = y_4$ but neither y_1 nor y_3 is zero.
   - b. $y_1 = -y_2$, $y_3 = y_4$. $\star$
   - c. $y_1 = -y_2$ and $y_3 = -y_4$. $\star$

Due to 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. Reordering thus leads us to the following condensed list of cases for the addition law:

---

0. The addition with zero, i.e. $\mathbf{P} + \{\infty, \infty\}$ or in short $\mathbf{P} + 0$.
1. The general case where all four x-coordinates are pairwise distinct.
2. The simple tangential case where $\mathcal{Q}_1 = \mathcal{Q}_2$ and the remaining x_3, x_4 are both distinct from each other as well as from x_1.
3. The double tangential case where $\mathcal{Q}_1 = \mathcal{Q}_2$ and $\mathcal{Q}_3 = \mathcal{Q}_4$ but $\mathcal{Q}_1 \neq \pm\mathcal{Q}_3$.
4. Case where $\mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3$ but $\mathcal{Q}_4 \neq \pm\mathcal{Q}_1$.
5. The quadruple case where all $\mathcal{Q}_i$ are identical.

Remark 2:

(i) For the above list to be complete, we have to 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.

So it is important to observe that this is already secretly included in the general case and the relevant cases 2 and 4 through the following argument:

Suppose $\mathcal{Q}_4 = \infty$, so the coordinate x_4 does not exist. The polynomial $p(x)$ we pass through the 3 remaining points is therefore necessarily at most quadratic instead of cubic so the corresponding matrix to invert is the upper left 3x3 sub-matrix of V, V' or V'''. We are then immediately sent to (††) of the second step.

(ii) In both lists, the cases do not overlap.

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 $\mathcal{Q}_1 = \mathcal{Q}_2$, $y_1 \neq 0$ 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 $V' \cdot \mathbf{p} = \mathbf{y}'$ with

$$V' := \begin{pmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 0 & 1 & 2x_1 & 3x_1^2 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{pmatrix}$$

and $\mathbf{y}'$ defined as $\mathbf{y}$ with y_2 replaced by $y_2' := \frac{C'(x_1)}{2y_1}$ which is well defined since $2y_1 \neq 0$.

One can see that V' is invertible by substracting x_1 times the previous column from every column and using Laplace:

$$\det(V') = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x_1 & x_1^2 \\ 1 & (x_3 - x_1) & x_3(x_3 - x_1) & x_3^2(x_3 - x_1) \\ 1 & (x_4 - x_1) & x_4(x_4 - x_1) & x_4^2(x_4 - x_1) \end{vmatrix}$$

$$= (x_3 - x_1)(x_4 - x_1) \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_3 & x_3^2 \\ 1 & x_4 & x_4^2 \end{vmatrix}.$$

Fitting perfectly well with our constraints, this expression is 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 (††) or (†) for x_5 or x_5 and x_6.

CASE 3, DOUBLE TANGENTIAL: Let $\mathcal{Q}_1 = \mathcal{Q}_2$ 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. Like before, we lack equations for our linear system, requiring the use of a second tangential constraint. Replace the fourth row of V' and $\mathbf{y}'$ exactly like we did for the second one: $y_4'' := \frac{C'(x_3)}{2y_3}$ and

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

V'' is invertible by a similar transformation to that of the previous case:

$$\det(V'') = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x_1 & x_1^2 \\ 1 & (x_3 - x_1) & x_3(x_3 - x_1) & x_3^2(x_3 - x_1) \\ 0 & 1 & 2x_3 - x_1 & 3x_3^2 - 2x_1x_3 \end{vmatrix}$$

$$= (x_3 - x_1) \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_3 & x_3^2 \\ 1 & (2x_3 - x_1) & (3x_3^2 - 2x_1x_3) \end{vmatrix}$$

$$= (x_3 - x_1) \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_3 & x_3^2 \\ -1 & -x_1 & x_3^2 - 2x_1x_3 \end{vmatrix}$$

$$= (x_3 - x_1) \begin{vmatrix} 1 & x_1 & x_1^2 \\ 0 & x_3 - x_1 & x_3^2 - x_1^2 \\ 0 & 0 & -(x_3 - x_1)^2 \end{vmatrix}.$$

This is again different from zero precisely whenever $x_3 \neq x_1$, so as before solve $V'' \cdot \mathbf{p} = \mathbf{y}''$ for $\mathbf{p}$, then (†) or (††) depending on p_3.

Case 4, Second Order Tangential: Let $\mathcal{Q}_1 = \mathcal{Q}_2 = \mathcal{Q}_3$ 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 $\mathcal{Q}_1$:

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

This is invertible in the given circumstance because

$$\begin{aligned} \det(V''') &= \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x_1 & x_1^2 \\ 0 & 0 & 2 & 4x_1 \\ 1 & x_4 - x_1 & x_4(x_4 - x_1) & x_4^2(x_4 - x_1) \end{vmatrix} \\ &= 2(x_4 - x_1) \begin{vmatrix} 1 & x_1 & x_1^2 \\ 0 & 1 & 2x_1 \\ 1 & x_4 & x_4^2 \end{vmatrix} \\ &= 2(x_4 - x_1) \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & x_1 \\ 1 & x_4 - x_1 & x_4(x_4 - x_1) \end{vmatrix} \\ &= 2(x_4 - x_1)^3 \neq 0 \text{ for } x_1 \neq x_4. \end{aligned}$$

With this, define $\mathbf{y}'''$ by taking $\mathbf{y}'$ and replacing the third coordinate by $y_3''' := \frac{C''(x_1)}{2y_1} - (\frac{C'(x_1)}{2y_1})^2$. Again, apply the same procedure as in the second steps of case 1 to find $\mathbf{P}_3$.

Case 5, Third Order Tangential: Given the quadruple situation where $\mathcal{Q}_i = \mathcal{Q}$ for every i and knowing the point $\mathcal{Q} := (x_0, y_0)$ with $y_0 \neq 0$, we solve

$$V'''' = \begin{pmatrix} 1 & x_0 & x_0^2 & x_0^3 \\ 0 & 1 & 2x_0 & 3x_0^2 \\ 0 & 0 & 2 & 6x_0 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

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

Here $\mathbf{y}''''$ is the same as $\mathbf{y}'''$ except for the last coordinate which should read

$$y_4''' := \frac{1}{2y_0}\Big(C'''(x_0) - \frac{dy}{dx}\Big|_{\mathcal{Q}}\Big(\big(\frac{dy}{dx}\Big|_{\mathcal{Q}}\big)^2 - \frac{d^2y}{dx^2}\Big|_{\mathcal{Q}}\Big)\Big).$$

The derivatives are known through the previous steps. Once more, we solve the linear system $V'''' \cdot \mathbf{p} = \mathbf{y}''''$ and subsequently (†) or (††) and we're done.