Elliptic Curves

1.1 Weierstrass Equations

Definition 1.1. An (affine) elliptic curve E over a field $\mathbb{F}$ is a curve which is given by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

1.2. If you define on the set of the terms $\{x^a y^b : (a,b) \in \mathbb{N}^2\}$, the weight function wt defined by $\mathrm{wt}(x) = 2, \mathrm{wt}(y) = 3$, remark that in (1.1) each coefficient a_i of a term τ has the value $i := 6 - \mathrm{wt}(\tau)$.

Such mnemonics is preserved throughout all the reformulations of (1.1).

1.3. If we assume that $\mathrm{char}(\mathbb{F}) \neq 2$, we can perform the linear transformation $y \to y - \frac{a_1x - a_3}{2}$ obtaining the equation

$$y^2 = x^3 + \frac{a_1^2 + 4a_2}{4}x^2 + \frac{a_1a_3 + 2a_4}{2}x + \frac{a_3^2 + 4a_6}{4} =: x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}. \tag{1.2}$$

1.4. If moreover $\mathrm{char}(\mathbb{F}) \neq 3$, the linear transformation $x \to x - \frac{b_2}{12}$ produces the equation

$$\begin{aligned}
y^2 &= \left(x - \frac{b_2}{12}\right)^3 + \frac{b_2}{4}\left(x - \frac{b_2}{12}\right)^2 + \frac{b_4}{2}\left(x - \frac{b_2}{12}\right) + \frac{b_6}{4} \\
&= x^3 + \left(3 \cdot \frac{b_2^2}{12^2} - 2\frac{b_2}{4}\frac{b_2}{12} + \frac{b_4}{2}\right)x + \left(-\frac{b_2^3}{12^3} + \frac{b_2}{4}\frac{b_2^2}{12^2} - \frac{b_4}{2}\frac{b_2}{12} + \frac{b_6}{4}\right) \\
&= x^3 + \left(\left(\frac{3}{12^2} - \frac{2}{48}\right)b_2^2 + \frac{b_4}{2}\right)x + \left(\left(-\frac{1}{12^3} + \frac{1}{4 \cdot 12^2}\right)b_2^3 - \frac{b_2b_4}{24} + \frac{b_6}{4}\right) \\
&= x^3 + \left(\frac{1-2}{48}b_2^2 + \frac{b_4}{2}\right)x + \left(\frac{-1+3}{2^6 3^3}b_2^3 + \frac{b_2b_4}{24} + \frac{b_6}{4}\right) \\
&= x^3 - \frac{b_2^2 - 24b_4}{48}x + \left(-\frac{-b_2^3 + 36b_2b_4 - 216b_6}{2^5 3^3}\right) \\
&= x^3 - \frac{b_2^2 - 24b_4}{48}x - \frac{-b_2^3 + 36b_2b_4 - 216b_6}{864} \\
&=: x^3 - \frac{c_4}{48}x - \frac{c_6}{864}
\end{aligned} \tag{1.3}$$

1.5. Denoting

$$\begin{aligned}
f(x,y) &= y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6, \\
g(x,y) &= y^2 - x^3 + \frac{c_4}{48}x + \frac{c_6}{864},
\end{aligned}$$

it holds

$$f\left(x - \frac{b_2}{12}, y - \frac{a_1\left(x - \frac{b_2}{12}\right) - a_3}{2}\right) = f\left(x - \frac{b_2}{12}, y - \frac{12a_1x - a_1b_2 - 12a_3}{24}\right) = g(x,y).$$

1.6. If we assume $\mathbb{F} = \mathbb{Q}$, it is natural to compute the polynomial $h(x,y) \in \mathbb{Z}[x,y]$ such that

$$h(x,y) = \alpha g(\frac{x}{\beta}, \frac{y}{\gamma}) \in \mathbb{Z}[x,y].$$

Such condition requires that $\alpha, \beta, \gamma \in \mathbb{Z}$ satisfy

$$\alpha = \gcd(\beta^3, \gamma^2, 48, 864) = \gcd(\beta^3, \gamma^2, 2^4 3, 2^5 3^3);$$

Figure 1.1:

$$\begin{array}{rcl} b_2 & := & a_1^2 + 4a_2, \\ b_4 & := & a_1a_3 + 2a_4, \\ b_6 & := & a_3^2 + 4a_6, \\ b_8 & := & a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2; \\ \\ c_4 & := & b_2^2 - 24b_4, \\ c_6 & := & -b_2^3 + 36b_2b_4 - 216b_6; \\ \\ \Delta & := & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6; \\ j & := & \frac{c_4^3}{\Delta} \text{ (if } \Delta \text{ is invertible)} \end{array}$$

related by the identities

$$4b_8 = b_2b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

the minimal solution is

$$\alpha = 2^6 3^6 = 6^6, \beta = 6^2, \gamma = 6^3$$

which gives

$$h(x,y) = y^2 - x^3 + \frac{6^4}{2^4 3} c_4 x + \frac{6^6}{2^5 3^3} c_6 = y^2 - x^3 + 27c_4x + 54c_6. \tag{1.4}$$

1.7. We will also use, when $\mathrm{char}(\mathbb{F}) \neq 2, 3$ the equation

$$y^2 = x^3 + Ax + B \tag{1.5}$$

where we have $A = -\frac{c_4}{48}, B = -\frac{c_6}{864}$.

1.2 Discriminant

Definition 1.8. Let $f \in \mathbb{F}[x,y]$ be a polynomial and let C be the curve over $\mathbb{F}$ given by the equation $f(x,y) = 0$.

A singular point of C is any point $(x_0, y_0) \in \overline{\mathbb{F}}^2$ (with coordinates in the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$) such that

$$f(x_0,y_0) = \frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0) = 0. \tag{1.6}$$

1.9. Let us restrict ourselves to the case $\mathrm{char}(\mathbb{F}) \neq 2$ and consider an elliptic curve given by

$$f(x,y) = y^2 - g(x);$$

the potential singular points $(x_0, y_0) \in \overline{\mathbb{F}}^2$ must satisfy equation (1.6); since we have

$$\frac{\partial f}{\partial x} = \frac{\partial g}{\partial x} \text{ and } \frac{\partial f}{\partial y} = 2y,$$

and we are assuming $\mathrm{char}(\mathbb{F}) \neq 2$, we have that (x_0, y_0) is a singular point if and only if

(a) $0 = \frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial g}{\partial x}(x_0)$,

(b) $0 = \frac{\partial f}{\partial y}(x_0,y_0) = 2y_0 \implies y_0 = 0$ and

(c) $0 = f(x_0,y_0) = y_0^2 - g(x_0)$, which, by (b), is equivalent to $g(x_0) = y_0^2 = 0$,

id est if and only if $y_0 = 0$ and $g(x_0) = g'(x_0) = 0$.

In other words the elliptic curve given by $f(x,y) = y^2 - g(x)$ has a singular point $P \in \overline{\mathbb{F}}^2$ if and only if $g(x)$ has a singular point x_0 if and only if the discriminant $\mathrm{Disc}(g)$ of g is zero. If $\mathrm{Disc}(g) = 0$ we have $P = (x_0, 0)$ where x_0 is the singular point of g.

1.10. We recall that for a polynomial $g(x) = e_0x^3 + e_1x^2 + e_2x + e_3$ its discriminant is

$$\mathrm{Disc}(g) = e_1^2e_2^2 - 4e_0e_2^3 - 4e_1^3e_3 - 27e_0^2e_3^2 + 18e_0e_1e_2e_3. \tag{1.7}$$

Remark that for $\bar{g}(x) = ag(\frac{x}{b})$, we have $\bar{g}g(x) = \frac{a}{b^3}e_0x^3 + \frac{a}{b^2}e_1x^2 + \frac{a}{b}e_2x + ae_3$ so that $\mathrm{Disc}(\bar{g}) = \frac{a^4}{b^6}$

1.11. Therefore, if we apply this formula to equation (1.2), *id est* to $g = 4x^3 + b_2x^2 + 2b_4x + b_6$ we obtain

$$\begin{aligned}\frac{\mathrm{Disc}(g)}{e_0^2} &= e_0^{-2}e_1^2e_2^2 - 4e_0^{-1}e_2^3 - 4e_0^{-2}e_1^3e_3 - 27e_3^2 + 18e_0^{-1}e_1e_2e_3 \\ &= \frac{1}{4}b_2^2b_4^2 - 2^3b_4^3 - \frac{1}{4}b_2^3b_6 - 27b_6^2 + \frac{18}{2}b_2b_4b_6 \\ &= \frac{1}{4}b_2^2\left(b_4^2 - b_2b_6\right) - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ &=: \Delta\end{aligned}$$

where we have defined

$$b_8 := \frac{1}{4}\left(b_2b_6 - b_4^2\right) = \frac{1}{4}\left(\left(a_1^2 + 4a_2\right)\left(a_3^2 + 4a_6\right) - \left(a_1a_3 + 2a_4\right)^2\right) = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2.$$

Definition 1.12. In case $\mathrm{char}(\mathbb{F}) \neq 2$, the discriminant Δ of the elliptic curve given by (1.2) is defined

$$\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Theorem 1.13. *If $\mathrm{char}(\mathbb{F}) \neq 2$, an elliptic curve given by a Weierstress equation (1.1) is singular if and only if $\Delta = 0$.*

1.14. Alternatively, in case $\mathrm{char}(\mathbb{F}) \neq 3$ too, one can compute (up to constants) $\mathrm{Disc}(g)$ via a direct computation of $\gcd(g(x), g'(x))$ using the euclidean algorithm; we do it using equation (1.3), and $g = x^3 - 27c_4x - 54c_6$.

A direct application of the Euclidean algorithm computes

- $r_{-1} := g = x^3 - 27c_4x - 54c_6$,
- $r_0 := \frac{g'}{3} = x^2 - 9c_4$,
- $r_1 := \frac{-1}{18}\left(r_{-1} - xr_0\right) = c_4x + 3c_6$,
- $c_4^2r_0 - \left(c_4x - 3c_6\right)r_1 = 9(c_6^2 - c_4^3)$.

whence

$$\gcd(g(x), g'(x) = 0 \iff c_6^2 - c_4^3 = 0.$$

A direct computation gives

$$\begin{aligned}c_4^3 - c_6^2 &= \left(b_2^2 - 24b_4\right)^3 - \left(-b_2^3 + 36b_2b_4 - 216b_6\right)^2 \\ &= \left(b_2^6 - 72b_2^4b_4 + 1728b_2^2b_4^2 - 13824b_4^3\right) \\ &- \left(b_2^6 - 72b_2^4b_4 + 432b_2^3b_6 + 1296b_2^2b_4^2 - 15552b_2b_4b_6 + 46656b_6^2\right) \\ &= -432b_2^3b_6 + 432b_2^2b_4^2 + 15552b_2b_4b_6 - 13824b_4^3 - 46656b_6^2 \\ &= -2^43^3b_2^3b_6 + 2^43^3b_2^2b_4^2 + 2^63^5b_2b_4b_6 - 2^93^3b_4^3 - 2^63^6b_6^2 \\ &= 2^63^3\left(\frac{b_4^2 - b_2b_6}{4}b_2^2 + 3^2b_2b_4b_6 - 2^3b_4^3 - 3^3b_6^2\right) \\ &= 1728\Delta\end{aligned}$$

while, for $g = x^3 - 27c_4x - 54c_6$, the discriminant formula gives $\mathrm{Disc}(g) = 78732\left(c_4^3 - c_6^2\right) = 2^23^9\left(c_4^3 - c_6^2\right)$

1.15. A faster evaluation is obtain, in case $\mathrm{char}(\mathbb{F}) \neq 2, 3$, by computing $\mathrm{Disc}(g)$ for the polynomial $g = x^3 + Ax + B$ connected to equation (1.5); the result is

$$\mathrm{Disc}(g) = -4A^3 - 27B^2.$$

If we set $A = -\frac{c_4}{48} - \frac{c_4}{2^43}, B = -\frac{c_6}{2^53^3}$ we obtain

$$-4A^3 - 27B^2 = \frac{c_4^3 - c_6^2}{3^32^{10}} = \frac{c_4^3 - c_6^2}{1728}\frac{1}{16} = \frac{\Delta}{16}.$$

1.16. Recalling that if $\bar{g}(x) = ag(\frac{x}{b})$, we have $\mathrm{Disc}(\bar{g}) = \frac{a^4}{b^6}$, if we compare the three cubic polynomials in $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) \neq 2, 3$, related to the equations (1.2)and (1.5) namely

$$\begin{aligned} g_1 &:= 4x^3 + b_2x^2 + 2b_4x + b_6, \\ g_2 &:= x^3 - \frac{c_4}{48}x - \frac{c_6}{864}, \\ g_3 &:= x^3 - 27c_4x - 54c_6 \end{aligned}$$

we have

- $g_1 = 4g_2$ so that necessarily $\operatorname{Disc}(g_1) = 4^4 \operatorname{Disc}(g_2) = 16\Delta$;
- $g_2(x) = g_3(\frac{x}{6^2})$ so that necessarily

$$\operatorname{Disc}(g_3) = 6^{12} \operatorname{Disc}(g_2) = \frac{6^{12}}{16}\Delta = \frac{6^{12}}{16 \cdot 1728}(c_4^3 - c_6^2) = \frac{2^{12}3^{12}}{2^{4+6}3^3}(c_4^3 - c_6^2) = 2^2 3^9 (c_4^3 - c_6^2) = 78732(c_4^3 - c_6^2).$$

We submarize the relations as

$c_4^3 - c_6^2$	$=$		$2^6 3^3 \Delta$	$2^{18}3^3 \operatorname{Disc}(g_1)$	$2^{10}3^3 \operatorname{Disc}(g_2)$	$2^{-2}3^{-9} \operatorname{Disc}(g_3)$
Δ	$=$	$2^{-6}3^{-3}(c_4^3 - c_6^2)$		$2^{-2} \operatorname{Disc}(g_1)$	$2^2 \operatorname{Disc}(g_2)$	$2^4 \operatorname{Disc}(g_3)$
$\operatorname{Disc}(g_1)$	$=$	$2^{-2}3^{-3}(c_4^3 - c_6^2)$	$2^4 \Delta$		$2^8 \operatorname{Disc}(g_2)$	$2^{-4}3^{-12} \operatorname{Disc}(g_3)$
$\operatorname{Disc}(g_2)$	$=$	$2^{-10}3^{-3}(c_4^3 - c_6^2)$	$2^{-4} \Delta$	$\operatorname{Disc}(g_1)$		$\operatorname{Disc}(g_3)$
$\operatorname{Disc}(g_3)$	$=$	$2^2 3^9 (c_4^3 - c_6^2)$	$2^8 3^{12} \Delta$	$\operatorname{Disc}(g_1)$	$2^{12}3^{12} \operatorname{Disc}(g_2)$	

1.17. Remark that if we define, for each field $\mathbb{F}$ without any restriction on characteristic, the values b_2, b_4, b_6, b_8, c_4, c_6, Δ, j according Figure 1.1, the relations

$$4b_8 = b_2b_6 - b_4^2 \text{ and } 1728\Delta = c_4^3 - c_6^2.$$

still hold also when

- $\operatorname{char}(\mathbb{F}) = 2$ where
$$b_2 = a_1^2, b_4 = a_1a_3, b_6 = a_3^2, c_4 = b_2^2, c_6 = -b_2^3,$$
so that
$$b_2b_6 - b_4^2 = a_1^2a_3^2 - (a_1a_3)^2 = 0 = 4b_8$$
and $c_4^3 - c_6^2 = (b_2^2)^3 - (-b_2^3)^2 = 0 = 1728\Delta$;
- $\operatorname{char}(\mathbb{F}) = 3$ where $c_4 = b_2^2, c_6 = -b_2^3$ so that, again
$$c_4^3 - c_6^2 = (b_2^2)^3 - (-b_2^3)^2 = 0 = 1728\Delta$$
while $b_2b_6 - b_4^2 = 4b_8$ was already proved in 1.10.

1.3 Singular points

1.18. Each cubic polynomial $f(x, y) \in \mathbb{F}$ can be expressed as a Taylor expansion on each point $P = (x_0, y_0) \in \mathbb{F}^2$:

$$\begin{aligned} f(x,y) &= f(P) + (x - x_0)\frac{\partial f}{\partial x}(P) + (y - y_0)\frac{\partial f}{\partial y}(P) + \\ &+ \frac{1}{2}(x - x_0)^2\frac{\partial^2 f}{\partial^2 x}(P) + \frac{1}{2}(x - x_0)(y - y_0)\frac{\partial^2 f}{\partial x \partial y}(P) + \frac{1}{2}(y - y_0)^2\frac{\partial^2 f}{\partial^2 y}(P) \\ &+ \frac{1}{6}(x - x_0)^3\frac{\partial^3 f}{\partial^3 x}(P) + r(x, y) \end{aligned}$$

where the term

$$r(x, y) = \frac{1}{12}(x - x_0)^2(y - y_0)\frac{\partial^3 f}{\partial^2 x \partial y}(P) + \frac{1}{12}(x - x_0)(y - y_0)^2\frac{\partial^3 f}{\partial x \partial^2 y}(P) + \frac{1}{6}(y - y_0)^3\frac{\partial^3 f}{\partial^3 y}(P)$$

assume the value 0 for an elliptic curve.

In the case $\operatorname{char}(\mathbb{F}) \neq 2, 3$, for the elliptic curve E given by

$$f(x, y) = y^2 - x^3 + \frac{c_4}{48}x + \frac{c_6}{864}$$

and the singular point $P = (x_0, y_0)$, we have

$$f(x_0,y_0) = \frac{\partial f}{\partial x}(x_0,y_0) = \frac{\partial f}{\partial y}(x_0,y_0) = 0;$$

moreover

$$\frac{\partial^2 f}{\partial^2 x}(P) = -6x, \frac{\partial^2 f}{\partial x \partial y}(P) = 0, \frac{\partial^2 f}{\partial^2 y}(P) = 2, \frac{\partial^3 f}{\partial^3 x} = -6$$

therefore

$$\begin{aligned} f(x,y) &= \frac{1}{2}\left(-6x_0(x-x_0)^2 + 2(y-y_0)^2\right) - (x-x_0)^3 \\ &= \frac{1}{2}\left(\left(\frac{(y-y_0)}{(x-x_0)}\right)^2 - 3x_0\right) - (x-x_0)^3. \end{aligned}$$

Let us restrict ourselves to the case $\mathbb{F} = \mathbb{R}$; in this case we have three diffierent cases;

- if $x_0 > 0$

$$f(x,y) = \left((y-y_0) - \sqrt{3x_0}(x-x_0)\right)\left((y-y_0) + \sqrt{3x_0}(x-x_0)\right) - (x-x_0)^3$$

  and we have a *node*;

- if $x_0 = 0$

$$f(x,y) = (y-y_0)^2 - (x-x_0)^3$$

  and we have a *cusp*;

- if $x_0 < 0$

$$f(x,y) = \left((y-y_0)^2 + 3|x_0|(x-x_0)^2\right) - (x-x_0)^3$$

  where $(y-y_0)^2 + 3|x_0|(x-x_0)^2$ is irreducible in $\mathbb{R}[x,y]$ and $P = (x_0,y_0)$ is its single root.

1.19. For a generic field $\mathbb{F}$, $\text{char}(\mathbb{F}) \neq 2,3$, we have essentially the three diffierent cases according the factorization structure of the polynomial $d(z) := z^2 - 3x_0 \in \mathbb{F}[z]$:

- if $d(z) = (z-\alpha)(z-\beta), \alpha,\beta \in \mathbb{F}, \alpha \neq \beta$, has two different factors in $\mathbb{F}[z]$ then

$$f(x,y) = ((y-y_0) - \alpha(x-x_0))((y-y_0) - \beta(x-x_0)) - (x-x_0)^3$$

  and we have a *split-case node*

- if $d(z) = (z-\alpha)^2, \alpha \in \mathbb{F}$ has a factor with multiplicity 2 in $\mathbb{F}[z]$ then

$$f(x,y) = ((y-y_0) - \alpha(x-x_0))^2 - (x-x_0)^3$$

  and we have a *cusp*

- if $d(z)$ is irreducible, then

$$f(x,y) = \left((y-y_0)^2 - 3x_0(x-x_0)^2\right) - (x-x_0)^3$$

  and we have a *nonsplit-case node*

1.4 Discriminant (2)

1.20. Let us now consider an elliptic curve given by a Weiwerstrass equation (1.1).
If it is singular we can wlog assume that singular point P is $P = (0,0)$; therefore

$$\begin{aligned} 0 &= f(0,0) &= a_6, \\ 0 &= \tfrac{\partial f}{\partial x}(0,0) &= a_4, \\ 0 &= \tfrac{\partial f}{\partial y}(0,0) &= a_3. \end{aligned}$$

We already remarked that the values introduced in Figure 1.1 are defined without any restriction on characteristic. Thus, for a singular curve (1.1), we have

$$b_2 = a_1^2 + 4a_2, b_4 = b_6 = b_8 = 0, c_4 = (a_1^2 + 4a_2)^2, c_6 = (a_1^2 + 4a_2)^3$$

so that $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = 0$.

Lemma 1.21. *If an elliptic curve given by a Weierstress equation (1.1) is singular then* $\Delta = 0$.

Moreover such singular curve is given by an equation $f(x,y) = x^3$ where we set

$$f(x,y) = y^2 + a_1xy - a_2x^2$$

and $f(x,y)$ factorizes in $\overline{\mathbb{F}}$ into either

- two linear distinct factors iff $a_1^2 + 4a_2 \neq 0$ (node case),
- a single linear factor with multiplicity 2 iff $a_1^2 + 4a_2 = 0$ (cusp case).

We have already proved in Theorem 1.13 the converse of Lemma 1.21iff $\mathrm{char}(\mathbb{F}) \neq 2$ and, in Corollaries 1.55 and 1.64, we will prove that also in case $\mathrm{char}(\mathbb{F}) = 2$.

Theorem 1.22. *An elliptic curve given by a Weierstress equation (1.1) is singular if and only if* $\Delta = 0$.
It has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$*; it has a cusp if and only if* $\Delta = 0$ *and* $c_4 = 0$.

1.5 Elliptic curves in the Reals

1.6 Projective space

1.7 Projective elliptic curves

1.23. Recall that for a projective curve C given by a homogeneous polynomial $F(X,Y,Z)$, a point P on C and a line $\ell := aX + bY + cZ$:

(1) P is non singular iff at least one among $\frac{\partial F}{\partial X}(P)$, $\frac{\partial F}{\partial Y}(P)$, $\frac{\partial F}{\partial Z}(P)$ is non zero,

(2) in which case the tangent L to the curve C at the non singular point P is

$$L = \frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z.$$

Up to a proper translation we can wlog assume $P = (0:0:1)$ and express F as

$$F(X,Y,Z) = \sum_{i=0}^{\deg(F)} f_i(X,Y)Z^{\deg(F)-i},$$

with $f_0 = 0$[1]

If moreover $\ell(P) = 0$, so that $c = 0$, its projective points are $\{bt : -at : 10\}$ and we have

$$F(bt,-at,1) = \sum_{i=1}^{\deg(F)} f_i(b,-a)t^i.$$

We define

(3) the intersection multiplicity of ℓ and F at P, $i(P,\ell,F)$, as

$$i(P,\ell,F) := \begin{cases} +\infty & \text{iff } F(bt,-at,1) = 0 \\ \min\{j : f_j \neq 0\} & \text{iff } F(bt,-at,1) = \sum_{i=j}^{\deg(F)} f_i(b,-a)t^i \neq 0; \end{cases}$$

(4) P a flex or inflection point of F if the intersection multiplicity of the tangent line L to F at P satisfies $i(P,\ell,F) \geq 3$.

1.24. We can consider the projective version of the elliptic curve E given by (1.1), namely the curve consisting of all (projective) solutions of the polynomial

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - \left(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\right) \tag{1.8}$$

whose finite points are the set $\{(x:y:1) : (x,y) \in E\}$ and whose single roint at infinity is the only solution of the equation

$$0 = F(X,Y,0) = X^3,$$

namely $O := (0:1:0)$.

[1]since $F(P) = 0 \iff f_i(0,0) = 0$ for each i and $f_0 \in \mathbb{F}$.

1.25. Since

$$\begin{aligned}\frac{\partial F}{\partial X} &= a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2,\\ \frac{\partial F}{\partial Y} &= 2YZ + a_1XZ + a_3Z^2,\\ \frac{\partial F}{\partial Z} &= Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2,\end{aligned}$$

and

$$\frac{\partial F}{\partial X}(O) = \frac{\partial F}{\partial Y} = 0, \frac{\partial F}{\partial Z}(O) = 1$$

, we cab deduce that

(1) O is non singular,

(2) the tangent to E at O is $L = Z$;

Moreover, since $F(X, Y, Z) = \sum_{i=1}^{3} f_iY^{3-i}$ with

$$\begin{aligned}f_1 &= Z,\\ f_2 &= a_1XZ + a_3Z^2,\\ f_3 &= -(X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3),\end{aligned}$$

we have $F(t, 1, 0) = t^3$ so that

(3) $i(O, L, F) = 3$ and

(4) O is a flex.

1.26. Let $G(X, Y, Z) \in \mathbb{F}[X, Y, Z]$ be a generic cubic[2]

$$G(X,Y,Z) = c_{300}X^3 + c_{210}X^2Y + c_{120}XY^2 + c_{030}Y^3 + c_{201}X^2Z + c_{111}XYZ + c_{021}Y^2Z + c_{102}XZ^2 + c_{012}YZ^2 + c_{033}Z^3$$

and the curve C defined by it; if we impose that

(1) $P = (0 : 1 : 0) \in C$,

(2) P is not singular,

(3) the tangent L to C at P is Z,

(4) P is a flex point and

(5) $Z \nmid G$

we obtain

(1) $0 = G(0, 1, 0) = c_{030}Y^3$;

(2) since $\frac{\partial G}{\partial Y}(P) = 3c_{030} = 0$, necessarily either $0 \neq \frac{\partial G}{\partial X}(P) = c_{120}$ or $0 \neq \frac{\partial G}{\partial Z}(P) = c_{021}$;

(3) the tangent $L = c_{120}X + c_{021}Z$ is $Z \iff c_{120} = 0$ and $c_{021} \neq 0$;

(4) $Z \mid c_{210}X^2Y + c_{111}XYZ + c_{012}YZ^2 \implies c_{210} = 0$;

(5) $Z \nmid G = c_{300}X^3 + c_{201}X^2Z + c_{111}XYZ + c_{021}Y^2Z + c_{102}XZ^2 + c_{012}YZ^2 + c_{033}Z^3 \implies c_{300} \neq 0$.

If we now compute $G(tx, ty, 1)$ we obtain

$$G(tx, ty, 1) = c_{300}t^3x^3 + c_{201}t^2x^2 + t^2c_{111}xy + c_{021}t^2y^2 + c_{102}tx + c_{012}ty + c_{033};$$

and we can further grant $c_{300}t^3 = c_{021}t^2 = 1$ setting $t = \frac{c_{021}}{c_{300}}$.

The equation, thus becomes

$$G = c_{300}\{X^3 + \frac{c_{201}}{c_{300}}X^2Z + \frac{c_{111}}{c_{300}}XYZ + Y^2Z + \frac{c_{201}}{c_{102}}XZ^2 + \frac{c_{012}}{c_{300}}YZ^2 + \frac{c_{033}}{c_{300}}Z^3$$

namely (1.1).

[2]The argiment of this section does not need any restriction on characteristic.

Lemma 1.27. *If $G(X,Y,Z) \in \mathbb{F}[X,Y,Z]$ is a cubic which has a flex at $(x_0 : y_0 : z_0)$, then there is a projective transformation Φ such that $f^{\Phi}(X,Y,Z) = f(\Phi_1^{-1}(X), \Phi_1^{-1}(Y), \Phi_1^{-1}(Z))$ has (1.8) as equation.*

Proof. In fact if Φ_1 is the translation such that $\Phi_1(x_0 : y_0 : z_0) = (0:1:0)$ then $f^{\Phi_1} := f(\Phi_1^{-1}(X), \Phi_1^{-1}(Y), \Phi_1^{-1}(Z))$ has a flax at $(0:1:0)$.

Let $L(X,Y,Z) = \alpha X + \beta Z$ be the tangent to f^{Φ_1} at $(0:1:0)$ and choose a non singular matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $L(a,b,1) = \alpha a + \beta b = 0$ and define

$$\Phi_2^{-1} = \begin{pmatrix} a & 0 & b \\ 0 & 1 & 0 \\ c & 0 & d \end{pmatrix}.$$

Then $\Phi_2^{-1}(\alpha : 0 : \beta) = (0:0:1)$ and L^{Φ_2} is the same line as Z so that $(f^{\Phi_1})^{\Phi_2} = f^{\Phi_2\Phi_1}$ has a flex at $(0:1:0)$ with Z as tangent..

The matrix

$$\Phi_3(t)^{-1} = \begin{pmatrix} t & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is such that

$$f^{\Phi_3(t)\Phi_2\Phi_1} = (f^{\Phi_2\Phi_1})\Phi_3(t) = f^{\Phi_2\Phi_1}(tX, tY, Z) = c_{YYZ}t^3Y^2Z + \cdots + c_{XXX}t^3X^3 + \cdots$$

Thus for $t = \frac{c_{YYZ}}{c_{XXX}}$ the coefficients of Y^2Z and X^3 are the same.. □

1.8 Bezout's Theorem

Fact 1.28 (Bezout's Theorem). *Let C_1 and C_2 be two projective curve with no common component. Then, it holds*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \deg(C_1)\deg(C_2).$$

where $I(C_1 \cap C_2, P)$ is properly defined as multiplicity index to each point $P \in C_1 \cap C_2$, in such a way that $I(C_1 \cap C_2, P) := i(P, \ell, C_1)$ in the particular case in which $C_2 = \ell$ is a line.

1.29. Thus if C is an irreducilbe non-singular elliptic curve and ℓ is any line, either

- either $C \cap \ell$ consists of three different point, or
- ℓ is the tangent to C at P, $i(P, \ell, C_1) = 2$ and there is a thrid point $Q \in C \cup \ell$, $Q \neq P$, or
- $P \in C \cup \ell$ is a flex point.

1.30. Let us assume that C is an elliptic curve with a singular point which we can wlog assume to be $P = (0:0;1)$ and consider the intersection $C \cap \ell$ where $\ell = ax + by$ is any line s.t. $P \in \ell$:

- if C is a cusp so that $F = Y^2Z - X^3$:
  - if $a = 0$, $F(t,0,1) = t^3$, $i(P, \ell, C) = 3$;
  - if $b = 0$, $F(0,t,1) = t^2$, $i(P, \ell, C) = 2$ the third point being $O = (0:1:0)$;
  - if $a \neq 0 \neq b$, $F(bt, -at, 1) = a^2t^2 - b^3t^3 = -t^2(t - \frac{a^2}{b^3}$ so that $i(P, \ell, C) = 2$ the third point being $Q := (c^2 : -c^3 : 1)$, with $c := \frac{a}{b}$
- if C is a split-case node so that $F = Y^2Z - d^2X^2Z - X^3$
  - if $a = 0$, $F(t,0,1) = -d^2t^2 - t^3 = -t^2(t + d^2)$, $i(P, \ell, C) = 2$ the third point being $O = (0 : -d^2 : 1)$;
  - if $b = 0$, $F(0,t,1) = t^2$, $i(P, \ell, C) = 2$ the third point being $O = (0:1:0)$;
  - if $a \neq 0 \neq b$, $F(bt, -at, 1) = a^2t^2 - d^2b^2t^2 - b^3t^3 = -t^2(t - \frac{a^2 - d^2b^2}{b^3}$ so that
    - $i(P, \ell, C) = 2$ the third point being $Q := (c^2 - d^2 : c^3 - d^2c : 1)$, with $c := \frac{a}{b}$ if $c \neq \pm d$
    - $i(P, \ell, C) = 3$ if $a^2 - d^2b^2 = 0$.
- if C is a nonsplit-case node. so that $F = (Y^2Z + d^2X^2Z - X^3$
  - if $a = 0$, $F(t,0,1) = d^2t^2 - t^3 = -t^2(t - d^2)$, $i(P, \ell, C) = 2$ the third point being $O = (0 : d^2 : 1)$;
  - if $b = 0$, $F(0,t,1) = t^2$, $i(P, \ell, C) = 2$ the third point being $O = (0:1:0)$;
  - if $a \neq 0 \neq b$, $F(bt, -at, 1) = a^2t^2 + d^2b^2t^2 - b^3t^3 = -t^2(t - \frac{a^2 + d^2b^2}{b^3}$ so that $i(P, \ell, C) = 2$ the third point being $Q := (c^2 + d^2 : c(c^2 + -d^2) : 1)$, with $c := \frac{a}{b}$

1.9 Arithmetics of the points of an elliptic curve (1)

1.10 Admissible change of variables

1.31. Let us consider the generic change of variables $\Phi : \mathbb{P}^3 \to \mathbb{P}^3$

$$X = a_{11}X' + a_{12}Y' + a_{13}Z', \quad Y = a_{21}X' + a_{22}Y' + a_{23}Z', \quad Z = a_{31}X' + a_{32}Y' + a_{33}Z'; \tag{1.9}$$

if we apply it to a cubic $F(X, Y, Z)$ in Weierstrass form, in order to obtain

$$F'(X', Y', Z') = F(a_{11}X' + a_{12}Y' + a_{13}Z', a_{21}X' + a_{22}Y' + a_{23}Z, a_{31}X' + a_{32}Y' + a_{33}Z')$$

still in Weierstrass form, we must at least be granted that

- $\Phi(Z) = Z$ so that $a_{31} = a_{32} = 0, a_{33} = 1$;
- $O = (0 : 1 : 0)$ is preserved so that $a_{12} = a_{32} = 0$;
- the weight $\mathrm{wt}(X) = 3, \mathrm{wt}(Y) = 2$ is preserved
- or (what is essentially the same) that $a_{11}^3 = a_{21}^2 \neq 0$.

1.32. It is then easy to realize that the most general allowable change of coordinates Φ which transform each cubic $F(X, Y, Z)$ in Weierstrass form into a cubic still in Weierstrass form is

$$X = u^2X' + rZ', \quad Y = u^3Y' + u^2sX' + tZ', \quad Z = Z'; \tag{1.10}$$

and (in the affine case)

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t. \tag{1.11}$$

1.33. Remark that there is an inverse transformation

$$x' = v^2x + r', \quad y' = v^3y' + v^2s'x + t' \tag{1.12}$$

which satisfies

$$\begin{array}{rclcrcl} & & uv & = & 1, & & \\ r & = & -u^2r', & & r' & = & -v^2r, \\ s & = & -us', & & s' & = & -vs, \\ t & = & -u^3[t' - s'r'], & & t' & = & -v^3[t - sr],. \end{array}$$

since

$$\begin{array}{rcll} x & = & u^2(v^2x + r') + r & = x, \\ y & = & u^3(v^3y + v^2s'x + t') + u^2s(v^2x + r') + t & \\ & = & u^3v^3y + u^2v^2(us' + s)x + (u^3t' + u^2sr' + t) & \\ & = & u^3v^3y + u^2v^2(us' + s)x + (u^3t' - u^3s'r' + t) & = y \\ x' & = & v^2(u^2x' + r) + r' & = x', \\ y' & = & v^3(u^3y + u^2sx' + t) + v^2s'(u^2x' + r) + t' & \\ & = & u^3v^3y' + u^2v^2(vs + s')x' + (v^3t + v^2s'r + t') & \\ & = & u^3v^3y' + u^2v^2(vs + s')x' + (v^3t - v^3sr + t') & = y' \end{array}$$

1.34. Thus if we apply the admissible change of coordinate (1.11) to

$$f(x, y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right)$$

we obtain

$$f(u^2x' + r, u^3y' + su^2x' + t)u^{-6} = y'^2 + a_1'x'y' + a_3'y' - \left(x'^3 + a_2'x'^2 + a_4'x' + a_6'\right)$$

where the values a_i' are defined as in Fig. 1.2

1.35. If we assume $\mathrm{char}(\mathbb{F}) \neq 2, 3$, and we apply (1.11) to an elliptic curve expressed as

$$f(x, y) = y^2 - \left(x^3 + Ax + B\right)$$

using (1.5) we obtain

$$u^6y'^2 + 2u^5sx'y' + 2u^3ty' - u^6x'^3 - u^4(3r - s^2)x'^2 - u^2(A + 3r^2 - 2st)x' - (Ar + B + r^3 - t^2);$$

thus the most general allowable change of coordinates Φ which grants that also $\Phi(f)$ is expressed via (1.5) must satisfie

$$0 = s = t = 3r - s^2 \text{ whenee } r = s = t = 0$$

and has the shape

$$x = u^2x', \quad y = u^3y', \tag{1.13}$$

so that

$$\Phi(f(x, y)) = u^6y'^2 - u^6x'^3 - u^2Ax' - B. \tag{1.14}$$

Figure 1.2:

$$\begin{array}{lcl} a'_1 & := & \frac{a_1+2s}{u} \\ a'_2 & := & \frac{a_2-a_1s+3r-s^2}{u^2} \\ a'_3 & := & \frac{a_3+a_1r+2t}{u^3} \\ a'_4 & := & \frac{a_4-sa_3+2a_2r-a_1(rs+t)+3r^2-2st}{u^4} \\ a'_6 & := & \frac{a_6-a_1rt+a_2r^2-a_3t+a_4r+r^3-t^2}{u^6} \end{array}$$

1.11 Invariant (1)

1.36. Thus if we apply the admissible change of coordinate (1.11) to

$$f(x,y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right)$$

we obtain the relations

$$\begin{array}{rcllcl} ua'_1 & = & a_1 + 2s, & & & \\ u^2a'_2 & = & a_2 - a_1s + 3r - s^2, & & & \\ u^3a'_3 & = & a_3 + a_1r + 2t & & = & \frac{\partial f}{\partial y}(r,t) \\ u^4a'_4 & = & a_4 - sa_3 + 2a_2r - a_1(rs+t) + 3r^2 - 2st & & = & -\frac{\partial f}{\partial x}(r,t) - s\frac{\partial f}{\partial x}(r,t) \\ u^6a'_6 & = & a_6 - a_1rt + a_2r^2 - a_3t + a_4r + r^3 - t^2 & & = & f(r,t) \end{array}$$

1.37. If we reformulate

$$f'(x',y') = {y'}^2 + a'_1x'y' + a'_3y' - \left(x'^3 + a'_2x'^2 + a'_4x' + a'_6\right)$$

as

$$f'(x',y') = {y'}^2 - \left(x'^3 + b'_2x'^2 + b'_4x' + b'_6\right)$$

we obtain

$$u^2b'_2 = (ua'_1)^2 + 4u^2a'_2 = a_1^2 + 4sa_1 + 4s^2 + 4a_2 - 4a_1s + 12r - 4s^2 = a_1^2 + 4a_2 + 12r = b_2 + 12r$$

and, with a similar computation

$$\begin{array}{rcl} u^4b'_4 & = & b_4 + rb_2 + 6r^2, \\ u^6b'_6 & = & b_6 + 2rb_4 + r^2b_2 + 4r^3, \\ u^8b'_8 & = & b_8 + 3rb_6 + 3r^2b_4 + r^3b_6 + 3r^4. \end{array}$$

1.38. If we further reformulate $f'(x',y')$ as

$$f'(x',y') = {y'}^2 - \left(x'^3 + c'_4x' + c'_6\right)$$

we have

$$u^4c'_4 = (u'^2b'_2)^2 - 24u^4b'_4 = b_2^2 + 24rb_2 + 144r^2 - 24b_4 - 24rb_2 - 144r^2 = b_2^2 - 24b_4 = c'_4$$

and

$$\begin{array}{rcl} u^6c'_6 & = & -(u'^2b'_2)^3 + 36(u^2b'_2)(u^4b'_4) - 216u^6b'_6 \\ & = & -b_2^3 - 36rb_2^2 - 432r^2b_2 + 1728r^3 \\ & + & 36b_2b_4 + 432b_4r + 36b_2^2r + 648b_2r^2 + 2592r^3 \\ & - & 216b_6 - 432rb_4 - 216r^2b_2 - 864r^3 \\ & = & -b_2^3 + 36b_2b_4 - 216b_6 \\ & = & c_6 \end{array}$$

1.39. A more involved computation gives

$$\begin{array}{rcl} u^{12}\Delta' & = & -(u^2b_2)^2(u^8b_8) - 8(u^4b_4^3) - 27(u^6b_6)^2 + 9(u^2b_2)(u^4b_4)(u^6b_6) \\ & = & \left(36r^2 + 6b_2r\right)\left(b_2b_6 - b_4^2 - 4b_8\right) - b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ & = & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ & = & \Delta \end{array}$$

Figure 1.3:

$$\begin{array}{rcll}
ua'_1 & = & a_1 + 2s, & \\
u^2a'_2 & = & a_2 - a_1s + 3r - s^2, & \\
u^3a'_3 & = & a_3 + a_1r + 2t & = \frac{\partial f}{\partial y}(r,t) \\
u^4a'_4 & = & a_4 - sa_3 + 2a_2r - a_1(rs+t) + 3r^2 - 2st & = -\frac{\partial f}{\partial x}(r,t) - s\frac{\partial f}{\partial x}(r,t) \\
u^6a'_6 & = & a_6 - a_1rt + a_2r^2 - a_3t + a_4r + r^3 - t^2 & = f(r,t) \\
 & & & \\
u^2b'_2 & = & b_2 + 12r & \\
u^4b'_4 & = & b_4 + rb_2 + 6r^2, & \\
u^6b'_6 & = & b_6 + 2rb_4 + r^2b_2 + 4r^3, & \\
u^8b'_8 & = & b_8 + 3rb_6 + 3r^2b_4 + r^3b_6 + 3r^4. & \\
 & & & \\
u^4c'_4 & = & c_4 & \\
u^6c'_6 & = & c_6 & \\
u^{12}\Delta' & = & \Delta & \\
j' & = & j &
\end{array}$$

1.40. As a consequence

$$j' := \frac{{c'_4}^3}{\Delta'} = \frac{(u^4c_4)^3}{u^{12}\Delta} = \frac{{c_4}^3}{\Delta} = j.$$

Definition 1.41. The j-invariant of the non-singular elliptoc curve (1.1) is the value $j := \frac{c_4^3}{\Delta}$.

Lemma 1.42. *Two isomrphic non-singular elliptic curves have the same invariant*

1.12 Invaraint (2)

1.43. Assuming char($\mathbb{F}$) $\neq 2,3$ and let us consider a non singular curve $f(x,y) = y^2 - x^3 - Ax - B$ expressed using (1.5); we have

$$j = \frac{{c_4}^3}{\Delta} = \frac{(-48A)^3}{\Delta} = \frac{-(2^43A)^3}{\Delta} = \frac{-2^{12}3^3A^3}{\Delta} = \frac{-2^63^32^2A^3}{\Delta} = \frac{-12^34A^3}{\Delta} = -1728\frac{4A^3}{\Delta}.$$

1.44. Let us now consider two non singular curves

$$f(x,y) = y^2 - x^3 - Ax - B \text{ and } f'(x',y') = y'^2 - x'^3 - A'x' - B'$$

expressed using (1.5).

If they are isomorphic via the transformation (1.13) we have

$$\begin{aligned}
\Phi(f) &= u^6y'^2 - u'^6x'^3 - u^2Ax' - B \\
&= u^6\left(y'^2 - x'^3 - \frac{A}{u^4}x' - \frac{B}{u^6}\right) \\
&= u^6\left(y'^2 - x'^3 - A'x' - B'\right)
\end{aligned}$$

whence

$$u^4A' = A \text{ and } u^6B' = B.$$

Moreover

$$\Delta = -16\left(4A^3 - 27B^3\right) = -16u^{12}\left(4A'^3 - 27B'^3\right) = u^{12}\Delta'$$

and

$$j = -1728\frac{(4A)^3}{\Delta} = -1728\frac{(4u^4A')^3}{u^{12}\Delta'} = -1728\frac{4A'^3}{\Delta'} = j$$

as we already know.

Lemma 1.45. *For two curves f, f' we have*

$$j = j' \iff A^3B'^2 = A'^3B^2$$

Proof. Using

$$\Delta = -16\left(4A^3 - 27B^3\right) \text{ and } j = -1728\frac{(4A)^3}{\Delta}$$

we have

$$\frac{(4A)^3}{4A^3-27B^3} = -16\frac{(4A)^3}{\Delta} = \frac{16}{1728}j = \frac{16}{1728}j' = \frac{(4A')^3}{4A'^3-27B'^3} \iff j = j';$$

moreover we have also the trivial equivalences

$$\left(4A'^3 - 27B'^3\right)\cdot(4A)^3 = \left(4A^3 - 27B^3\right)\cdot(4A')^3 \iff \frac{(4A)^3}{4A^3-27B^3} = \frac{(4A')^3}{4A'^3-27B'^3}$$

and

$$4^4A^3A'^3 + 1728A^3B'^2 = \left(4A'^3 - 27B'^3\right)\cdot(4A)^3 = \left(4A^3 - 27B^2\right)\cdot(4A')^3 = 4^4A^3A'^3 + 1728A'^3B'^2 \iff A^3B'^2 = A^3B'^2.$$

□

1.46. Consider the two non singular curves

$$f(x,y) = y^2 - x^3 - Ax - B \text{ and } f'(x',y') = y'^2 - x'^3 - A'x' - B'$$

we intend to classify all transformations

$$x = u^2x', y = u^3y' : f'(x',y') = f(u^2x', u^3y')$$

under the assumption that $j = j'$.

Under this assumptions we have

- $u^4A' = A$ and $u^6B' = B$ from $f'(x',y') = f(u^2x', u^3y')$;
- $A^3B'^2 = A'^3B^2$ (Lemma 1.45)
- $4A^3 - 27B^3 = -\frac{1}{16}\Delta \neq 0$ (since f is non singular)
- $4A'^3 - 27B'^3 = -\frac{1}{16}\Delta' \neq 0$ (since f' is non singular)

Moreover, we intend to describe the group structure of the automorphisms of the curve f, *id est* under the further assumptions

- $A = A', B = B'$.

To do so, we need to consider three cases

(1) If $\boxed{B=0}$, we can further deduce, from $\Delta \neq 0$, $\boxed{A \neq 0}$, whence, from $A^3B'^2 = A'^3B^2 = 0$, $\boxed{B'=0}$ and, from $\Delta' \neq 0$, $\boxed{A' \neq 0}$; this case is studied in 1.47

(2) If $\boxed{A=0}$, we can further deduce, from $\Delta \neq 0$, $\boxed{B \neq 0}$, whence, from $0 = A^3B'^2 = A'^3B^2$, $\boxed{A'=0}$ and, from $\Delta' \neq 0$, $\boxed{B' \neq 0}$; this case is studied in 1.48

(3) If $\boxed{AB \neq 0}$, from $A^3B'^2 = A'^3B^2$ we deduce that $A' = 0 \iff B' = 0$ and,since $\Delta' \neq 0$ this implies $\boxed{A'B' \neq 0}$; this case is studied in 1.49

1.47. Since $A \neq 0 \neq A'$ we can set $u = \sqrt[4]{\frac{A}{A'}}$ and we obtain the transfiormation

$$\begin{aligned} y^2 - x^3 - Ax &= f(x,y) = f(u^2x', u^3y') \\ &= u^6y'^2 - u^6x'^3 - Au^2x' \\ &= u^6\left(y'^2 - x'^3 - \frac{A}{u^4}x'\right) \\ &= u^6\left(y'^2 - x'^3 - A'x'\right) = u^6f'(x',y') \end{aligned}$$

Note that we have

$$c_6 = -864B = 0, c_4 = -48A \neq 0, 1728\Delta = c_4^3 - c_6^2 = c_4^3, \boxed{j = \frac{c_4^3}{\Delta} = 1728}.$$

1.48. Since $B \neq 0 \neq B'$ we can set $u = \sqrt[6]{\frac{B}{B'}}$ and we obtain the transfiormation

$$\begin{aligned} y^2 - x^3 - B &= f(x,y) = f(u^2x', u^3y') \\ &= u^6y'^2 - u^6x'^3 - B \\ &= u^6\left(y'^2 - x'^3 - \frac{B}{u^6}\right) \\ &= u^6\left(y'^2 - x'^3 - B'\right) = u^6 f'(x', y') \end{aligned}$$

Note that we have

$$c_6 = -864B \neq 0, c_4 = -48A = 0, 1728\Delta = c_4^3 - c_6^2 = -c_6^3, \boxed{j = \frac{c_4^3}{\Delta} = 0}.$$

1.49. Since both $A \neq 0 \neq A'$ and $B \neq 0 \neq B'$ and $A^3B'^2 = A'^3B^2$ we have $\left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2$ so that

$$\sqrt[6]{(\frac{B}{B'})} = \sqrt[4]{(\frac{A}{A'})} =: u$$

satisfies $u^{12} = \left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2$

We thus obtain the transfiormation

$$\begin{aligned} y^2 - x^3 - Ax - B &= f(x,y) = f(u^2x', u^3y') \\ &= u^6y'^2 - u^6x'^3 - Au^2x' - B \\ &= u^6\left(y'^2 - x'^3 - \frac{A}{u^4}x' - \frac{B}{u^6}\right) \\ &= u^6\left(y'^2 - x'^3 - A'x' - B'\right) = u^6 f'(x', y') \end{aligned}$$

Note that $c_4 = -48A \neq 0$ and $\boxed{j = -1728\frac{(4A)^3}{\Delta} \neq 0}$.

Moreover

$$j = 1728 \implies c_4^3 - c_6^2 = 1728\Delta = j\Delta = c_4^3 \iff c_6^2 = 0 \iff c_6 = 0$$

and conversely $c_6 = 0 \implies j = \frac{c_4^3}{\Delta} = \frac{c_4^3 - c_6^2}{\Delta} = 1728$; thus

Thus we have $c_6 = -864B \neq 0$ whence $\boxed{j \neq 1728}$.

1.50. If, moreover $f = f'$, *id est* $A = A', B = B'$ we have

$\underline{B = 0}$: $A = A' \implies u^4 = \frac{A}{A'} = 1$ and the automorphism groop is isomorphic to that of the 4^{th} root of the unity, namely $\mathbb{Z}_4$.

$\underline{A = 0}$: $B = B' \implies u^6 = \frac{B}{B'} = 1$ and the automorphism groop is isomorphic to that of the 6^{th} root of the unity, namely $\mathbb{Z}_6$.

$\underline{AB \neq 0}$: Since we have both $A = A' \implies u^4 = \frac{A}{A'} = 1$ and $B = B' \implies u^6 = \frac{B}{B'} = 1$ we obtain $u^2 = 1$, $u = \{\pm 1\}$ and the automorphism groop is isomorphic to that of the 2^{th} root of the unity, namely $\mathbb{Z}_2$.

1.13 Invaraint (3)

1.14 Arithmetics of the points of an elliptic curve (2)

1.15 Elliptic curve in characteristic 2

1.51. Let us consider a non singular elliptic curve

$$f(x,y) = y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6 = 0$$

in a field $\mathbb{F}$, $\operatorname{char}\mathbb{F} = 2$.

We thus have

$$b_2 = a_1^2, b_4 = a_1a_3, b_6 = a_3^2, c_4 = b_2^2 = a_1^4, c_6 = a_1^6,$$

and $j = \frac{a_1^{12}}{\Delta}$.

Thus there two diffierent cases; either

- $a_1 = 0 \iff j = 0$ or
- $a_1 \neq 0 \iff j \neq 0$

1.16 Elliptic curve in characteristic 2: $j = 0$

1.52. Since $j = 0$ we have
$$b_2 = b_4 = c_1 = c_2 = 0 \text{ and } b_6 = a_3^2,$$
so that $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = b_6^2 = a_3^4$.

Moreover

$$\begin{aligned} f(x+a_2, y) &= y^2 + a_3 y + (x^3 + a_2 x^2 + a_2^2 x + a_2^3) + a_2(x^2 + a_2^2) + a_4(x + a_2) + a_6 \\ &= y^2 + a_3 y + x^3 + (a_4 + a_2^2)x + (a_6 + a_2 a_4 + a_2^3) \end{aligned}$$

As a consequence

Lemma 1.53. *If $a_1 = 0$, then*

(1) $\Delta = 0 \iff a_3 = 0$*;*

(2) *we can wlog assume $a_2 = 0$.*

Lemma 1.54. *Let $\beta, \gamma \in \overline{\mathbb{F}}$ such that $\beta^2 = a_4, \gamma^2 = a_6$.*

If $a_1 = 0$, (β, γ) is a singular point if and only if $a_3 = 0$.

Proof. We have

(1) $\frac{\partial f}{\partial x} = x^2 + a_4$,

(2) $\frac{\partial f}{\partial y} = a_1 x + a_3 = a_3$,

(3) $f(x, y) = y^2 + a_3 y + (x^2 + a_4)x + a_6$.

so that, if there is a singular point (x_0, y_0) then

(2) $a_3 = \frac{\partial f}{\partial y}(x_0, y_0) = 0$,

(1) $0 = \frac{\partial f}{\partial x}(x_0, y_0) = x_0^2 + a_4$ so that $x_0 = \beta$,

(3) $0 = f(x_0, y_0) = y_0^2 + a_6$ so that $y_0 = \gamma$;

conversily, if $a_3 = 0$, then

(1) $\frac{\partial f}{\partial x}(\beta, \gamma) = \beta^2 + a_4 = 0$,

(2) $\frac{\partial f}{\partial x}(\beta, \gamma) = a_3 = 0$,

(3) $f(\beta, \gamma) = \gamma^2 + a_3\gamma + (\beta^2 + a_4)\beta + a_6 = \gamma^2 + a_6 = 0$.

□

Corollary 1.55. *If $\mathrm{char}(\mathbb{F}) = 2$ and $a_1 = 0$, an elliptic curve given by a Weierstress equation (1.1) is singular if and only if $\Delta = 0$.*

1.56. The admissible isomorphisms (1.11) between

$$f(x, y) = y^2 + a_3 y + x^3 + a_4 x + a_6 \text{ and } f'(x', y') = y'^2 + a_3' y' + x'^3 + a_2' x^2 + a_6,$$

since

$$\begin{aligned} 0 = a_2' &:= \tfrac{a_2 - a_1 s + 3r - s^2}{u^2} & \Longrightarrow\quad r &= s^2 \\ a_3' &:= \tfrac{a_3 + a_1 r + 2t}{u^3} & \Longrightarrow\quad u^3 &= \tfrac{a_3}{a_3'} \\ a_4' &:= \tfrac{a_4 - s a_3 + 2a_2 r - a_1(rs+t) + 3r^2 - 2st}{u^4} & \Longrightarrow\quad a_4' &= \tfrac{a_4 + s a_3 + s^4}{u^4} \\ a_6' &:= \tfrac{a_6 - a_1 rt + a_2 r^2 - a_3 t + a_4 r + r^3 - t^2}{u^6} & \Longrightarrow\quad a_6' &= \tfrac{a_6 + a_3 t + a_4 s^2 + s^6 + t^2}{u^6}, \end{aligned}$$

are

$$x = u^2 x' + s^2, \quad y = u^3 y' + u^2 s x' + t$$

and must satisfy

$$u^3 = \frac{a_3}{a_3'}, \quad s^4 + a_3 s + a_4 - u^4 a_4' = 0, \quad t^2 + a_3 t + s^6 + a_4 s^2 + a_6 - u^6 a_6' = 0$$

Corollary 1.57. *Denote*

- $g_1(x) := x^3 + \frac{a_3}{a_3'} \in \mathbb{F}[x]$,
- $\mathbb{K}_1 := \mathbb{F}[x]/g_1(x)$ *which is a separable extension since* $g_1'(x) \neq 0$,
- $u \in \mathbb{K}_1$ *s.t.* $g_1(u) = 0$;
- $g_2(x,y) := y^4 + a_3 y + a_4 - x^4 a_4' \in \mathbb{F}[x,y]$,
- $h_2(y) := g_2(u,y) = y^4 + a_3 y + a_4 - u^4 a_4' \in \mathbb{K}_1[y]$,
- $\mathbb{K}_2 := \mathbb{K}_1[y]/h_2(y) = \mathbb{F}[x,y]/\mathbb{I}(g_1(x), g_2(x,y))$ *which is a separable extension since* $h_2'(y) = a_3 \neq 0$;
- $s \in \mathbb{K}_2$ *s.t.* $h_2(s) = 0$;
- $g_3(x,y,z) := z^2 + a_3 z + y^6 + a_4 y^2 + a_6 - x^6 a_6' \in \mathbb{F}[x,y,z]$,
- $h_3(x,y,z) := g_2(u,s,z) = z^2 + a_3 z + s^6 + a_4 s^2 + a_6 - u^6 a_6' \in \mathbb{K}_2[z]$,
- $\mathbb{K}_3 := \mathbb{K}_2[y]/h_3(y) = \mathbb{F}[x,y,y]/\mathbb{I}(g_1(x), g_2(x,y) g_3(x,y,z))$ *which is a separable extension since* $h_3'(z) = a_3 \neq 0$;
- $t \in \mathbb{K}_3$ *s.t.* $h_3(t) = 0$.

Then the two curves f, f' *with the same invariant* $j = 0$ *are isomorphic via*

$$x = u^2 x' + s^2, \quad y = u^3 y' + u^2 s x' + t$$

Corollary 1.58. *The 24 automorphisms of* $f(x,y) = y^2 + a_3 y + x^3 + a_4 x + a_6$ *are given by the triple* (u,s,t) *satisfying the equations*

$$u^3 = 1, \quad s^4 + a_3 s + a_4(1-u) = 0, \quad t^2 + a_3 t + s^6 + a_4 s^2 + a_6(1-u) = 0.$$

Lemma 1.59. *The curve*

$$f(x,y) = y^2 - y - x^3$$

has 0 *as invariant.*

1.17 Elliptic curve in characteristic 2: $j \neq 0$

1.60. It is sufficient to properly choose r, s, t in (1.11) in order to obtain $a_1' = 1, a_3' = 0, a_4' = 0$. In fact (see Fig.1.2)

$$\begin{array}{rcl|ccccc}
1 = a_1' & = & \frac{a_1}{u} & \iff & u & = & a_1 \\
0 = a_3' & := & \frac{a_3 + a_1 r}{u^3} & \iff & r & = & \frac{a_3}{a_1} \\
0 = a_4' & := & \frac{a_4 - s a_3 + 2 a_2 r - a_1(rs+t) + 3r^2 - 2st}{u^4} & & & & \\
 & = & \frac{a_4 - s(a_3 + a_1 r) - a_1 t + r^2}{u^4} & & & & \\
 & = & \frac{a_4 - a_1 t + r^2}{u^4} & \iff & t & = & \frac{a_4 + r^2}{a_1} = \frac{a_1^2 a_4 + a_3^2}{a_1^3}
\end{array}$$

1.61. For

$$f(x,y) = y^2 + xy + x^3 + a_2 x^2 + a_6 = 0$$

we have

$$b_2 = 1, b_4 = b_6 = 0, c_4 = c_6 = 1 \text{ and } b_8 = a_6,$$

so that $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = a_6$ and $j = a_6^{-1}$.

Lemma 1.62. *If* $a_1 \neq 0$, $(0,0)$ *is a singular point if and only if* $a_6 = 0$.

Proof. We have

(1) $\frac{\partial f}{\partial x} = y + x^2$,

(2) $\frac{\partial f}{\partial y} = x$,

(3) $f(x,y) = y^2 + xy + x^3 + a_2 x^2 + a_6$.

so that, if there is a singular point (x_0, y_0) then

(2) $x_0 = \frac{\partial f}{\partial y}(x_0, y_0) = 0$,

(1) $0 = \frac{\partial f}{\partial x}(0, y_0) = y_0$,

(3) $0 = f(0,0) = a_6$;

conversily, if $a_6 = 0$, then

(1) $\frac{\partial f}{\partial x}(0,0) = 0$,

(2) $\frac{\partial f}{\partial x}(0,0) = 0$,

(3) $f(0,0) = a_6 = 0$.

□

Corollary 1.63. *If* $\mathrm{char}(\mathbb{F}) = 2$ *and* $a_1 \neq 0$*, an elliptic curve given by a Weierstress equation (1.1) is singular if and only if* $\Delta = 0$.

1.64. The admissible isomorphisms (1.11) between

$$f(x,y) = y^2 + xy + x^3 + a_2x^2 + a_6 \text{ and } f'(x',y') = y'^2 + x'y' + x'^3 + a_2'x^2 + a_6,$$

since

$$\begin{array}{rcllrcl}
1 = a_1' & = & \frac{a_1}{u} & \Longrightarrow & u & = & 1 \\
0 = a_3' & := & \frac{a_3 + a_1 r + 2t}{u^3} & \Longrightarrow & r & = & 0 \\
0 = a_4' & := & \frac{a_4 - s(a_3 + a_1 r) - a_1 t + r^2}{u^4} & \Longrightarrow & t & = & 0 \\
a_6' & := & \frac{a_6 - a_1 rt + a_2 r^2 - a_3 t + a_4 r + r^3 - t^2}{u^6} & \Longrightarrow & a_6' & = & a_6 \\
a_2' & := & \frac{a_2 - a_1 s + 3r - s^2}{u^2} & \Longrightarrow & a_2' & = & a_2 - s - s^2,
\end{array}$$

are

$$x = x', \quad y = y' + sx'$$

and must satisfy

$$a_2' = a_2 - s - s^2 \text{ and } a_6' = a_6.$$

Corollary 1.65. *Denote* $g(x) := x^2 + x + a_2 + a_2' \in \mathbb{F}[x]$ *and* $\mathbb{K} := \mathbb{F}[x]/g(x)$ *which is a separable extension since* $g'(x) = 1$ *and let* $s \in \mathbb{K}$ *be s.t.* $g(s) = 0$.

Then the two curves f, f' *with the same invariant* $j = a_6^{-1} = a_6'^{-1}$ *are isomorphic via*

$$x = x', \quad y = y' + sx'$$

Corollary 1.66. *The two automorphisms of* $f(x,y) = y^2 + xy + x^3 + a_2x^2 + a_6$ *are obtained setting* $s = 0, 1$*, namely*

$$x = x', y = y' \text{ and } x = x'y = y' + x'$$

Lemma 1.67. *For each* $j \in \mathbb{F}, j \neq 0$*, the curve*

$$f(x,y) = y^2 + xy + x^3 + j^{-1}$$

has j *as invariant.*

1.68. For

$$f(x,y) = y^2 + xy + x^3 + a_2x^2 + a_6 = 0$$

we have $x\frac{\partial y}{\partial x} + y = x^2$ so that for $P = (x,y)$ the point $(x_3, y_3) := P + P$ satisfies

$$
\begin{aligned}
x_3 &= \left(\frac{\partial y}{\partial x}\right)^2 + a_1\frac{\partial y}{\partial x} - a_2 - 2x \\
&= \left(\frac{x^2+y}{x}\right)^2 + \frac{x^2+y}{x} + a_2 \\
&= (\frac{x^4+y^2}{x^2} + \frac{x^2+y}{x} + a_2 \\
&= (\frac{x^4+xy+x^3+a_2x^2+a_6}{x^2} + \frac{x^2+y}{x} + a_2 \\
&= (\frac{x^4+xy+x^3+a_2x^2+a_6+x(x^2+y)+a_2x^2}{x^2} \\
&= (\frac{x^4+a_6}{x^2} \\
y^3 &= -\left(\frac{\partial y}{\partial x} + a_1\right)x_3 - \frac{\partial y}{\partial x}x - y - a_3 \\
&= \frac{\partial y}{\partial x}x_3 + \frac{\partial y}{\partial x}x + x_3 + y \\
&= \frac{x^2+y}{x}x_3 + x^2 + y + x_3 + y \\
&= \frac{x^2+y}{x}x_3 + x^2 + x_3 +
\end{aligned}
$$

1.18 Elliptic curve in characteristic 3

1.69. Let us consider a non singular elliptic curve

$$f(x,y) = y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6 = 0$$

in a field $\mathbb{F}$, $\operatorname{char}\mathbb{F} = 3$.

Since $2 = -1$ and $4 = 1$ in $\mathbb{F}$ we can perform the transformation $y \to y + a_1y + a_3$ and express the curve via the equation (1.2)

$$y^2 = x^3 + b_2x^2 - b_4x + b_6,$$

with

$$b_2 = a_2, b_4 = -a_4, b_6 = a_6, b_8 = a_2a_6 - a_4^2; c_4 = b_2^2 = a_2^2, c_6 = -b_2^3 = -a_2^3$$

so that

$$\Delta = -b_2^2b_8 - b_4^3 = a_2^2a_4^2 - a_2^3a_6 - a_4^3$$

and $j = \frac{a_2^6}{\Delta}$.

Thus there are two diffierent cases; either

- $a_2 = 0 \iff j = 0$ or
- $a_2 \neq 0 \iff j \neq 0$

1.19 Elliptic curve in characteristic 3: $j \neq 0$

1.70. For $f(x,y) = y^2 - x^3 - b_2x^2 + b_4x - b_6$ we have

$$
\begin{aligned}
f(x+\alpha, y) &= y^2 - (x+\alpha)^3 - b_2(x+\alpha)^2 + b_4(x+\alpha) - b_6 \\
&= y^2 - (x^3+\alpha^3) - b_2(x^2 - \alpha x + \alpha^2) + b_4(x+\alpha) - b_6 \\
&= y^2 - x^3 - b_2x^2 + (b_2\alpha + b_4)x - (\alpha^3 + b_2\alpha^2 - b_4\alpha + b_6)
\end{aligned}
$$

and it is sufficient to set

$$\alpha := -\frac{b_4}{b_2}, \text{ and } a_6 := \alpha^3 + b_2\alpha^2 - b_4\alpha + b_6$$

in order to present the curve as

$$f'(x,y) = y^2 - x^3 - a_2x^2 - a_6$$

with $c_4 = a_2^2, \Delta = -a_2^3a_6$ and $j = \frac{a_2^6}{-a_2^3a_6} = -\frac{a_2^3}{a_6}$.

1.71. The admissible isomorphism between

$$f(x,y)=y^2-x^3-a_2x^2-a_6 \text{ and } f'(x',y')=y'^2-x'^3-a_2'x'^2-a_6'$$

since

$$\begin{array}{rcl}0=a_1' & = & \frac{a_1+2s}{u} & \Longrightarrow & s & = & 0\\ 0=a_3' & := & \frac{a_3+a_1r+2t}{u^3} & \Longrightarrow & t & = & 0\\ 0=a_4' & := & \frac{a_4-sa_3+2a_2r-a_1(rs+t)+3r^2-2st}{u^4} & \Longrightarrow & r & = & 0\\ a_2' & := & \frac{a_2-a_1s+3r-s^2}{u^2} & \Longrightarrow & a_2' & = & \frac{a_2}{u^2}\\ a_6' & := & \frac{a_6-a_1rt+a_2r^2-a_3t+a_4r+r^3-t^2}{u^6} & \Longrightarrow & a_6' & = & \frac{a_6}{u^2}\end{array}$$

are

$$x=u^2x',\quad y=u^3y''$$

and must satisfy

$$u^2a_2'=a_2 \text{ and } u^6a_6'=a_6.$$

1.72. If the two curves f,f' have the same invariant $j=-\frac{a_2^3}{a_6}=-\frac{a_2'^3}{a_6'}$ then $\frac{a_6'}{a_6}=\left(\frac{a_2}{a_2'}\right)^3$.

Corollary 1.73. *The two curves f,f' with the same invariant $j=-\frac{a_2^3}{a_6}=-\frac{a_2'^3}{a_6'}$ are isomorphic via*

$$x=u^2x',\quad y=u^3y'$$

where $u^2=\left(\frac{a_2}{a_2'}\right)$.

Corollary 1.74. *The two automorphisms of $f(x,y)=y^2+xy+x^3+a_2x^2+a_6$ are obtained setting $u=\pm1$, namely*

$$x=x',y=y' \text{ and } x=x',y=-y''$$

Lemma 1.75. *For each $j\in\mathbb{F},j\neq 0$, the curve*

$$f(x,y)=y^2-x^3-x^2-j^{-1}$$

has j as invariant.

1.20 Elliptic curve in characteristic 3: $j=0$

1.76. Since $a_2=0$ we have

$$b_2=0,b_4=-a_4,b_6=a_6,b_8=-a_4^2;c_4=c_6=0$$

so that $\Delta=b_4^3=-a_4^3$.

1.77. The admissible isomorphism between

$$f(x,y)=y^2+x^3+a_4x+a_6 \text{ and } f'(x',y')=y'^2+x'^3+a_4'x^2+a_6$$

since

$$\begin{array}{rcl}0=a_2' & := & \frac{a_2-a_1s+3r-s^2}{u^2} & \Longrightarrow & s & = & 0\\ 0=a_3' & := & \frac{a_3+a_1r+2t}{u^3} & \Longrightarrow & t & = & 0\\ a_4' & := & \frac{a_4-sa_3+2a_2r-a_1(rs+t)+3r^2-2st}{u^4} & \Longrightarrow & a_4' & = & \frac{a_4}{u^4}\\ a_6' & := & \frac{a_6-a_1rt+a_2r^2-a_3t+a_4r+r^3-t^2}{u^6} & \Longrightarrow & a_6' & = & \frac{a_6+a_4r+r^3}{u^6}\end{array}$$

are

$$x=u^2x'+r,\quad y=u^3y'$$

and must satisfy

$$u^4=\frac{a_4}{a_4'},\quad u^6a_6'=a_6+a_4r+r^3.$$

Corollary 1.78. *Denote*

- $g_1(x):=x^4+\frac{a_4}{a_4'}\in\mathbb{F}[x]$,
- $\mathbb{K}_1:=\mathbb{F}[x]/g_1(x)$ *which is a separable extension since* $g_1'(x)=1$,
- $u\in\mathbb{K}_1$ *s.t.* $g_1(u)=0$;

- $g_2(x,y) := y^3 + a_4 y + a_6 - x^6 a_6' \in \mathbb{F}[x,y]$,
- $h_2(y) := g_2(u,y) = y^3 + a_4 y + a_6 - x^6 a_6' \in \mathbb{K}_1[y]$,
- $\mathbb{K}_2 := \mathbb{K}_1[y]/h_2(y) = \mathbb{F}[x,y]/\mathbb{I}(g_1(x), g_2(x,y))$ *which is a separable extension since* $h_2'(y) = a_4 \neq 0$;
- $r \in \mathbb{K}_2$ *s.t.* $h_2(r) = 0$;

Then the two curves f, f' *with the same invariant* $j = 0$ *are isomorphic via*

$$x = u^2 x' + r, \quad y = u^3 y'.$$

Corollary 1.79. *The 12 automorphisms of* $f(x,y) = y^2 + x^3 + a_4 x + a_6$ *are given by the pairs* (u,r) *satisfying the equations*

$$u^4 = 1, \quad r^3 + a_4 r + a_6(1 - u^2) = 0.$$

More precisely they are the 12 pairs (u,r) *such that either*

$r^3 + a_4 r = 0$ *and* $u = 1$, *or*

$r^3 + a_4 r = 0$ *and* $u = -1$, *or*

$r^3 + a_4 r + 2a_6 = 0$ *and* $u = \alpha$, *or*

$r^3 + a_4 r + 2a_6$ *and* $u = -\alpha$,

where $\alpha \in \mathbb{F}_{\mathrm{sep}}$ *is such that* $\alpha^2 = -1$.

Lemma 1.80. *The curve*

$$f(x,y) = y^2 - x^3$$

has 0 *as invariant.*