5
Pontos Galoisianos em Curvas Algébricas de gênero três em característica dois

Neste capítulo estudaremos em que casos os pontos de uma curva algébrica não singular, completa, não hiperelíptica de gênero três, sobre um corpo algebricamente fechado de característica dois, são pontos de Galois. Um ponto Q de uma curva de gênero três pode ser um ponto genérico com seqüência de lacunas 1,2,3 e $d_Q = 4$, ou, um ponto de Weierstrass com seqüência de lacunas 1,2,4 para pontos de inflexão ou 1,2,5 para pontos de bitangência e em ambos casos temos $d_Q = 3$.

5.1
O ponto infinito como um ponto de Galois

Nesta seção daremos condições para que o ponto $Q = P_\infty$ seja um ponto Galoisiano, com $d_Q = 3$. Para efeitos de cálculo do grupo de Galois de extensões cúbicas utilizaremos uma versão do teorema de Cardano para corpos de característica dois.

Teorema(Cardano) 5.1 *Seja K corpo de característica dois, e seja a equação cúbica irredutível*

$$Y^3 + \alpha Y^2 + \beta Y + \gamma = 0,$$

com $\alpha, \beta, \gamma \in K$. Esta equação tem grupo de Galois A_3 se

$$\frac{(\beta + \alpha^2)^3}{(\beta\alpha + \gamma)^2} \in \mathcal{P}(K),$$

onde $\mathcal{P}$ é o operador de Artin-Schreier $\mathcal{P} : a \longmapsto a^2 + a$. Caso contrário, o grupo é S_3.

Demonstração: Considere a transformação $Y_1 = Y + \alpha$. A equação resultante é

$$Y_1^3 + (\beta + \alpha^2)Y_1 + (\beta\alpha + \gamma) = 0.$$

Fazendo a transformação $Y_1 = Y_2 + Y_3$ e substituindo na equação acima obtemos

$$[Y_2^3 + Y_3^3 + (\beta\alpha + \gamma)] + (Y_2 + Y_3)[(\beta + \alpha^2) + Y_2Y_3] = 0.$$

Escolhamos Y_2 e Y_3 de forma que $Y_2Y_3 + (\beta + \alpha^2) = 0$ e a equação se reduz a

$$Y_3^6 + (\beta\alpha + \gamma)Y_3^3 + (\beta + \alpha^2)^3 = 0.$$

Utilizando a transformação não linear $Y_4 = Y_3^3$, temos

$$Y_4^2 + (\beta\alpha + \gamma)Y_4 + (\beta + \alpha^2)^3 = 0.$$

Como o polinômio é irredutível temos que $\beta\alpha+\gamma \neq 0$, logo podemos utilizar a transformação,

$$Y_5 = \frac{Y_4}{\beta\alpha + \gamma},$$

para ter finalmente

$$Y_5^2 + Y_5 + \frac{(\beta + \alpha^2)^3}{(\beta\alpha + \gamma)^2} = 0,$$

a equação clássica de Artin-Schreier. Esta equação tem grupo de Galois A_3 se

$$\frac{(\beta + \alpha^2)^3}{(\beta\alpha + \gamma)^2} \in \mathcal{P}(K).$$

Caso contrário o grupo é S_3. □

Uma curva não singular, completa, não hiperelítica de gênero três sobre um corpo de característica dois e ponto de Weierstrass $Q = P_\infty$ com seqüência de ordens 0,1,4 é isomorfa à curva dada pela equação

$$y^3 + (a_0 + a_1x + a_2x^2)y + (b_1x + b_2x^2 + b_3x^3 + x^4) = 0,$$

e ela é não singular na origem se $(a_0, b_1) \neq (0, 0)$. Neste caso $f_Q = x$ e, pelo teorema 5.1, para $K = k(x)$, $\alpha = 0$, $\beta = a_2x^2 + a_1x + a_0$ e $\gamma = x^4 + b_3x^3 + b_2x^2 + b_1x$, temos que a extensão $k(C)|k(x)$ é de Galois exatamente quando o grupo de Galois da equação é A_3, isto é, quando

$$\frac{(a_2x^2 + a_1x + a_0)^3}{(x^4 + b_3x^3 + b_2x^2 + b_1x)^2} \in \mathcal{P}(K).$$

Nas notações do teorema de Cardano, isto só é possível se $Y_5 \in k(x)$, e isto ocorre se $Y_4 \in k(x)$. A equação de Y_4 em termos da equação da curva é dada

por

$$Y_4^2 + (x^4 + b_3x^3 + b_2x^2 + b_1x)Y_4 + (a_2x^2 + a_1x + a_0)^3 = 0. \qquad (5\text{-}1)$$

Se $Y_4 \in k(x)$, temos que o único polo, na curva, de Y_4 é o ponto Q. Como a equação (5-1) se anula, temos que duas das três parcelas

$$2v_Q(Y_4), \ \ -12 + V_Q(Y_4), \ \ -18,$$

se anulam, isso só é possível se $\mathrm{div}_Q(Y_4) = 12P_\infty$, isto é

$$Y_4 = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0.$$

Substituindo esta expressão de Y_4 na equação (5-1) encontramos algumas condições para os coeficientes c_j

$$c_3 = b_3 \qquad c_2 = b_2 + a_2^3 \qquad c_1 = b_1 + a_1a_2^2 + a_2^3b_3$$

$$c_0 = a_2a_1^2 + a_2^2(a_0 + a_1b_3) + a_2^3(b_2 + b_3^2) + a_2^6$$

e as seguintes condições, que chamaremos de *Condições de Galois*

$$\begin{aligned} a_2^6b_3 + a_2^3b_3^3 + a_1a_2^2b_3^2 + a_0a_2^2b_3 + a_1^2a_2b_3 + a_2^3b_1 + a_1^3 + a_1a_2^2b_2 &= 0 \\ a_1a_2^2b_1 + a_2^3b_1b_3 + a_0^2a_2 + a_0a_1^2 + a_2^6b_2 + a_2^3b_2^2 + a_2^3b_2b_3^2 + a_1a_2^2b_2b_3 + & \\ a_0a_2^2b_2 + a_1^2a_2b_2 + a_1^2a_2^4 + a_2^6b_3^2 &= 0 \\ a_0^2a_1 + a_2^6b_1 + a_2^3b_1b_2 + a_2^3b_1b_3^2 + a_1a_2^2b_1b_3 + a_0a_2^2 + a_1^2a_2b_1 &= 0 \\ a_1^2a_2^4b_3^2 + a_2^6b_2^2 + a_2^6b_3^4 + a_0^2a_2^4 + a_1^4a_2^2 + a_2^{12} + a_0^3 &= 0. \end{aligned} \qquad (5\text{-}2)$$

Pelo Teorema 1.5 [[10], p 6] temos que um ponto com esta seqüência de ordens 0,1,4 tem peso de Weierstrass maior do que 2, e de fato temos que o peso é pelo menos 4.
O ponto Q tem peso 4 se $a_2 \neq 0$. Se $a_2 = 0$ então, pela condições de Galois (5-2), temos que $a_0 = a_1 = 0$. Logo, o peso de Q é 20 e $[k(x)(Y_4) : k(x)] = 1$. Se $a_2 \neq 0$, então $[k(x)(Y_4) : k(x)] = 2$. Assim,

Teorema 5.1 *O ponto infinito da curva*

$$y^3 + (a_1x + a_0)y + x^4 + b_3x^3 + b_2x^2 + b_1x = 0$$

é um ponto de Weierstrass de peso maior ou igual do que 5, e ele é um ponto de Galois quando $a_0 = a_1 = 0$.

Estudemos o que acontece quando $a_2 \neq 0$. Podemos normalizar a equação da curva e supor que $a_2 = 1$, logo a equação é dada por

$$y^3 + (a_2x^2 + a_1x + a_0)y + (x^4 + b_3x^3 + b_2x^2 + b_1x) = 0.$$

Para esta curva, a tangente no ponto $Q = P_\infty$ é a reta no infinito, a característica teta é dada por $2Q$, e temos que a característica teta é canônica se $a_1 = 0$.
Se $b_1 \neq 0$, o posto da matriz de Hasse-Witt é no máximo dois e é exatamente dois quando $a_1 = 0$ e $b_3 \neq 0$. As condições de Galois (5-2) são equivalentes a

$$\begin{aligned} b_3 + b_3^3 + a_0b_3 + b_1 &= 0 \\ b_1b_3 + a_0^2 + b_2 + b_2^2 + b_2b_3^2 + a_0b_2 + b_3^2 &= 0 \\ 1 + a_0 + b_2 + b_3^2 &= 0 \\ 1 + a_0^2 + a_0^3 + b_2^2 + b_3^4 &= 0. \end{aligned} \tag{5-3}$$

Multiplicando a terceira equação por b_3 e comparando com a primeira temos

$$b_1 = b_2b_3.$$

Como $b_1 \neq 0$ e $b_3 \neq 0$, temos que $b_2 \neq 0$.
Utilizando a igualdade acima e a terceira equação na segunda em (5-3) temos

$$a_0^2 + b_2^2 + a_0b_2 + 1 + a_0 = 0. \tag{5-4}$$

Da última equação em (5-3) temos que

$$b_2^2 + b_3^4 + a_0^2 + 1 + a_0^3 = (1 + b_2 + b_3^2 + a_0)^2 + a_0^3 = 0.$$

Pela terceira equação, temos que $a_0 = 0$. Substituindo este valor em (5-4), temos que $b_2 = 1$ e da terceira equação, temos que $b_3 = 0$, o que é uma contradição. Portanto, $b_1 = 0$. Como a curva é não singular, em particular na origem, temos que a_0 e b_1 não se anulam simultaneamente, logo $a_1 \neq 0$. As condições de Galois se reduzam a

$$\begin{aligned} b_3 + b_3^3 + a_0b_3 &= 0 \\ a_0^2 + a_0b_2 + b_2 + b_2^2 + b_2b_3^2 + b_3^2 &= 0 \\ 1 + a_0^2 + a_0^3 + b_2^2 + b_3^4 &= 0. \end{aligned} \tag{5-5}$$

Se $b_3 \neq 0$, estas condições se reduzem ainda mais

$$\begin{aligned} 1 + b_3^2 + a_0 &= 0 \\ a_0^2 + a_0 b_2 + b_2 + b_2^2 + b_2 b_3^2 + b_3^2 &= 0 \\ 1 + a_0^2 + a_0^3 + b_2^2 + b_3^4 &= 0. \end{aligned} \tag{5-6}$$

Da primeira equação temos

$$a_0 = b_3^2 + 1.$$

Substituindo a expressão de a_0 na última equação temos

$$b_2^2 = a_0^3 = 1 + b_3^2 + b_3^4 + b_3^6$$

e da segunda equação, utilizando as expressões de a_0 e a última relação, temos

$$b_3^6 = 0.$$

Logo, $b_3 = 0$, contradição. Portanto, $b_3 = 0$.
Podemos concluir que se a reta no infinito é a característica teta canônica então o ponto Q é de Galois se, e somente se, $b_3 = 0$ e neste caso o posto da matriz de Hasse-Witt é $\sigma = 1$. Portanto, as condições de Galois estão dadas por

$$\begin{aligned} a_0^2 + a_0 b_2 + b_2 + b_2^2 &= 0 \\ \\ 1 + a_0^2 + a_0^3 + b_2^2 &= 0. \end{aligned} \tag{5-7}$$

Observe que se $a_0 = 1$ então $b_2 = 1$. Das duas equações temos que

$$b_2 = \frac{1 + a_0^3}{1 + a_0}.$$

Substituindo na última equação temos que $a_0^3(a_0 + 1)^3 = 0$, como $a_0 \neq 0$ então $a_0 = 1$. Assim temos o

Teorema 5.2 *Na curva*

$$y^3 + (x^2 + a_1 x + a_0)y + x^4 + b_3 x^3 + b_2 x^2 + b_1 x = 0,$$

a reta no infinito é a bitangente canônica se $a_1 = 0$, e o ponto no infinito é um ponto de Weierstrass, ele é de Galois quando $b_1 = b_3 = 0$ e $a_0 = a_2 = 1$.

Neste caso, o invariante de Hasse-Witt é igual a um.

5.2
Pontos genéricos como pontos Galoisianos

Se Q é um ponto genérico de uma curva de gênero três sobre um corpo de característica dois, temos que sua seqüência de ordens é 0,1,2, logo $d_Q = 4$. A equação da curva é dada por

$$h = y^4 + \mathsf{a}_3 y^3 + \mathsf{a}_2 y^2 + \mathsf{a}_1 y + \mathsf{a}_0 = 0, \tag{5-8}$$

onde $\mathsf{a}_i \in k(f_Q)$. Suponhamos que este polinômio é separável e irredutível, logo o conjunto das raízes R_h tem 4 elementos distintos. O grupo $G_Q = \mathrm{Gal}(k(C)|k(f_Q))$ age transitivamente em R_h, logo G_Q é um subgrupo transitivo de S_4.
Por outro lado, S_4 admite os seguintes subgrupos:

(1) Três subgrupos de Sylow de ordem 8(e logo não normais):

$$\{1,(12)(34),(13)(24),(14)(23),(12),(34),(1423),(1324)\},$$
$$\{1,(12)(34),(13)(24),(14)(23),(13),(24),(1432),(1234)\},$$
$$\{1,(12)(34),(13)(24),(14)(23),(14),(23),(1342),(1243)\},$$

isomorfos a D_4 e transitivos.

(2) O grupo alternado A_4 tem doze elementos e é normal em S_4:

$$A_4 = \{1,(12)(34),(13)(24),(14)(23),(123),(124),(132),(134),(142),(143),(234),(243)\}$$

que também é transitivo e não tem nenhum subgrupo de ordem seis(sendo o menor contra-exemplo para a recíproca do teorema de Lagrange).

(3) Quatro grupos de Sylow não transitivos, pois todos tem um ponto fixo.

$$\{1,(123),(132)\},$$
$$\{1,(124),(142)\},$$
$$\{1,(134),(143)\},$$
$$\{1,(234),(243)\}.$$

(4) Temos outros grupos de ordem quatro

$$\begin{aligned} V = \{&1,(12)(34),(13)(24),(14)(23)\},\\ &\{1,(1234),(13)(24),(1432)\},\\ &\{1,(1324),(12)(34),(1423)\},\\ &\{1,(1342),(14)(23),(1243)\}, \end{aligned}$$

o primeiro subgrupo é conhecido como o *grupo de Klein* ou *Viergruppe*, que é normal em S_4, e em A_4, os outros subgrupos são conjugados do grupo de Klein. O grupo de Klein é isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, enquanto que seus conjugados são isomorfos a $\mathbb{Z}/4\mathbb{Z}$

(5) Outros subgrupos tem ordem dois, que correspondem às involuções, e não são transitivos.

(6) O grupo gerado pelas permutações (a,b) e (c,d,e) onde $\text{card}(a,b,c,d,e)=4$ é todo S_4, enquanto que (a,b) e (a,b,c), com a,b e c distintos, geram o grupo de ordem seis dado por

$$\{1,(a,b),(a,b,c),(a,c,b),(a,c),(b,c)\}.$$

Estes grupos não são normais, e existem quatro grupos assim, contados pelo elemento que cada um deixa fixo, não são transitivos e são todos isomorfos a S_3.

Seja H a interseção de V com o grupo de Galois $G_Q = \text{Gal}(k(C)|k(f_Q))$, isto é, $H = V \cap G_Q$.
Se $\text{R}_h = \{r_1, r_2, r_3, r_4\}$ então a subextensão que corresponde, pelo Teorema Fundamental, ao grupo H é $k(t_1,t_2,t_3)$, onde

$$\begin{aligned} t_1 &= r_1r_2 + r_3r_4,\\ t_2 &= r_1r_3 + r_2r_4,\\ t_3 &= r_1r_4 + r_2r_3. \end{aligned}$$

O polinômio

$$\begin{aligned} g(x) &= (x-t_1)(x-t_2)(x-t_3) \\ &= x^3 + \left(\sum_{i<j} r_i r_j\right) x^2 + \left(\sum_i r_i\right)\left(\sum_{i<j<k} r_i r_j r_k\right) x + \\ &\quad \left(\left(\sum_i r_i\right)^2 \prod_i r_i + \left(\sum_{i<j<k} r_i r_j r_k\right)^2\right) \\ &= x^3 + \mathsf{a}_2 x^2 + \mathsf{a}_1\mathsf{a}_3 x + (\mathsf{a}_3^2\mathsf{a}_0 + \mathsf{a}_1^2) \end{aligned}$$

é chamado a *resolvente cúbica* de $h(x)$, e será separável exatamente quando $h(x)$ o for. De fato, $h(x)$ e $g(x)$ tem o mesmo determinante $\delta = \delta_h = \delta_g$. Logo a quártica irredutível (5-8) tem o grupo de Galois G_Q contido no grupo de Klein V exatamente quando $t_i \in k(f_Q)$ para todo $i = 1, 2, 3$, e como o grupo de Klein não possui subgrupos transitivos próprios, e a quártica (5-8) é irredutível temos que $V = G_Q$. Pelo teorema 5.1, se a cúbica $g(x)$ é irredutível então o grupo de Galois G_g é A_3 se

$$\frac{(\mathsf{a}_1\mathsf{a}_3 + \mathsf{a}_2^2)^3}{(\mathsf{a}_1\mathsf{a}_2\mathsf{a}_3 + \mathsf{a}_0\mathsf{a}_3^2 + \mathsf{a}_1^2)^2} \in \mathcal{P}(K),$$

caso contrário é S_3. O grupo de Galois da resolvente cúbica $g(x)$ é um subgrupo do grupo de Galois G_Q. Se g é redutível então G_g e G_Q são 2-grupos, enquanto que se $G(x)$ é irredutível então o grupo G_g contém um 3-subgrupo de Sylow de G_Q. Portanto, para que o ponto genérico Q seja de Galois o polinômio $g(x)$ deve ser redutível.

5.3 A curva C_a

A curva C_a é definida pela equação

$$y^3 + ay + x^4 + x = 0.$$

Pelo visto anteriormente, esta curva tem invariante de Hasse-Witt $\sigma = 0$ e 5 pontos de Weierstrass: o ponto $P_\infty = (0:1:0)$ de peso 20 e os pontos $P_{\alpha,0} = (\alpha : 0 : 1)$, com $\alpha \in \mathbb{F}_4$, de peso 1 cada. Pelo teorema 5.1, temos que P_∞ não é um ponto de Galois, o fecho normal $k(E_{P_\infty})$ de $k(C_a)$ é dada pela

adjunção da raiz z, Y_4 na notação do teorema de Cardano, da equação

$$z^2 + (x^a + x)z + a^3 = 0.$$

Pelo teorema III.5.10 de [[9], p,96] a extensão $k(C_a)|k(x)$ tem o seguinte diferente

$$Diff_{k(C_a)|k(x)} = 2\left(P_\infty + \sum_{\alpha\in\mathbb{F}_4} P_{\alpha,a^{1/2}}\right),$$

onde $P_{\alpha,a^{1/2}} = (\alpha : a^{1/2} : 1)$. No cálculo do diferente $Diff_{k(E_{P_\infty})|k(C_a)}$ devemos tratar com ramificação não moderada. Denotemos por P_∞^+ e P_∞^- os pontos de $k(x,z)$ que estão acima do ponto P_∞. Temos que

$$\mathrm{div}(z) = 4P_\infty^+ - 4P_\infty^-,$$

e

$$\mathrm{div}(z + a^{3/2}) = \sum_{\alpha\in\mathbb{F}_4} P_{\alpha,a^{3/2}} - 4P_\infty^-.$$

Pelo teorema III.5.10 de [[9], p.96], segue que

$$Diff_{k(z,x)|k(x)} = 2\left(\sum_{\alpha\in\mathbb{F}_4} P_{\alpha,a^{3/2}}\right).$$

Das notações do teorema 5.1, temos que $Y_3 = z^{1/3}$, $Y_2 = \frac{a}{z^{1/3}}$ e $Y_1 = Y_2 + Y_3 = \frac{a}{z^{1/3}} + z^{1/3}$, ou seja

$$y = \frac{a}{z^{1/3}} + z^{1/3}.$$

Assim obtemos um valor de y para cada raiz cúbica de z. Então os pontos $P_{\alpha,\, a^{3/2}}$ são não ramificados na extensão $k(E_{P_\infty})|k(x,z)$, pois existem três pontos $P^i_{\alpha,\, a^{3/2}}$ em $k(E_{P_\infty})$ acima de $P_{\alpha,\, a^{3/2}}$, segundo a escolha $\xi^i a^{1/2}$, com $i = 0, 1, 2$, onde ξ é raiz de $X^2 + X + 1 = 0$.
Por outro lado, os pontos P_∞^+ e P_∞^- são ramificados na extensão $k(E_{P_\infty})|k(x,z)$, pois eles são ramificados em $k(E_{P_\infty})|k(x)$ mas não em $k(x,z)|k(x)$. Como $k(E_{P_\infty})|k(x,z)$ é de Galois, o índice de ramificação de cada ponto é três. Logo, em $k(E_{P_\infty})$ temos

$$\mathrm{div}(x + \alpha) = 2\sum_{i=0,1,2} P^i_{\alpha,a^{3/2}} - 3(P_\infty^+ + P_\infty^-),$$

e

$$\mathrm{div}(x^4 + x) = 2\sum_{i=0,1,2}\sum_{\alpha\in\mathbb{F}_4} P^i_{\alpha,a^{3/2}} - 12(P_\infty^+ + P_\infty^-).$$

Pela equação

$$x^4 + x = y^3 + ay + \frac{z^2 + a^3}{z},$$

segue que

$$\mathrm{div}(y) = 2\sum_{\alpha\in\mathbb{F}_4} P^0_{\alpha,a^{3/2}} - 4(P^+_\infty + P^-_\infty),$$

e

$$\mathrm{div}(y^2 + a) = 2\sum_{i=1,2}\sum_{\alpha\in\mathbb{F}_4} P^i_{\alpha,a^{3/2}} - 8(P^+_\infty + P^-_\infty).$$

Como a extensão $k(E_{P_\infty})|k(x,z)$ é de Galois, então todos os expoentes do diferente acima de um ponto fixo coincidem, ver corolário III.7.2 de [[9], p. 110]e como os pontos P^+_∞ e P^-_∞ são ramificados em $k(E_{P_\infty})|k(x,z)$, pelo teorema de Dedekind, temos que

$$\mathit{Diff}_{k(E_{P_\infty})|k(x,z)} = 2(P^+_\infty + P^-_\infty).$$

Todas as extensões de corpos do diagrama

$$\begin{array}{ccc} k(C_a) & \longrightarrow & k(E_{P_\infty}) \\ \uparrow & & \uparrow \\ k(x) & \longrightarrow & k(x,z) \end{array}$$

são de Galois exceto a extensão do lado esquerdo. Os grupos de galois das extensões horizontais são geradas pelo homomorfismo $z \mapsto z + x^4 + x$.
O grupo de Galois da extensão do lado direito consiste dos homomorfismos

$$y = \frac{a}{z^{1/3}} + z^{1/3} \mapsto \frac{a}{\xi z^{1/3}} + \xi z^{1/3},$$

onde ξ é raiz de $X^2 + X + 1 = 0$.
Pela fórmula

$$\mathit{Diff}_{k(E_{P_\infty})|k(x)} = \mathit{Con}_{k(E_{P_\infty})|k(C_a)}(\mathit{Diff}_{k(x,z)|k(x)}) + \mathit{Diff}_{k(E_{P_\infty})|k(x,z)},$$

temos que

$$\mathit{Diff}_{k(E_{P_\infty})|k(x)} = 2\left(\sum_{i=0,1,2}\sum_{\alpha\in\mathbb{F}_4} P^i_{\alpha,a^{3/2}}\right) + 2(P^+_\infty + P^-_\infty).$$

Como uma conseqüência temos que $g_{k(x,z)} = 3$ e $g_{E_{P_\infty}} = 9$. O discriminante da extensão $k(E_{P_\infty})|k(x)$ é dado por

$$\mathcal{N}_{k(E_{P_\infty})|k(x)}\left(Diff_{k(E_{P_\infty})|k(x)}\right) = 6\sum_{\alpha\in\mathbb{F}_4} P_\alpha + 4P_\infty,$$

e a conorma em $k(C_a)$ é dada por

$$Con_{k(C_a)|k(x)}\left(\mathcal{N}_{k(E_{P_\infty})|k(x)}\left(Diff_{k(E_{P_\infty})|k(x)}\right)\right) = 6\sum_{\alpha\in\mathbb{F}_4}(2P_{\alpha,a^{1/2}}+P_{\alpha,0})+12P_\infty.$$

Vejamos o que acontece com os outros pontos de Weierstrass da forma $P_{\alpha,\,0}$. A tangente a curva C_a no ponto $P_{\alpha,\,0}$ é dada pela equação $x + ay + \alpha = 0$ que intersecta novamente a curva no ponto $P_{\alpha+a^{-3},\,a^{-4}} = (\alpha + \frac{1}{a^3} : \frac{1}{a^4} : 1)$, podemos observar que estes pontos de Weierstrass intersectam a curva em pontos incidentes a reta $y = \frac{1}{a^4}$, obtendo assim uma configuração geométrica interessante. Isto mostra que o parâmetro a é um invariante das classes de isomorfismos da curva. Ou seja, as curvas C_a e $C_{a'}$ são isomorfas se, e somente se, $a = a'$.
A função

$$f_{P_{\alpha,\,0}} = \frac{y + \frac{1}{a^4}}{x + ay + \alpha}$$

tem polo de ordem 3 no ponto $P_{\alpha,\,0}$. Também temos

$$(x + ay + \alpha)f_{P_{\alpha,\,0}} + (y + \frac{1}{a^4} = 0.$$

A resultante desta equação e a equação da curva C_a, dividida por $y + \frac{1}{a^4}$ é

$$\left(f^4_{P_{\alpha,\,0}}a^{16} + a^{12}\right)y^3 + a^8y^2 + 1 + f^3_{P_{\alpha,\,0}}a^{12} = 0. \qquad (5\text{-}9)$$

O Teorema de Cardano afirma que a extensão é de Galois se

$$\frac{(\beta+\alpha^2)^3}{(\beta\alpha+\gamma)^2} = \frac{a^4 f^6_{P_{\alpha,\,0}}}{(a^{12}f^4_{P_{\alpha,\,0}} + f_{P_{\alpha,\,0}} + a^8)^2)^2(af_{P_{\alpha,\,0}}+1)^8} \in \mathcal{P}(k(f_{P_{\alpha,\,0}})).$$

Mas

$$\frac{a^4 f^6_{P_{\alpha,\,0}}}{(a^{12}f^4_{P_{\alpha,\,0}} + f_{P_{\alpha,\,0}} + a^8)^2(af_{P_{\alpha,\,0}}+1)^8} = \left(\frac{a^2 f^3}{(a^{12}f^4_{P_{\alpha,\,0}} + f_{P_{\alpha,\,0}} + a^8)(af_{P_{\alpha,\,0}}+1)^4}\right)^2.$$

Pelo

Lema 5.1 *Seja k um corpo de característica p positiva, então $h \in \mathcal{P}(k)$ se, e somente se, $h^p \in \mathcal{P}(k)$.*

Se

$$\frac{a^4 f_{P_{\alpha,0}}^6}{(a^{12}f_{P_{\alpha,0}}^4 + f_{P_{\alpha,0}} + a^8)^2)^2(af_{P_{\alpha,0}}+1)^8} \in \mathcal{P}(k(f_{P_{\alpha,0}})),$$

então

$$\frac{a^2 f^3}{(a^{12}f_{P_{\alpha,0}}^4 + f_{P_{\alpha,0}} + a^8)(af_{P_{\alpha,0}}+1)^4} \in \mathcal{P}(k(f_{P_{\alpha,0}})).$$

Por outro lado, um polo de qualquer elemento em $\mathcal{P}(k(f_{P_{\alpha,0}}))$ tem ordem par e qualquer zero de $a^{12}f_{P_{\alpha,0}}^4 + f_{P_{\alpha,0}} + a^8$ na expressão dada acima é um polo simples. Logo, a extensão $k(C_a)|k(f_{P_{\alpha,0}})$ não é de Galois e o grupo da equação cúbica é S_3.

O fecho normal $k(E_{P_{\alpha,0}})$ é obtido pela adjunção da raiz z, Y_4 na notação do teorema de Cardano, de

$$z^2 + \frac{a^{16}f_{P_{\alpha,0}}^3(a^{12}f_{P_{\alpha,0}}^4 + f_{P_{\alpha,0}} + a^8)}{(a^{12}+a^{16}f_{P_{\alpha,0}}^4)^2}z + \left(\frac{a^{20}f_{P_{\alpha,0}}^4}{(a^{12}+a^{16}f_{P_{\alpha,0}}^4)^2}\right)^3 = 0. \quad (5\text{-}10)$$

A equação (5-10) tem seus coeficientes no anel $\mathcal{O}_P$ para qualquer ponto P em $k(f_{P_{\alpha,0}})$, exceto para os pontos $P_{\alpha+a^{-3},\beta} = (\alpha + \frac{1}{a^3} : \beta : 1)$ com $\beta^2 + \frac{1}{a^4}\beta + a + \frac{1}{a^8} = 0$, que são zeros de $\left(a^3(1+af_{P_{\alpha,0}})\right)^4$.

Logo, os zeros P_∞ e $P_{\alpha+a^{-3},\beta}$ com $\beta^2 + \frac{1}{a^4}\beta + a + \frac{1}{a^8} = 0$ de $f + \frac{1}{a}$ são não ramificados na extensão $k(C_a)|k(f_{P_{\alpha,0}})$ e $f + \frac{1}{a}$ é um parâmetro local em $k(C_a)$ para cada zero.

Pelo teorema III.5.10 de [[9], p.96], temos que nos pontos P em $k(C_a)$ o expoente do diferente d_P satisfaz

$$d_P \leq v_P\left(y^2 + \frac{a^4}{[a^3(1+af_{P_{\alpha,0}})]^4}\right) = 2v_P\left(y + \frac{1}{a^4(1+af_{P_{\alpha,0}})^2}\right).$$

Em particular, para $P = P_{\alpha,0}$,

$$v_{P_{\alpha,0}}(y) = 1 \qquad \text{e} \qquad v_{P_{\alpha,0}}\left(\frac{1}{a^4(1+af_{P_{\alpha,0}})^2}\right) = 6,$$

logo

$$2v_{P_{\alpha,0}}\left(y + \frac{1}{a^4(1+af_{P_{\alpha,0}})^2}\right) = 2.$$

Confirmando o expoente do diferente esperado $d_{P_{\alpha,0}} = e_{P_{\alpha,0}} = 2$.

Logo, os pontos de ramificação da extensão $k(C_a)|k(f_{P_{\alpha,0}})$ estão nos zeros de $y + \frac{1}{a^4(1+af_{P_{\alpha,0}})^2}$. Para localizar os zeros substituimos a expressão

$$y = \frac{1}{a^4(1+af_{P_{\alpha,0}})^2}$$

em (5-9) obtendo

$$a^4 f_{P_{\alpha,\,0}}^3 (a^{12} f_{P_{\alpha,\,0}}^4 + f_{P_{\alpha,\,0}} + a^8) = 0;$$

novamente a função $f_{P_{\alpha,\,0}}$ é um parâmetro local para cada zero e assim cada zero é não ramificado em $k(C_a)|k(f_{P_{\alpha,\,0}})$. Os pontos de ramificação em $k(C_a)|k(f_{P_{\alpha,\,0}})$ devem satisfazer

$$a^{12} f_{P_{\alpha,\,0}}^4 + f_{P_{\alpha,\,0}} + a^8 = 0.$$

Seja γ uma raiz desta equação, se $Q|P_\gamma$, com $v_{P_\gamma}(f_{P_{\alpha,\,0}} + \gamma) = 1$, então

$$v_Q(f_{P_{\alpha,\,0}} + \gamma) = e_Q.$$

Considerando $f_{P_{\alpha,\,0}} = \gamma$ em (5-9) encontramos $y = \gamma^{-1/2}$.
A função $t = y + \gamma^{-1/2}$ é um parâmetro local em Q e logo

$$f_{P_{\alpha,\,0}} = \gamma + \frac{\gamma^{1/2} + a^4}{a^8 \gamma^2} t^2 + \cdots$$

Como $\gamma \neq a^8$ temos que o coeficiente de t^2 é diferente de zero, logo $e_Q = 2$. Denotemos este pontos como $Q_{\gamma,\,\gamma^{-1/2}}$. O diferente da extensão $k(C_a)|k(f_{P_{\alpha,\,0}})$ é dado por

$$Diff_{k(C_a)|k(f_{P_{\alpha,\,0}})} = 2\left(P_{\alpha,\,0} + \sum_{a^{12}\gamma^4+\gamma+a^8=0} Q_{\gamma,\,\gamma^{-1/2}}\right).$$

A seguintes contas fixam notações de pontos em $k(z, f_{P_{\alpha,\,0}})$ e no fecho normal $k(E_{P_{\alpha,\,0}})$ da extensão $k(C_a)|k(f_{P_{\alpha,\,0}})$. Em $k(z, f_{P_{\alpha,\,0}})$,

$$\mathrm{div}(f_{P_{\alpha,\,0}} + \gamma) = 2R_{\gamma,\,a^{18}\gamma^3} - (R_\infty^1 + R_\infty^2).$$

Logo, os pontos $R_{\gamma,\,a^{18}\gamma^3}$ são ramificados em $k(z, f_{P_{\alpha,\,0}})|k(f_{P_{\alpha,\,0}})$. Pelo teorema III.5.10 de [[9], p.96], temos que

$$Diff_{k(z,f_{P_{\alpha,\,0}})|k(f_{P_{\alpha,\,0}})} = 2\left(\sum_{a^{12}\gamma^4+\gamma+a^8=0} R_{\gamma,\,a^{18}\gamma^3}\right).$$

Nas notações da demonstração do teorema de Cardano, segue que

$$y = \frac{\frac{f_{P_{\alpha,\,0}}^4}{a^4(1+af_{P_{\alpha,\,0}})^8}}{z^{1/3}} + z^{1/3},$$

assim temos uma escolha de y para cada valor da raiz cúbica de z. Os pontos $R_{\gamma,\, a^{18}\gamma^3}$ são não ramificados na extensão $k(E_{P_{\alpha,\,0}})|k(z, f_{P_{\alpha,\,0}})$, pois existem três pontos $R^i_{\gamma,\, a^{18}\gamma^3}$ em $k(E_{P_{\alpha,\,0}})$ acima de $R_{\gamma,\, a^{18}\gamma^3}$. Por outro lado, os pontos R^i_∞ para $i = 1, 2$ são ramificados em $k(E_{P_{\alpha,\,0}})|k(z, f_{P_{\alpha,\,0}})$, pois eles são ramificados em $k(E_{P_{\alpha,\,0}})|k(f_{P_{\alpha,\,0}})$ mas não em $k(z, f_{P_{\alpha,\,0}})|k(f_{P_{\alpha,\,0}})$. Como $k(E_{P_{\alpha,\,0}})|k(z, f_{P_{\alpha,\,0}})$ é de Galois, o índice de ramificação de cada ponto é três.

Para uma extensão em relação ao ponto no infinito temos que os únicos pontos ramificados na extensão $k(E_{P_{\alpha,\,0}})|k(z, f_{P_{\alpha,\,0}})$ são R^i_∞ para $i = 1, 2$. Logo, temos que

$$Diff_{\,k(E_{P_{\alpha,\,0}})|k(z,f_{P_{\alpha,\,0}})} = 2(R^1_\infty + R^2_\infty),$$

$$Diff_{\,k(E_{P_{\alpha,\,0}})|k(f_{P_{\alpha,\,0}})} = 2\left(\sum_{i=0,1,2}\sum_{a^{12}\gamma^4+\gamma+a^8=0} R^i_{\gamma,\, a^{18}\gamma^3}\right) + 2(R^1_\infty + R^2_\infty),$$

$g_{k(z,fp)} = 3$ e $g_{k(E_{P_{\alpha,\,0}})} = 9$.

No caso dos pontos genéricos da curva C_a, podemos considerar dois casos:

Caso 1: Pontos da forma $P_{\alpha,\,\beta} = (\alpha : \beta : 1)$ com $\alpha \in \mathbb{F}_4$ e $\beta^2 = a$.

Caso 2: Pontos da forma $P_{\alpha,\,\beta} = (\alpha : \beta : 1)$ com $\beta^2 \neq a$.

No primeiro caso obtemos a função

$$f_{P_{\alpha,\,\beta}} = \frac{x + ay + \alpha}{(x+\alpha)^2}.$$

Da resultante com a equação da curva temos a equação minimal de y sobre $k(f_{P_{\alpha,\,\beta}})$

$$f^4_{P_{\alpha,\,\beta}} y^4 + a^4 y^2 + (1 + f^3_{P_{\alpha,\,\beta}})y + a^2 f_{P_{\alpha,\,\beta}}(1 + f^3_{P_{\alpha,\,\beta}}) = 0.$$

A resolvente cúbica associada é dada por

$$g(T) = T^3 + \left(\frac{a}{f_{P_{\alpha,\,\beta}}}\right)^4 T^2 + \left(\frac{1 + f^3_{P_{\alpha,\,\beta}}}{f^4_{P_{\alpha,\,\beta}}}\right)^2.$$

Vejamos que $g(T)$ é irredutível em $k(f_{P_{\alpha,\,\beta}})$. Suponhamos que isso não acontece e que existe uma raiz y_0 em $k(f_{P_{\alpha,\,\beta}})$ de $g(T)$, ou seja

$$y_0^3 + \left(\frac{a}{f_{P_{\alpha,\,\beta}}}\right)^4 y_0^2 + \left(\frac{1 + f^3_{P_{\alpha,\,\beta}}}{f^4_{P_{\alpha,\,\beta}}}\right)^2 = 0. \qquad (5\text{-}11)$$

Se R não é polo nem zero de $f_{P_{\alpha,\,\beta}}$, então $v_R(y_0) = 0$. Se R_1 é o polo de $f_{P_{\alpha,\,\beta}}$ devemos ter

$$3v_{R_1}(y_0), \quad 4 + 2v_{R_1}(y_0), \quad 2,$$

Do anulamento de (5-11) temos duas possibilidades

$$3v_{R_1}(y_0) = 4 + 2v_{R_1}(y_0), \quad \text{logo} \quad v_{R_1}(y_0) = 4,$$

ou

$$4 + 2v_{R_1}(y_0) = 2, \quad \text{logo} \quad v_{R_1}(y_0) = -1,$$

Se R_2 é o zero de $f_{P_{\alpha,\,\beta}}$ devemos ter

$$3v_{R_2}(y_0), \quad -4 + 2v_{R_2}(y_0), \quad -8,$$

Do anulamento de (5-11) temos duas possibilidades

$$3v_{R_2}(y_0) = -4 + 2v_{R_2}(y_0), \quad \text{logo} \quad v_{R_2}(y_0) = -4,$$

ou

$$-4 + 2v_{R_2}(y_0) = -8, \quad \text{logo} \quad v_{R_2}(y_0) = -2,$$

Logo, o único zero possível de y_0 seria R_1 com $v_{R_1}(y_0) = 4$. Por outro lado,

$$\begin{aligned} 8 + v_{R_1}\left(1 + \tfrac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right) &= 2v_{R_1}(y_0) + v_{R_1}\left(1 + \tfrac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right) \\ &= v_{R_1}\left(y_0^2\left(1 + \tfrac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right)\right) \\ &= v_{R_1}\left(\tfrac{1+f^6_{P_{\alpha,\,\beta}}}{f^8_{P_{\alpha,\,\beta}}}\right) = 2. \end{aligned}$$

Logo, $v_{R_1}\left(1 + \frac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right) = -6$ que é impossível, pois

$$v_{R_1}\left(1 + \frac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right) = \min\left\{1, v_{R_1}\left(\frac{y_0}{f^4_{P_{\alpha,\,\beta}}}\right)\right\} = \min\{0, 8\} = 0.$$

Pelo visto anteriormente, o ponto $P_{\alpha,\,\beta}$ com $\alpha \in \mathbb{F}_4$ e $\beta^2 \neq a$, não é um ponto de Galois.

Consideremos o caso $P_{\alpha,\,\beta} = (\alpha : \beta : 1)$ com $\beta^2 \neq a$. Neste caso temos

$$f_{P_{\alpha,\,\beta}} = \frac{1}{(x + (\beta^2 + a)y + \alpha^4)^2}\left(y^2 + (\beta^2 + a)^{-4}y + \beta^2 + (x + (\beta^2 + a)y + \alpha^4)\frac{y + (\beta^2 + a)^{-4}}{\beta^2}\right).$$

Da resultante com a equação da curva temos a equação minimal de y sobre $k(f_{P_{\alpha,\,\beta}})$

$$(f^4_{P_{\alpha,\,\beta}}(\beta^2+a)^{16}\beta^8+(\beta^2+a)^{12}+\beta^8(\beta^2+a)^8)y^4+(\beta^2+a)^8y^3+((\beta^2+a)^4+\beta^8)y^2+$$

$$(f^3_{P_{\alpha,\,\beta}}(\beta^2+a)^{12}\beta^6+(\beta^2+a)^8\beta^6 f_{P_{\alpha,\,\beta}}+1)y+\beta^6 f_{P_{\alpha,\,\beta}}(\beta^2+a)^4+\beta^{12}(\beta^2+a)^8+$$

$$f^4_{P_{\alpha,\,\beta}}(\beta^2+a)^{16}\beta^{12}=0.$$

A resolvente cúbica associada é dada por

$$\begin{aligned} g(T) \;&= T^3+\left(\frac{(\beta^2+a)+\beta^2}{f_{P_{\alpha,\,\beta}}(\beta^2+a)^4\beta^2+(\beta^2+a)^3+(\beta^2+a)^2\beta^2}\right)^4 T^2+ \\ &\left(\frac{f^3_{P_{\alpha,\,\beta}}(\beta^2+a)^{12}\beta^6+(\beta^2+a)^8\beta^6 f_{P_{\alpha,\,\beta}}+1}{(f_{P_{\alpha,\,\beta}}(\beta^2+a)^4\beta^2+(\beta^2+a)^3+(\beta^2+a)^2\beta^2)^8}\right)T+ \\ &\frac{1}{(\beta^2+a)^{16}(f_{P_{\alpha,\,\beta}}\beta^2(\beta^2+a)^2+(\beta^2+a)+\beta^2)^{12}}(f^{10}_{P_{\alpha,\,\beta}}(\beta^2+a)^{32}\beta^{20}+f^6_{P_{\alpha,\,\beta}}(\beta^2+a)^{28}\beta^{12}+ \\ &(\beta^2(\beta^2+a)^2((\beta^2+a)^4\beta+1))^4 f^4_{P_{\alpha,\,\beta}}+((\beta^2+a)^4\beta^3((\beta^2+a)+\beta^2))^4 f^2_{P_{\alpha,\,\beta}}+ \\ &((\beta^2+a)^2\beta)^6 f_{P_{\alpha,\,\beta}}+((\beta^2+a)+\beta^2+(\beta^2+a)^2\beta^3)^4). \end{aligned}$$

Como no caso anterior, temos que a resolvente é irredutível em $k(f_{P_{\alpha,\,\beta}})$. Vejamos isto, suponhamos que $g(T)$ tem uma raiz y_0. Seja R polo de $f_{P_{\alpha,\,\beta}}$. Como $g(y_0)=0$, temos que dois dos valores das quatro parcelas

$$3v_R(y_0),\quad 4+2v_R(y_0),\quad 5+v_R(y_0),\quad 2,$$

devem coincidir e são os menores possíveis. Temos 4 possibilidades

(a) $3v_R(y_0)=4+2v_R(y_0)$, logo $v_R(y_0)=4$, mas isto não é possível pois o menor valor seria o último, 2, que é menor que os valores dos dois primeiros termos.

(b) $4+2v_R(y_0)=5+v_R(y_0)$, logo $v_R(y_0)=1$, mas isto não é possível pois o menor valor seria o último, 2, que é menor que os valores dos termos centrais.

(c) $4+2v_R(y_0)=2$, logo $v_R(y_0)=-1$, mas isto não é possível , pois o termo com o menor valor seria o primeiro, com valor -3, menor que o valor dos dois termos escolhidos.

(d) $5 + v_R(y_0) = 2$, logo $v_R(y_0) = -3$, também não é possível pois o termo com o menor valor é o primeiro, com valor -9, menor que os dois valores dos termos escolhidos.

Então, o único polo possível de y_0 é R_2 e a cúbica resultante não tem raiz. Portanto, o ponto $P_{\alpha,\beta}$ não é um ponto de Galois.