

**Lemma Q.1.** *Proof:*

Denote  $h = x_2^2 - f(x_1)$  and assume  $h = u \cdot v$  where  $u, v \in \bar{K}[x_1, x_2]$ .

First assume  $u, v \in \bar{K}[x_1, x_2] \setminus \bar{K}[x_1]$  i.e.  $\deg_{x_2}(u) > 0, \deg_{x_2}(v) > 0$ . Because  $\deg_{x_2}(u) + \deg_{x_2}(v) = \deg_{x_2}(h) = 2 \implies \deg_{x_2}(u) = 1 = \deg_{x_2}(v)$ . W.l.o.g assume  $lc_{x_2}(u) = 1 = lc_{x_2}(v)$ , we can do that since  $lc_{x_2}(h) = 1$ . Therefore we can write  $u = x_2 - s_1$  and  $v = x_2 - s_2$  where  $s_1, s_2 \in \bar{K}[x_1]$ . This gives us

$$x_2^2 - f(x_1) = h = (x_2 - s_1)(x_2 - s_2) = x_2^2 - (s_1 + s_2)x_2 + s_1s_2$$

So it must hold that  $s_1 = -s_2$  and then  $h = x_2^2 + s_1(-s_1) \implies f(x_1) = s_1^2$ .

Now assume w.l.o.g  $u \in \bar{K}[x_1]$ . We compare the leading coefficients.

$$1 = lc_{x_2}(h) = lc_{x_2}(u) \cdot lc_{x_2}(v) = u \cdot lc_{x_2}(v)$$

This shows that  $u$  must be invertible in  $\bar{K}[x_1, x_2] \implies u \in \bar{K}^*$ . In other words  $h$  is absolutely irreducible. □

**Sublemma Q.3.5** *Let  $F/K$  be an algebraic function field,  $\text{char}(K) \neq 2$ , that is given by  $y^2 = f(x)$ ,  $f$  being a quaternary polynomial that possesses a simple root. Let  $P \in \mathbb{P}_{F/K}$ . If  $x \notin P$  or  $y \notin P$ , then  $x, y \notin P$  and  $2v_P(x) = v_P(y)$ .*

*Proof:* In  $F$  it holds  $y^2 = f(x)$  by definition which implies that for every  $P \in \mathbb{P}_{F/K}$   $v_P(y^2) = 2v_P(y) = v_P(f(x))$ .

Assume  $v_P(x) < 0 \leq v_P(y)$ . By properties of valuation we have  $\deg(f)v_P(x) = v_P(f(x)) = 2v_P(y) \implies 2v_P(x) = v_P(y)$  and by assumption  $v_P(y) > v_P(x) \implies 2v_P(x) > v_P(x) \iff v_P(x) > 0$ . That's a contradiction.

Now assume  $v_P(x) \geq 0 > v_P(y)$ .  $v_P(x) \geq 0 \implies v_P(f(x)) \geq 0$  then  $0 \leq v_P(f(x)) = 2v_P(y) < 0$  which is again a contradiction.

We have proven  $v_P(x) < 0 \iff v_P(y) < 0$ . Therefore we have the equality  $4v_P(x) = 2v_P(y) \iff 2v_P(x) = v_P(y)$  assuming  $v_P(x) < 0$  or  $v_P(y) < 0$ . □

**Lemma Q.4.** *Proof:* By sublemma Q.3.5 we know, that if  $P \in \mathbb{P}_{F/K} : x^{-1} \in P \implies y^{-1} \in P$  and  $2v_P(x) = v_P(y)$ . This proves  $(y)_- = 2(x)_-$  ( $x^{-1}, y^{-1}$  "share" places and the valuation is 2:1).

Let's first assume that  $f$  possesses a multiple root. Therefore  $f(x_1) = (x_1 - \alpha)^2 g(x_1)$  where  $\deg(g) = 2$  and  $g$  is not a square. By Q.3  $F$  is given by  $z^2 = g(x)$  i.e.  $F = K(x, z)$ .  $[F : K(x)] = 2$  since  $\min_{z, K(x)}(T) = T^2 - g(x)$ , that polynomial has  $z$  as a root in  $F$  and it is absolutely irreducible (as a polynomial in  $K[x, T]$ ) since  $g$  is not a square. We can then assume  $\bar{K} = K$  since  $[F : \bar{K}(x)] = 2$  (same polynomial) and  $[F : K(x)] = [F : \bar{K}(x)][\bar{K} : K] = 2 \implies [\bar{K} : K] = 1$ .

Then we know  $\deg((x)_-) = [F : K(x^{-1})] = [F : K(x)] = 2$  i.e.  $\deg(D) = 2$ .

Now assume  $f$  is separable. We can then use the same argument for  $K = \bar{K}$  since  $\min_{y, K(x)}(T) = T^2 - f(x)$  and by Q.1 this one is also absolutely irreducible.  $F = K(x, y) \implies [F : K(x)] = [F : \bar{K}(x)][\bar{K} : K] = 2 \implies [\bar{K} : K] = 1$ . And again  $\deg(D) = 2$ .

Now let's prove that the genus is at most 1. Since  $\deg(D) = 2 \implies \sum_{P: x^{-1} \in P} v_P(x) \deg(P) = 2$  means we have 2 possibilities (we are assuming  $K = \bar{K}$  which implies  $\forall P \in \mathbb{P}_{F/K} : \deg(P) = 1$ ):

1. There exists a unique place  $P_\infty : v_{P_\infty}(x) = -2, v_{P_\infty}(y) = -4$  and  $D = 2P_\infty$
2. There are 2 distinct places  $P, Q$  s.t.  $v_P(x) = -1 = v_Q(x), v_P(y) = -2 = v_Q(y)$  and  $D = P + Q$ .

In both cases we can see that for  $k \geq 2 : \{1, x, \dots, x^k, y, yx, \dots, yx^{k-2}\} \subset \mathcal{L}(kD)$  because  $(x^k)_+ + kD = k((x)_+ - (x)_-) + k(x)_- = k(x)_+ \geq 0$  and also  $(y)_- = 2(x)_-$  so it holds if we substitute  $x^2$  for  $y$ . This subset is linearly indepent over  $K$  because  $y$  cannot be expressed as a linear combination of  $x^i$  since  $f$  has one simple root (if  $f(x) = g^2(x) \implies y = g(x)$ ). The set also contains  $2k$  elements. Therefore  $l(kD) \geq 2k$ .

We know that for a sufficiently large  $k$  (if  $l(kD) \geq 2g - 1$ ,  $g$  genus) we have  $l(kD) = \deg(kD) - g + 1$  having  $\deg(kD) = 2k, l(kD) \geq 2k \implies 0 \leq l(kD) - \deg(kD) = -g + 1 \iff g \leq 1$ .

□

**Proposition Q.5.** *Proof:* As noted by paragraph before Q.5. w.l.o.g. we can assume  $f(x) = x^4 + bx^2 + cx + d$ . Denote  $bx^2 + cx + d = g(x) = f(x) - x^4$ . First we will prove that for both  $z \in Z = \{y + x^2, y - x^2\} : [F : K(z)] = 2$ .

Denote  $z_1 = y + x^2, z_2 = y - x^2$ . First we show that  $F = K(x, z_i)$  for  $i = 1, 2$ .  $F$  can be expressed as  $K(x, y)$ .  $y \in K(x, z_i)$  since  $z_i \pm x^2 = y$ . This shows  $F \subseteq K(x, z_i)$  and the converse is obvious. Also  $K(x, z_i) \neq K(z_i)$  because for genus 1 it is a contradiction. If genus is 0 then  $F = K(x + y)$  and it would mean  $K(x + y) = K(y \pm x^2)$ .

We will find minimal polynomial  $m(T)$  of  $x$  over  $K(z_1)$  then  $\deg(m) = [F : K(z_1)] = [K(x, z_1) : K(z_1)]$ .  $z_2 = z_1 - 2x^2$  and  $z_1 z_2 = y^2 - x^4 = g(x)$ . Then:

$$z_1(z_1 - 2x^2) = g(x) = bx^2 + cx + d$$

Then  $m(T) = z_1(z_1 - 2T^2) - bT^2 - cT - d \in K(z_1)[T]$ .  $\deg(m) = 2$  and  $m(x) = 0$  and  $F \neq K(z_1) \implies$  this must be a minimal polymial of  $x$  over  $K(z_1)$ .

In a similar way we can find a minimal polynomial of  $x$  over  $K(z_2) : m(T) = z_2(z_2 + 2T^2) - bT^2 - cT - d \in K(z_2)[T]$ .

We have shown  $[F : K(z_i)] = 2$ .

Choose  $P \leq D$  a place. We will prove that for at least one  $z \in Z : v_P(z) < v_P(x)$ .

$$\begin{aligned} y^2 = f(x) &\iff y^2 - x^4 = g(x), 0 \leq \deg(g) \leq 3 \implies \\ (y + x^2)(y - x^2) = g(x) &\implies v_P(y + x^2) + v_P(y - x^2) = v_P(g(x)) = \deg(g)v_P(x) \end{aligned}$$

Denote  $z_1 = y + x^2, z_2 = y - x^2$ . Assume to contrary  $v_P(z_1) \geq v_P(x)$  and  $v_P(z_2) \geq v_P(x)$ . We will look at all possible cases.

$\deg(g) = 3$ :  $3v_P(x) = v_P(z_1) + v_P(z_2) \geq v_P(x) + v_P(x) \implies v_P(x) > 0$  which is a contradiction since  $v_P(x) < 0$ .

$\deg(g) = 2$ :  $2v_P(x) = v_P(z_1) + v_P(z_2)$ .

First consider  $v_P(x) = v_P(z_1) = v_P(z_2)$  and  $v_P(x) = -2$ , then  $2P = (x)_- = (z_1)_- = (z_2)_-$ . Then  $z_1, z_2 \in \mathcal{L}(D)$  but then also  $\frac{z_1 + z_2}{2} = y \in \mathcal{L}(D)$  which is a contradiction since  $(y)_- = 2(x)_-$ .

Now let's assume  $v_P(x) = -1$  and then there also exist a different place  $Q$  s.t.  $v_Q(x) = v_Q(z_1) = v_Q(z_2) = -1$ . Since  $\deg((z)_-) = 2$  then again  $P + Q = (x)_- = (z_1)_- = (z_2)_-$  and we have the same contradiction.

We have proven that  $v_P(x) = v_P(z_1) = v_P(z_2)$  is impossible therefore for one  $z$  it must hold  $v_P(z) < v_P(x)$ .

$\deg(g) = 1$ :  $v_P(x) = v_P(z_1) + v_P(z_2)$ . First assume  $v_P(x) = -2$ . And also  $v_P(z_1) = v_P(z_2) = -1$ . This is impossible since  $\deg((z)_-) = 2$  but for every other place  $Q \neq P$ :  $0 = v_Q(z_1) + v_Q(z_2) \implies v_Q(z_1) = -v_Q(z_2)$ . If there was  $Q_1 : v_{Q_1}(z_1) = -1 \implies v_{Q_1}(z_2) = 1$  and  $Q_2 : v_{Q_2}(z_2) = -1 \implies v_{Q_2}(z_1) = 1$ . Then for some  $P_1, P_2$  places of degree 1:  $(z_1) = (P_1 + Q_2) - (P + Q_1)$ ,  $(z_2) = (P_2 + Q_1) - (P + Q_2)$ . Set  $D' = P + Q_1 + Q_2$  then  $z_1, z_2 \in \mathcal{L}(D')$  and as before this means that  $y \in \mathcal{L}(D')$  which is a contradiction.

Now if  $v_P(x) = -1$  then either  $v_P(z) < v_P(x)$  for a  $z \in Z$  or w.l.o.g  $v_P(z_1) = -1$  and  $v_P(z_2) = 0$ . Then also assume first  $v_Q(z_1) = -1 \implies v_Q(z_2) = 0$ . But since  $\deg((z)_+) = 2$  there must be a place  $P'$  s.t.  $v_{P'}(z_2) > 0$  and  $v_{P'}(x) = 0$  since  $P' \neq P, Q$  but it must be  $v_{P'}(z_1) < 0$ . This again contradicts the degree of the divisor.

If  $v_Q(z_1) = 0$  and  $v_Q(z_2) = -1$ . Then again there must be a place  $P_1$  s.t.  $v_{P_1}(z_1) = -1$  and  $v_{P_1}(z_2) = 1$  and a place  $P_2(z_2) = 1 \implies v_{P_2}(z_1) = -1$ . This also contradicts divisor degree.

The last case is  $\deg(g) = 0$ :  $v_P(z_1) = -v_P(z_2) \implies (z_1) = -(z_2)$ . First assume  $v_P(z_1) = 0 \implies v_P(z_2) = 0$  and same for  $v_Q$  ( $Q$  not necessarily different from  $P$ ). Then there exist places  $P_1, P_2, Q_1, Q_2 \neq P, Q$  s.t.  $(z_1) = P_1 + P_2 - (Q_1 + Q_2)$ ,  $(z_2) = -(z_1)$ . Set  $D' = P_1 + P_2 + Q_1 + Q_2$  then  $z_1, z_2 \in \mathcal{L}(D')$  but also  $y \in \mathcal{L}(D')$  which is again contradiction since  $(y)_- = 2(x)_-$ .

If  $v_P(z_1) = 1 \implies v_P(z_2) = -1$ . There exists another place  $P'$  s.t.  $v_{P'}(z_1) = 1 \implies v_{P'}(z_2) = -1$ . There must be again two places  $Q_1, Q_2$  s.t.  $(z_1) = P + P' - (Q_1 + Q_2)$ ,  $(z_2) = -(z_1)$ . Put  $D' = P + P' + Q_1 + Q_2$  then again  $y \in \mathcal{L}(D')$  which is a contradiction.

We have proven that for each place  $P \leq D$  at least one  $z \in Z$  must have  $v_P(z) < v_P(x)$ . This shows also that  $(x)_- = P + Q$  for distinct  $P, Q$ . If  $P = Q$  then  $v_P(x) = -2 \implies v_P(z) \leq -3$  which contradicts  $[F : K(z)] = 2$ . Since  $\deg((z)_-) = 2$  and  $v_P(z) < -1$  it must be that  $(z)_- = 2P$ ,  $(z')_- = 2Q$  for  $z, z' \in Z$ . Since we have not distinguished  $P$  and  $Q$  we can say  $(z_1)_- = 2P$  and  $(z_2)_- = 2Q$ . □

**Theorem Q.6.** *Proof:* Assume genus 0. There exists  $t \in F$  s.t.  $(t) = P - Q$  and also  $(t^{-1}) = -(t) = Q - P$ . Also  $l(D) = \deg(D) + 1 = 3$ .

$t \in \mathcal{L}(D)$  since  $(t) + D = P - Q + P + Q = 2P \geq 0$ . Also  $t^{-1} \in \mathcal{L}(D) : (t^{-1}) + D = Q - P + P + Q = 2Q \geq 0$ .  $t$  and  $t^{-1}$  are linearly independent since  $t \notin K$ . This means  $\{1, t, t^{-1}\}$  is a basis of  $\mathcal{L}(D)$ .

$x \in \mathcal{L}(D) \implies x = c_0 + c_1 t + c_2 t^{-1}$  for some  $c_i \in K$ . This is equivalent to saying  $tx = u(t)$ ,  $u(t) \in K[t]$ ,  $\deg(u) = 2$ .

In the same way we see  $\{1, t, t^{-1}, t^2, t^{-2}\}$  for a basis of  $\mathcal{L}(2D)$ . Again  $y \in \mathcal{L}(2D) : (y) + 2D = (y)_+ - (y)_- + 2(x)_- = (y)_+ \geq 0$ . This means  $t^2 y = v(t)$  where  $v(t) \in K[t]$ ,  $\deg(v) = 4$ .

$y^2 = f(x) \iff t^4 y^2 = t^4 f(x)$ . Substitute  $yt = v(t)$  and  $xt^2 = u(t)$  then we have equality  $v^2(t) = t^4 f(\frac{u(t)}{t})$ .  $f$  is a polynomial of degree 4 therefore it has up to 4 different roots  $1 \leq i \leq 4 : \alpha_i \implies v^2(t) = t^4 (\frac{u(t)}{t} - \alpha_1)(\frac{u(t)}{t} - \alpha_2)(\frac{u(t)}{t} - \alpha_3)(\frac{u(t)}{t} - \alpha_4)$  we can

rewrite this as

$$v^2(t) = (u(t) - t\alpha_1)(u(t) - t\alpha_2)(u(t) - t\alpha_3)(u(t) - t\alpha_4)$$

$v^2(t) = v(t)v(t)$  is a polynomial of degree 8, which has at most 4 different roots. Also  $u(t) - t\alpha_i$  is a polynomial of degree 2. There exist at most two  $\alpha \in K$  s.t.  $u(t) - t\alpha$  has a root of multiplicity 2. This is because the root of a quadratic polynomial has multiplicity 2 when the discriminant  $D$  is 0. If  $g(x) - \alpha x = ax^2 + (b - \alpha)x + c \implies 0 = D = (b - \alpha)^2 - 4ac \iff \alpha = \pm 2\sqrt{ac} + b$ .

Also if  $i \neq j : \alpha_i \neq \alpha_j$  the polynomials  $u(t) - t\alpha_i$  and  $u(t) - t\alpha_j$  do not have common roots. This means that if  $1 \leq i \leq 4 : \alpha_i$  are all different then  $v^2(t)$  has at least  $6 = 2 + 2 + 1 + 1$  different roots. This a contradiction.

Therefore if genus is 0 then  $f$  cannot be separable. We have shown that genus of  $F$  is 0 or 1, this means that for  $f$  separable we must have genus 1.

Denote  $w = x_2^2 - f(x_1)$ .

$$\frac{\partial w}{\partial x_1} = -f'(x_1), \frac{\partial w}{\partial x_1} = 2x_2 \quad (1)$$

For a singularity  $\alpha = (\alpha_1, \alpha_2)$ ,  $\alpha_2$  must be 0 and  $\alpha_1$  must be a root of  $f(x_1)$  and also of  $f'(x_1)$  this is true iff  $f(x_1)$  is separable. If  $f(x_1)$  is not separable then it shares a common root  $\alpha_1$  with  $f'(x_1)$  and this gives us singularity at  $(\alpha_1, 0)$ . This proves the rest of the theorem. □

**Theorem Q.7.** *Proof:* Denote  $D = P + Q$  a divisor. Due to genus being 1  $\forall k \geq 1 : l(kD) = 2k$ .  $l(D) = 2$  and that means there exists  $x \notin K$  s.t.  $\{1, x\}$  is a basis of  $\mathcal{L}(D)$  and also  $(x)_- \leq P + Q$ . Then  $(x)^2 = 2(x) = 2(x)_+ - 2(x)_- \implies x^2 \in \mathcal{L}(2D)$ ,  $\{1, x, x^2\}$  is linearly independent in  $\mathcal{L}(2D)$  but  $l(2D) = 4$  that means there exists  $y \in \mathcal{L}(2D) \setminus \mathcal{L}(D)$  such that  $\{1, x, x^2, y\}$  is a basis of  $\mathcal{L}(2D)$ .

Denote  $B = \{1, x, x^2, x^3, x^4, y, yx, yx^2, y^2\}$ , clearly  $B \subseteq \mathcal{L}(4D)$ ,  $l(4D) = 8$  and  $|B| = 9 \implies 1 \leq i \leq 8 : \exists a_i \in K :$

$$y^2 = a_1y + a_2yx + a_3yx^2 + a_4x^4 + a_5x^3 + a_6x^2 + a_7x + a_8$$

Denote  $C = \{1, x, x^2, x^3, y, yx\}$ .  $C$  is a basis of  $\mathcal{L}(3D)$ ,  $C \cup \{yx^2, y^2\}$  is also a basis of  $\mathcal{L}(4D)$  since  $y^2, yx^2 \in \mathcal{L}(4D) \setminus \mathcal{L}(3D)$  because we have chosen  $y$  s.t.  $(y)_- \geq 2P$  or  $(y)_- \geq 2Q$ .

If  $a_4 = 0$  that would be a contradiction to  $C \cup \{yx^2, y^2\}$  being a basis of  $\mathcal{L}(4D)$  since  $y^2$  would be a linear combination of 7 elements.

Now we make a substitution  $y \rightarrow y - \frac{a_1 + a_2x + a_3x^2}{2}$ . This gives us form:

$$y^2 = b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5$$

where  $b_1 = a_4 + \frac{a_3^2}{4}$ . If  $b_1 = 0$  then  $y^2$  would be a linear combination of elements in  $\mathcal{L}(3D)$  that is a contradiction. □

**Theorem Q.8.** *Proof:* Denote  $f(x) = g(x^2)$ .  $F$  is EFF therefore genus is 1 and there exists a place of degree 1. Also this means  $K$  algebraically closed.

If  $g(x)$  has a multiple root  $\alpha$ , then  $f(x) = g(x^2)$  has also a multiple root because  $g(x) = (x - \alpha)^2 \implies g(x^2) = (x - \sqrt{\alpha})^2(x + \sqrt{\alpha})^2$ . Set  $z = \frac{y}{x - \sqrt{\alpha}}$ . Then  $F$  is given by

$z^2 = (x + \sqrt{\alpha})^2$ . This means (using same technique as in Q.2) that  $F = K(x + z)$  which means  $F$  has genus 0, a contradiction.

From now on we can assume  $g(x)$  has 2 distinct roots. If  $f(x) = g(x^2)$  would have a multiple root then it's genus would not be 1 by Q.6. So we can assume  $g(x^2)$  separable.

First we will prove the second part of the theorem. We have shown that  $g(x^2)$  must be separable. Therefore by Q.5 we have places of degree 1 ( $P \neq Q$ ),  $(x)_- = P + Q$  and  $(y + x^2)_- = 2Q$ ,  $(y - x^2)_- = 2P$ .

$$y^2 = g(x^2) = x^4 + 2bx^2 + c \iff y^2 - (x^4 - 2bx^2 - b^2) = c - b^2 \implies \\ (y - (x^2 + b))(y + (x^2 + b)) = c - b^2$$

Since  $g(x^2)$  is separable  $g(x)$  must have simple roots. If  $g(x)$  has a multiple root then it's discriminant is 0 and that happens iff  $c - b^2 = 0$ . So we know  $0 \neq c - b^2 \in K$ .

$$0 = v_P(c - b^2) = v_P(y - (x^2 + b)) + v_P(y + (x^2 + b)) \\ v_P(y - (x^2 + b)) = v_P(y - x^2) = -2 \implies v_P(y + (x^2 + b)) = 2$$

Similarly we can show  $v_Q(y - (x^2 + b)) = 2$  and  $v_Q(y + x^2 + b) = -2$ .

Since  $\deg((y+x^2+b)_+) = \deg((y+x^2+b)_-) = \deg((y+x^2)_-) = 2 \implies \text{div}(y+x^2+b) = 2P - 2Q$  and similarly  $\text{div}(y + x^2 + b) = 2Q - 2P$ .

We have proven the last part of the theorem. Now let's prove the equivalence.

As we have shown before. We can assume  $g(x^2)$  separable and then we have involution  $P-Q$  as shown above since  $2P-2Q = (t)$  for  $t \in F$ . We only have to show that  $P-Q \neq (t)$  for some  $t \in F$ .

If  $t \in F$  s.t.  $(t) = P - Q \implies \deg((t)_+) = 1 = [F : K(t)]$  and that would be contradiction with  $F$  being EFF.

Now we assume we have involution. This mean we have  $P \neq Q$  places of degree one s.t.  $2[P - Q] = (t)$ ,  $t \in F$  and  $P - Q \neq (s)$ ,  $s \in F$ . Using Q.7 we know  $F$  is given by  $y^2 = f(x)$ ,  $\deg(f) = 4$  and  $f$  monic where  $x, y \in F$ ,  $(x)_- = P + Q$ . We can also assume  $f$  separable since  $F$  is of genus 1 using Q.6. If  $f$  has no simple root then similarly it can be shown  $F$  has genus 0.

By Q.5 we also have  $(y - x^2)_- = 2P$  and  $(y + x^2)_- = 2Q$ . We know that  $t \in \mathcal{L}(2P)$ ,  $t^{-1} \in \mathcal{L}(2Q)$ . Since  $t \notin K$   $\{1, t\}$  forms a basis of  $\mathcal{L}(2P)$  and  $\{1, t^{-1}\}$  forms a basis of  $\mathcal{L}(2Q)$  therefore there exist  $p_1, p_2, q_1, q_2 \in K$  s.t.  $y - x^2 = p_1 + p_2t$ ,  $y + x^2 = q_1 + q_2t^{-1}$ . We know that  $f(x) = x^4 + ax^3 + bx^2 + cx + d$ ,  $a, b, c, d \in K$ . We want to show that  $a = 0 = c$ .

We have  $y^2 - x^4 = (y - x^2)(y + x^2) = ax^3 + bx^2 + cx + d \iff (p_1 + p_2t)(q_1 + q_2t^{-1}) - d = ax^3 + bx^2 + cx$ . If we use new names for the coefficients on the left side ( $s_1, s_2, s_3 \in K$ ,  $s_1, s_2 \neq 0$ ) we get:

$$s_1t + s_2t^{-1} + s_3 = ax^3 + bx^2 + cx$$

We know  $v_P(t) = 2$  and  $v_P(t^{-1}) = -2$ . Assume  $s_3 \neq 0$ . Then  $v_P(s_2t^{-1} + s_3) = -2$  since  $v_P(s_3) = 0$ . Also this means that  $v_P(s_1t + s_2t^{-1} + s_3) = -2$ . If  $s_3 = 0$  we get the same result. We now have:

$$-2 = v_P(ax^3 + bx^2 + cx) = v_P(x) + v_P(ax^2 + bx + c)$$

Since  $v_P(x) = -1$  we have  $v_P(ax^2 + bx + c) = -1$ . It must be that  $a = 0$ .

Now we have  $s_1t + s_2t^{-1} + s_3 = bx^2 + cx \iff cx = s_1t + s_2t^{-1} + s_3 - bx^2$ . Assume  $c \neq 0$ . If  $b = 0$  then  $x \in K(t)$  and since  $y + x^2 \in K(t)$  we have  $y \in K(t) \implies F = K(t)$  which is a contradiction with genus being 1. If  $b \neq 0$  then  $x \in K(t, x^2)$  and also since  $(y - x^2) - (y + x^2) \in K(t) \implies x^2 \in K(t) \implies x \in K(t)$  and also  $y \in K(t)$  which is again a contradiction with  $F$  being genus 1.

Therefore it must be  $a = 0 = c$ . □

**Proposition G.2** *Proof:* Since  $F/K$  is given by  $y^2 = g(x^2)$  we know that  $F = K(x, y)$ .

Clearly  $K(\tilde{x}, \tilde{y}) \subseteq K(x, y)$ . The other inclusion is also clear since  $x = \tilde{x}^{-1}\tilde{y}$  and  $y = 2\tilde{x} - x^2 - b$ .

Now we need to show that  $-\tilde{y}^2 + \tilde{x}^3 - b\tilde{x}^2 + \frac{b^2-c}{4}\tilde{x} = 0$  in  $F$ .

$$\tilde{y}^2 = \tilde{x}^3 - b\tilde{x}^2 + \frac{b^2-c}{4}\tilde{x}$$

Substitute  $\tilde{x}, \tilde{y}$ :

$$\begin{aligned} \frac{x^2u^2}{4} &= \frac{u^3}{8} - \frac{bu^2}{4} + \frac{b^2-c}{8}u \\ 2x^2u^2 &= u^3 - 2bu^2 + (b^2-c)u \end{aligned}$$

Divide by  $u \neq 0$  in  $F$ :

$$2x^2u = u^2 - 2bu + (b^2 - c)$$

Substitute  $u = y + x^2 + b$ :

$$\begin{aligned} 2x^2(y + x^2 + b) &= (y^2 + x^4 + 2yx^2 + 2by + 2bx^2 + b^2) - 2b(y + x^2 + b) + b^2 - c \\ &\iff \\ y^2 - x^4 - 2bx^2 - c &= y^2 - g(x^2) = 0 \end{aligned}$$

We have shown that  $\tilde{y}^2 = \tilde{x}^3 - b\tilde{x}^2 + \frac{b^2-c}{4}\tilde{x}$  in  $F$  since  $y^2 = g(x^2)$  in  $F$  by definition.

The only thing left is to show that  $y^2 - x^3 + bx^2 + \frac{b^2-c}{4}x$  is irreducible in  $K[x, y]$ . Using Eisenstein criterion with  $x \in K[x]$  as a prime element we get that this polynomial is indeed irreducible in  $(K[x])[y]$ . □

**Theorem G.3** *Proof:* Assume we have  $(a_2, a_4) \in K \times K$  s.t.  $a_4 \neq 0 \neq a_2^2 - 4a_4$ . Set  $b = -a_2$  and  $c = -4a_4 + a_2^2$ . If  $c = 0$  this would mean that  $4a_4 = a_2^2$  which is a contradiction with  $a_2^2 - 4a_4 \neq 0$ . If  $b^2 - c = 0 \iff c = b^2$  then this would imply  $-4a_4 + a_2^2 = a_2^2 \iff a_4 = 0$  which is again a contradiction.

On the other hand assume we have  $(b, c) \in K \times K$  s.t.  $c \neq 0 \neq b^2 - c$ . Set  $a_2 = -b, a_4 = \frac{b^2-c}{4}$ . If  $a_4 = 0$  this would imply  $b^2 - c = 0$  which is contradiction. If  $a_2^2 - 4a_4 = 0 \iff b^2 = b^2 - c \iff c = 0$  which is a contradiction.

We have therefore proven that G.1 holds.

Denote the rational map  $C_1 \rightarrow C_2$  as  $\psi$  and the map  $C_2 \rightarrow C_1$  as  $\phi$ . Also  $f(x_1, x_2) = x_2^2 - x_1^3 - a_2x_1^2 - a_4x_1, C_1 = V_f, g(x_1, x_2) = x_2^2 - x_1^4 - 2bx_1^2 - c, C_2 = V_g$ .

Now we need to show that  $\psi$  and  $\phi$  are actually  $K$ -rational maps. We will use lemma R.6 from the lecture.

First we know that  $\phi$  is a rational map thanks to proposition G.2. By proposition G.2 (since  $a_2 = -b, a_4 = \frac{b^2-c}{4}$ ) we have shown that  $(\rho_1, \rho_2) = 0 \in K(C_2)$  where  $(\rho_1, \rho_2) = \left(\frac{x_2+x_1^2+b}{2} + (g), \frac{x_1(x_2+x_1^2+b)}{2} + (g)\right)$ . By lemma R.6 this means that  $\phi$  is a  $K$ -rational map  $C_2 \rightarrow C_1$ .

To show that  $\psi$  is a  $K$ -rational map  $C_1 \rightarrow C_2$  we need to prove that  $g(\rho_1, \rho_2) = 0 \in K(C_1)$  where  $(\rho_1, \rho_2) = \left(\frac{x_2}{x_1} + (f), \frac{x_1^2 - a_4}{x_1} + (f)\right)$ .

$$g(\rho_1, \rho_2) = \frac{(x_1^2 - a_4)^2}{x_1^2} - \frac{x_2^4}{x_1^4} - 2b \frac{x_2^2}{x_1^2} - c$$

$$g(\rho_1, \rho_2) = 0 \iff x_1^4 g(\rho_1, \rho_2) = 0 \text{ and using } b = -a_2, c = a_2^2 - 4a_4 \implies$$

$$x_1^4 g(\rho_1, \rho_2) = -x_2^4 + 2a_2 x_1^2 x_2^2 + x_1^6 + 2a_4 x_1^4 - a_2^2 x_1^4 + a_4^2 x_1^2$$

$$\text{Substitution } x_1^6 = (x_2^2 - a_2 x_1^2 - a_4 x_1)^2: x_1^4 g(\rho_1, \rho_2) = -2a_4 x_1 x_2^2 + 2a_4 x_1^4 + 2a_2 a_4 x_1^3 + 2a_4^2 x_1^2 = 2a_4 x_1 (-x_2^2 + x_1^3 + a_2 x_1^2 + a_4 x_1) = 0 \in K(C_1)$$

This proves that  $\psi$  is a  $K$ -rational map  $C_1 \rightarrow C_2$ .

By definition of birational equivalence we need to show that  $\phi \circ \psi = id_{C_1}$  and  $\psi \circ \phi = id_{C_2}$ .

Let's start with  $id_{C_1}$ , we want to show that  $\phi \circ \psi$  can be represented as  $(x_1, x_2) \in K(C_1)$ . First coordinate:

$$\frac{\frac{x_1^2 - a_4}{x_1} + \frac{x_2^2}{x_1^2} + b}{2} = \frac{x_1^3 - a_4 x_1 + x_2^2 + x_1^2 b}{2x_1^2}$$

Substitution for  $x_2^2$  in  $K(C_1)$  and using  $b = -a_2$ :

$$\frac{2x_1^3}{2x_1^2} = x_1$$

Second coordinate (again using  $b = -a_2$ ):

$$\frac{\frac{x_2}{x_1} \left( \frac{x_1^2 - a_4}{x_1} + \frac{x_2^2}{x_1^2} - a_2 \right)}{2} = \frac{x_2(x_1^3 - a_4 x_1 + x_2^2 - a_2 x_1^2)}{2x_1^3}$$

Substitution for  $x_2^2$  again:

$$\frac{x_2(2x_1^3)}{2x_1^3} = x_2$$

We have shown that  $\phi \circ \psi = id_{C_1}$  i.e.

Now for  $\psi \circ \phi$ . First coordinate:

$$\frac{\frac{x_1(x_2 + x_1^2 + b)}{2}}{\frac{x_2 + x_1^2 + b}{2}} = \frac{x_1(x_2 + x_1^2 + b)}{x_2 + x_1^2 + b} = x_1$$

Second coordinate:

$$\frac{\left( \frac{x_2 + x_1^2 + b}{2} \right)^2 - a_4}{\frac{x_2 + x_1^2 + b}{2}} = \frac{\frac{x_2^2 + x_1^4 + 2x_1^2 x_2 + 2bx_2 + 2bx_1^2 + b^2 - 4a_4}{4}}{\frac{x_2 + x_1^2 + b}{2}}$$

Using substitution for  $x_1^4$  in  $K(C_2)$  and  $-4a_4 = -b^2 + c$ :

$$\frac{2x_2^2 + 2x_1^2 x_2 + 2bx_2}{2x_2 + 2x_1^2 + 2b} = x_2$$

We have proved that both compositions of those rational maps are identities therefore  $C_1$  and  $C_2$  are birationally equivalent.

□

**Theorem G.4 Proof:** Assume we have  $(a_2, \gamma) \in K \times K$  s.t.  $\gamma^2 \neq 0 \neq a_2^2 - 4\gamma^2$ . Set  $B = \gamma^{-1}$ ,  $A = a_2\gamma^{-1}$ . Since  $\gamma \neq 0$  then also  $\gamma^{-1} = B$  cannot be 0. If  $A^2 = 4$  then  $a_2^2\gamma^{-2} = 4 \iff a_2^2 - 4\gamma \neq 0$  which is a contradiction.

On the other hand if we have  $(A, B) \in K \times K$  s.t.  $B(A^2 - 4) \neq 0$  then set  $\gamma = B^{-1}$  and  $a_2 = AB^{-1}$ . If  $\gamma^2 = 0$  this would imply  $\gamma = 0$  which is a contradiction with  $B \neq 0$ . If  $a_2^2 - 4\gamma^2 = 0 \iff a_2^2 = 4\gamma^2$  this would imply  $\frac{A^2}{B^2} = 4B^{-2} \iff A^2 = 4$  which is again contradiction.

We have therefore proven that G.2 holds.

As in G.3 denote  $f(x_1, x_2) = x_2^2 - x_1^3 - a_2x_1^2 - a_4x_1$ ,  $C_1 = V_f$  and  $g(x_1, x_2) = Bx_2^2 - x_1^3 - Ax_1^2 - x_1$ ,  $C_2 = V_g$ . Denote the rational map  $C_1 \rightarrow C_2$  as  $\psi$  and the rational map  $C_2 \rightarrow C_1$  as  $\phi$ .

First we show that  $\psi$  is a  $K$ -rational map  $C_1 \rightarrow C_2$  using R.6 as in G.3. We want to show  $g(\rho_1, \rho_2) = 0 \in K(C_1)$  where  $(\rho_1, \rho_2) = (\gamma^{-1}x_1 + (f), \gamma^{-1}x_2 + (f))$ . We know that  $\gamma^{-1} = \frac{1}{\sqrt{a_4}}$  and  $a_4 \neq 0$ ,  $B = \frac{1}{\sqrt{a_4}}$ ,  $A = \frac{a_2}{\sqrt{a_4}}$ .

$$g(\rho_1, \rho_2) = \frac{1}{\sqrt{a_4}} \left( \frac{x_2}{\sqrt{a_4}} \right)^2 - \frac{x_1^3}{\sqrt{a_4}^3} - \frac{a_2}{\sqrt{a_4}} \frac{x_1^2}{\sqrt{a_4}^2} - \frac{x_1}{\sqrt{a_4}} = \frac{x_2^2 - x_1^3 - a_2x_1^2 - a_4x_1}{a_4\sqrt{a_4}} = 0$$

Now we want to show  $f(\rho_1, \rho_2) = 0 \in K(C_2)$  where  $(\rho_1, \rho_2) = (B^{-1}x_1 + (g), B^{-1}x_2 + (g))$ . Similarly  $a_4 = \frac{1}{B^2}$  since  $B \neq 0$  and  $a_2 = \frac{A}{B}$ :

$$f(\rho_1, \rho_2) = \frac{x_2^2}{B^2} - \frac{x_1^3}{B^3} - \frac{A}{B} \frac{x_1^2}{B^2} - \frac{1}{B^2} \frac{x_1}{B_1} = \frac{Bx_2^2 - x_1^3 - Ax_1^2 - x_1}{B^3} = 0$$

So  $\psi$  and  $\phi$  are both  $K$ -rational maps. Now as in G.3 we show birational equivalence by proving  $\phi \circ \psi = id_{C_1}$  and  $\psi \circ \phi = id_{C_2}$  which is trivial in this case.

$$\begin{aligned} \phi \circ \psi &= (B^{-1}(Bx_1), B^{-1}(Bx_2)) = (x_1, x_2) \\ \psi \circ \phi &= (\gamma^{-1}(\gamma x_1), \gamma^{-1}(\gamma x_2)) = (x_1, x_2) \end{aligned}$$

□

**Proposition G.5 Proof:** Assume we have  $(a, d) \in K^* \times K^*$ ,  $a \neq d$ . Set  $B = \frac{4}{a-d}$ ,  $A = \frac{2(a+d)}{a-d}$ .  $B \neq 0$  and if  $A = 2$  then this is a contradiction with  $d \neq 0$  and if  $A = -2$  then it is contradiction with  $a \neq 0$ .

On the other hand assume  $(A, B) \in K \times K$  s.t.  $B \neq 0$  and  $A^2 \neq 4$ . Set  $a = \frac{A+2}{B}$  and  $d = \frac{A-2}{B}$ . If  $a = 0$  or  $d = 0$  this is a contradiction with  $A \neq \pm 2 \iff A^2 \neq 4$ . If  $a = d \iff 2 = -2$  which is a contradiction. We have shown that G.3 holds.

Denote the rational map  $C_1 \rightarrow C_2$  as  $\psi$  and the rational map  $C_2 \rightarrow C_1$  as  $\phi$ . First let's prove that  $\psi$  is a rational map.

Theorem G.4 gives us a  $K$ -rational map  $\Psi_1 : C_1 \rightarrow C'$  s.t.  $\Psi_1(x_1, x_2) = (B^{-1}x_1, B^{-1}x_2)$  where  $C' = V_f$  where  $f(x_1, x_2) = x_2^2 - x_1^3 - a_2x_1^2 - a_4x_1$  and  $a_2 = \frac{A}{B}$  and  $a_4 = \frac{1}{B^2}$ . Theorem G.3 gives us a  $K$ -rational map  $\Psi_2 : C' \rightarrow C_2$  where  $\Psi_2(x_1, x_2) = \left( \frac{x_2}{x_1}, \frac{x_1^2 - a_4}{x_1} \right)$ . We can use G.3 because due to the paragraph before G.5 we know that  $C_2$  in G.5 and  $C_2$  in G.3 are equal.

By composition of these 2  $K$ -rational maps we get  $\Psi_2 \circ \Psi_1 = \psi$ . Since  $\Psi_1, \Psi_2$  are  $K$ -rational maps of finite degree (because every  $\rho$  we used in the proofs were transcendental over  $K$ ) we get by Theorem R.9 from the lecture that  $\psi$  is also a  $K$ -rational map  $C_1 \rightarrow C_2$ .



Using similar process theorem G.3 gives us a  $K$ -rational map  $\Phi_1 : C_2 \rightarrow C'$  s.t.  $\Phi_1(x_1, x_2) = \left( \frac{x_2+x_1^2+b}{2}, \frac{x_1(x_2+x_1^2+b)}{2} \right)$  where  $C' = V_g$  where  $g(x_1, x_2) = x_2^2 - x_1^3 - a_2x_1^2 - a_4x_1$  where  $a_2 = -b, a_4 = \frac{b^2-c}{4}$  where (using paragraph above G.5)  $b = \frac{-a-d}{2}, c = ad$  so in total  $a_2 = \frac{a+d}{2}$  and  $a_4 = \frac{(a-d)^2}{16}$ . Theorem G.4 gives us a  $K$ -rational map  $\Phi_2 : C' \rightarrow C_1$  s.t.  $\Phi_2(x_1, x_2) = (Bx_1, Bx_2)$  where in theorem G.4 we have  $A = \frac{a_2}{\sqrt{a_4}}$  and  $B = \frac{1}{\sqrt{a_4}}$ . If we resubstitute we get  $A = \frac{2(a+d)}{a-d}$  and  $B = \frac{4}{a-d}$ .

Again the composition  $\Phi_2 \circ \Phi_1 = \phi$ . Since  $\Phi_2, \Phi_1$  are  $K$ -rational maps of finite degree then  $\phi$  is a  $K$ -rational map  $C_2 \rightarrow C_1$ .

Now we need to show  $\phi \circ \psi = id_{C_1}$  and  $\psi \circ \phi = id_{C_2}$ .

$$\begin{aligned} \phi \circ \psi &= (\Phi_2 \circ \Phi_1) \circ (\Psi_2 \circ \Psi_1) = \Phi_2 \circ (\Phi_1 \circ \Psi_2) \circ \Psi_1 = \Phi_2 \circ id_{C'} \circ \Psi_1 = \\ &= \Phi_2 \circ \Psi_1 = id_{C_1} \end{aligned}$$

We have used Theorem G.3 which states  $\Psi_2 \circ \Psi_1 = id_{C'}$ ,  $\Phi_2 \circ \Psi_1 = id_{C_1}$ . Similarly due to Theorem G.5:

$$\psi \circ \phi = (\Psi_2 \circ \Psi_1) \circ (\Phi_2 \circ \Phi_1) = \Psi_2 \circ id_{C'} \circ \Phi_1 = \Psi_2 \circ \Phi_1 = id_{C_2}$$

We have shown that  $C_1$  and  $C_2$  are birationally equivalent. □

**Lemma W.1 Proof:** Denote  $f(x_1, x_2) = a_1x_1^2 + a_2x_2^2 - 1 - dx_1^2x_2^2 \in K[x_1, x_2]$ . First we will prove  $f$  absolutely irreducible  $\implies d \neq a_1a_2$  and at least one  $a_i \neq 0$ .

Assume  $d = a_1a_2$ . Then  $f(x_1, x_2) = a_1x_1^2 + a_2x_2^2 - 1 - a_1a_2x_1^2x_2^2 = (1 - a_1x_1^2)(-1 + a_2x_2^2)$ . If  $a_1 = 0 = a_2$  then  $f(x_1, x_2) = -1 - dx_1^2x_2^2 = (\sqrt{-d}x_1x_2 - 1)(\sqrt{-d}x_1x_2 + 1) \in \bar{K}[x_1, x_2]$ . This proves the implication.

On the other hand assume  $d \neq a_1a_2$ , at least one  $a_i \neq 0$  and  $f(x_1, x_2) = u(x_1, x_2)v(x_1, x_2)$  where  $u, v \in \bar{K}[x_1, x_2]$ . We have  $2 = \deg_{x_1}(f) = \deg_{x_1}(u) + \deg_{x_1}(v)$  and  $2 = \deg_{x_2}(f) = \deg_{x_2}(u) + \deg_{x_2}(v)$ . We can assume that  $u, v \notin \bar{K}$  because then it would contradict  $f$  reducible in  $\bar{K}[x_1, x_2]$ .

W.l.o.g. we have 4 possibilities:

1.  $\deg_{x_1}(u) = 0, \deg_{x_2}(u) = 1, \deg_{x_1}(v) = 2, \deg_{x_2}(v) = 1$
2.  $\deg_{x_1}(u) = 0, \deg_{x_2}(u) = 2, \deg_{x_1}(v) = 2, \deg_{x_2}(v) = 0$
3.  $\deg_{x_1}(u) = 1, \deg_{x_2}(u) = 0, \deg_{x_1}(v) = 1, \deg_{x_2}(v) = 2$
4.  $\deg_{x_1}(u) = 1, \deg_{x_2}(u) = 1, \deg_{x_1}(v) = 1, \deg_{x_2}(v) = 1$

For each case we will find a contradiction.

Case 1:  $u = ax_2 + b \in \bar{K}[x_2], v = cx_1^2 + ex_1^2x_2 + fx_2 + gx_1 + h \in \bar{K}[x_1, x_2]$ . If we compare the coefficients  $f = uv$  we get conditions:  $bh = -1, bf + ah = 0, af = a_2, bg = 0, ag = 0, bc = a_1, ac + be = 0, ae = -d$ .  $bh = -1 \implies b \neq 0 \neq h, ac + be = 0 \implies e = \frac{-ac}{b}, bc = a_1 \implies c = \frac{a_1}{b} \implies e = \frac{-a_1a}{b^2} \implies ae = \frac{-a_1a^2}{b^2}$ . If  $a_2 = 0 \implies a = 0$  or  $f = 0$  if  $a = 0 \implies -d = 0$  a contradiction. If  $f = 0 \implies bf + ah = ah = 0$  and since  $h \neq 0 \implies a = 0$  again. So we can assume  $a_2 \neq 0 \implies f \neq 0$ . Now  $ae = \frac{-a_1a^2}{b^2} = \frac{-a_1a^2f}{b^2f} = \frac{-a_1a_2a}{b^2f}$ . If  $\frac{a}{b^2f} = 1$  we have  $d = a_1a_2$  a contradiction.  $\frac{a}{b^2f} = \frac{ah}{bbhf} = \frac{-bf}{-bf} = 1$ .

Case 2:  $u = ax_2^2 + bx_2 + c \in \bar{K}[x_2], v = ex_1^2 + fx_1 + g \in \bar{K}[x_1]$ . Again we get conditions:  $cg = -1, bg = 0, ag = a_2, cf = 0, bf = 0, af = 0, ce = a_1, be = 0, ae = -d$ . We know  $c \neq 0 \neq g$  and this gives us  $a = \frac{a_2}{g}, e = \frac{a_1}{c} \implies ae = \frac{a_1a_2}{cg} = -a_1a_2 = -d$  a contradiction.

Case 3:  $u = ax_1 + b \in \bar{K}[x_1], v = cx_2^2 + ex_2^2x_1 + fx_2 + gx_1 + h \in \bar{K}[x_1, x_2]$ . We get:  $bh = -1, bf = 0, bc = a_2, bg + ah = 0, af = 0, ac + be = 0, ag = a_1, ae = -d$ . We have  $b \neq 0 \neq h$ . If  $a_1 = 0$  this would imply  $a = 0$  or  $g = 0$ . If  $a = 0 \implies -d = 0$  a contradiction. If  $g = 0 \implies ah = 0 \implies a = 0$  again a contradiction. Therefore we have  $a = \frac{a_1}{g}$ . Also  $bc = a_2 \iff c = \frac{a_2}{b}$  and  $e = \frac{-ac}{b} \implies e = \frac{-aa_2}{b^2}$ . Together  $ae = \frac{-aa_2a_1}{b^2g}$ . Again we want to show  $\frac{a}{b^2g} = 1$  which is true since  $\frac{a}{b^2g} = \frac{a}{b(-ah)} = \frac{a}{-a(bh)} = 1$ .

Case 4: We know  $\deg_{x_1}(u) = 1 = \deg_{x_1}(v)$ . Consider  $f \in (K[x_2])[x_1] \iff f = x_1^2(a_1 - dx_2^2) + (a_2x_2^2 - 1)$ . Since  $\deg_{x_1}(u) = 1 = \deg_{x_1}(v)$  means that  $f = (a'x_1 + b')(c'x_1 + d') \in (K[x_2])[x_1]$  i.e.  $f$  has roots  $\frac{b'}{a'}, \frac{d'}{c'} \in \bar{K}(x_2)$ .

Since  $f$  is a quadratic polynomial it must be that the discriminant of  $f : D = -4(a_1 - dx_2^2)(a_2x_2^2 - 1)$  is a square in  $\bar{K}(x_2)$  which is equivalent to saying it is a square in  $\bar{K}[x_2]$  since  $D \in \bar{K}[x_2]$ . This means that  $a_1 - dx_2^2$  must have a double root and same for  $a_2x_2^2 - 1$  or they have a common root.

If  $a_1 - dx_2^2$  has a double root then its discriminant is 0  $\iff a_1d = 0$  similarly for  $a_2x_2^2 - 1$  it must be that  $a_2 = 0$ . If  $a_1 \neq 0 \neq a_2$  we have a contradiction. If one  $a_i = 0$  we have also a contradiction since  $d \neq 0$ .

The only possibility left is that they have a common root.  $\pm \frac{\sqrt{da_1}}{d}$  are the roots of the first polynomial and  $\pm \frac{\sqrt{a_2}}{a_2}$  are the roots of the other polynomial. We know that at least one  $a_i$  is non zero. If  $a_1 = 0, a_2 \neq 0$  then obviously they don't have common roots and same goes for  $a_2 = 0, a_1 \neq 0$ . Now we can assume  $a_i$  are both non zero and in that case if we want a common root we get a requirement that  $d = a_1a_2$  which is a contradiction.  $\square$

**Proposition W.2** *Proof:* By lemma Q.1 we know that  $f_1$  is absolutely irreducible since  $a \neq d$  and by lemma W.1 we know that  $f_2$  is absolutely irreducible since  $a \neq d$ .

Denote the  $K$ -rational map from  $C_1 \rightarrow C_2$  as  $\psi$  and the  $K$ -rational map from  $C_2 \rightarrow C_1$  as  $\phi$ . First we show  $\psi$  is a  $K$ -rational map  $C_1 \rightarrow C_2$ . We want to show  $f_2(\rho_1, \rho_2) = 0 \in K(C_1)$  where  $(\rho_1, \rho_2) = \left(\frac{1}{x_1} + (f_1), \frac{x_2}{x_1^2 - d} + (f_1)\right)$ .

$$\begin{aligned} f_2(\rho_1, \rho_2) &= a \frac{1}{x_1^2} + \frac{x_2^2}{(x_1^2 - d)^2} - 1 - d \frac{1}{x_1^2} \frac{x_2^2}{(x_1^2 - d)^2} \\ (x_1^2 - d)^2 x_1^2 f_2(\rho_1, \rho_2) &= a(x_1^2 - d)^2 + x_1^2 x_2^2 - x_1^2 (x_1^2 - d)^2 - dx_2^2 = \\ &= x_1^2 x_2^2 - dx_2^2 - x_1^6 + 2dx_1^4 + ax_1^4 - d^2 x_1^2 - 2adx_1^2 + ad^2 \\ &\text{Substitute for } x_2^2 = x_1^4 - dx_1^2 - ax_1^2 + ad: \\ &\quad -dx_2^2 + dx_1^4 - d^2 x_1^2 - adx_1^2 - ad^2 \\ &\text{Substitute for } x_1^4 = x_2^2 + dx_1^2 + ax_1^2 - ad: \\ &\quad 0 \implies f_2(\rho_1, \rho_2) = 0 \end{aligned}$$

Now we do the same for  $\phi$ . We want to show  $f_1(\rho_1, \rho_2) = 0 \in K(C_2)$  where  $(\rho_1, \rho_2) = \left(\frac{1}{x_1} + (f_2), \frac{x_2(1 - dx_1^2)}{x_1^4} + (f_2)\right)$ .

$$\begin{aligned} f_1(\rho_1, \rho_2) &= \frac{x_2^2(1 - dx_1^2)^2}{x_1^4} - \frac{1}{x_1^4} + \frac{(d + a)}{x_1^2} - ad \\ x_1^4 f_1(\rho_1, \rho_2) &= x_2^2(1 - dx_1^2)^2 - 1 + dx_1^2 + ax_1^2 - adx_1^4 = x_2^2(1 - dx_1^2)^2 - (1 - ax_1^2)(1 - dx_1^2) \\ &\text{As mentioned before W.2 in } K(C_2) \text{ we have } x_2^2(1 - dx_1^2)^2 = (1 - ax_1^2)(1 - dx_1^2) \\ &\implies f_1(\rho_1, \rho_2) = 0 \end{aligned}$$

Now we want to prove  $\phi \circ \psi = id_{C_1}$  and  $\psi \circ \phi = id_{C_2}$ . First coordinate is trivially  $x_1$  in both cases. The second coordinate for  $\phi \circ \psi$ :

$$\frac{\frac{x_2}{x_1^2-d} \left(1 - d \frac{1}{x_1^2}\right)}{\frac{1}{x_1^2}} = \frac{x_1^2 x_2 (1 - \frac{d}{x_1^2})}{x_1^2 - d} = \frac{x_2(x_1^2 - d)}{x_1^2 - d} = x_2$$

And for  $\psi \circ \phi$ :

$$\frac{\frac{x_2(1-dx_1^2)}{x_1^2}}{\frac{1}{x_1^2} - d} = \frac{x_2(1-dx_1^2)}{1-dx_1^2} = x_2$$

This proves that  $C_1$  and  $C_2$  are birationally equivalent.

Since  $f_1, f_2$  are absolutely irreducible (which implies  $f_1, f_2$  irreducible in  $K[x_1, x_2]$ ) and  $C_1, C_2$  are birationally equivalent we can use corollary R.10 from the lecture and we have that  $K(C_1) \cong K(C_2)$ .

If  $a = 0$  then  $f_1(x_1, x_2) = x_2^2 - f(x_1)$  where  $f(x_1) = x_1^2(x_1^2 - d)$ . 0 is a multiple root of  $f$  therefore  $f$  is not separable. Theorem Q.6 states that in this case  $K(C_1)/K$  has genus 0.

If  $a \neq 0$  then  $f$  is separable since its roots are  $\pm\sqrt{a}, \pm\sqrt{d}$  which are distinct since also  $d \neq 0$ . By Q.6 again the genus is 1. Since  $K(C_1)/K$  and  $K(C_2)/K$  are isomorphic their genera coincide. □

**Theorem W.3 Proof:** First assume  $(a, d) \in K^* \times K^*, a \neq d$ . Set  $B = \frac{4}{a-d}, A = 2 + \frac{4d}{a-d}$ . By definition  $B \neq 0$ . If  $A = 2 \implies d = 0$  a contradiction. If  $A = -2 \implies a = 0$  again a contradiction. On the other hand assume  $(A, B) \in K \times K$  s.t.  $B \neq 0$  and  $A^2 \neq 4$ . Set  $d = \frac{A-2}{B}, a = \frac{A+2}{B}$ . If  $a = 0$  or  $d = 0$  contradicts  $A \neq \pm 2$ . If  $a = d$  then we have also a contradiction. This proves (W.2).

Denote the  $K$ -rational map  $C_1 \rightarrow C_2$  as  $\psi$  and the  $K$ -rational map  $C_2 \rightarrow C_1$  as  $\phi$ . We will use similar steps as in the proof of G.5.

First assume we have  $(A, B) \in K \times K, B \neq 0, A^2 \neq 4$ . By applying G.5 we get a  $K$ -rational map  $\Psi_1 : C_1 \rightarrow C'$  s.t.  $\Psi_1(x_1, x_2) = \left(\frac{x_2}{x_1}, \frac{x_1^2-1}{Bx_1}\right)$  where  $C' = V_g, g(x_1, x_2) = x_2^2 - (x_1 - a)(x_1 - d)$  ( $a, d$  given by W.2). Also by using Proposition W.2 we have another  $K$ -rational map  $\Psi_2 : C' \rightarrow C_2$  s.t.  $\Psi_2(x_1, x_2) = \left(\frac{1}{x_1}, \frac{x_2}{x_1^2-d}\right)$ .  $\Psi_1$  and  $\Psi_2$  are  $K$ -rational maps of finite degree so their composition is also a  $K$ -rational map of finite degree. Now we will check that  $\psi = \Psi_2 \circ \Psi_1$ . Using  $d = \frac{A-2}{B}$  we check again the coordinates of the composition of maps. First coordinate:

$$\frac{1}{\frac{x_2}{x_1}} = \frac{x_1}{x_2}$$

And the second:

$$\frac{\frac{x_1^2-1}{Bx_1}}{\frac{x_2^2}{x_1^2} - d} = \frac{\frac{x_1^2-1}{Bx_1}}{\frac{x_2^2}{x_1^2} - \frac{A-2}{B}} = \frac{x_1(x_1^2-1)}{Bx_2^2 - x_1^2(A-2)}$$

Substitute  $Bx_2^2 = x_1^3 + Ax_1^2 + x_1$ :

$$\frac{x_1(x_1-1)(x_1+1)}{x_1^3 + 2x_1^2 + x_1} = \frac{(x_1-1)(x_1+1)}{(x_1+1)^2} = \frac{x_1-1}{x_1+1}$$

We have shown  $\Psi_2 \circ \Psi_1 = \psi$ . Therefore  $\psi$  is a  $K$ -rational map  $C_1 \rightarrow C_2$ .

Now assume we have  $(a, d) \in K^* \times K^*, a \neq d$ . By Proposition W.2 we have a  $K$ -rational map  $\Phi_1 : C_2 \rightarrow C'$  s.t.  $\Phi_1(x_1, x_2) = \left(\frac{1}{x_1}, \frac{x_2(1-dx_1^2)}{x_1^2}\right)$  where  $C' = V_g, g(x_1, x_2) = x_2^2 - (x_1 - a)(x_1 - d)$ . Using theorem G.5 we also have a  $K$ -rational map  $\Phi_2 : C' \rightarrow C_1$  s.t.  $\Phi_2(x_1, x_2) = \left(\frac{2(x_2+x_1^2)-(a+d)}{a-d}, x_1 \frac{2(x_2+x_1^2)-(a+d)}{a-d}\right)$ .  $\Phi_1, \Phi_2$  are  $K$ -rational maps of finite degree and therefore their composition is also a  $K$ -rational map of finite degree.

We will show  $\Phi_2 \circ \Phi_1 = \phi$ . First coordinate:

$$\begin{aligned} \frac{2\left(\frac{x_2(1-dx_1^2)}{x_1^2} + \frac{1}{x_1^2}\right) - a - d}{a - d} &= \frac{ax_1^2 + dx_1^2 - 2 - 2x_2 + 2dx_1^2x_2}{(d-a)x_1^2} \\ \text{Substitute } ax_1^2 - 1 &= dx_1^2x_2^2 - x_2^2: \\ \frac{dx_1^2x_2^2 - x_2^2 - 1 - 2x_2 + dx_1^2 + 2dx_1^2x_2}{dx_1^2 - ax_1^2} &= \frac{(x_2+1)^2(dx_1^2-1)}{dx_1^2 - ax_1^2} \\ \text{Substitute } ax_1^2 &= dx_1^2x_2^2 - x_2^2 + 1: \\ \frac{(x_2+1)^2(dx_1^2-1)}{dx_1^2 - dx_1x_2^2 + x_2^2 - 1} &= \frac{(x_2+1)^2(dx_1^2-1)}{(dx_1^2-1)(-x_2^2+1)} = \frac{(x_2+1)^2}{(1-x_2)(1+x_2)} = \frac{1+x_2}{1-x_2} \end{aligned}$$

Second coordinate is clearly  $\frac{1+x_2}{x_1(1-x_2)}$  since it is the first coordinate multiplied by  $\frac{1}{x_1}$ .

This proves  $\Phi_2 \circ \Phi_1 = \phi$ . Therefore  $\phi$  is a  $K$ -rational map  $C_2 \rightarrow C_1$ .

Now we want to prove the birational equivalence e.g.  $\phi \circ \psi = id_{C_1}$  and  $\psi \circ \phi = id_{C_2}$ . Using the fact that these maps are compositions of maps mentioned and from W.2 we know that  $\Phi_1 \circ \Psi_2 = id_{C'}$  and from G.5 we know  $\Phi_2 \circ \Psi_1 = id_{C_1}$ :

$$\phi \circ \psi = (\Phi_2 \circ \Phi_1) \circ (\Psi_2 \circ \Psi_1) = \Phi_2 \circ (\Phi_1 \circ \Psi_2) \circ \Psi_1 = \Phi_2 \circ id_{C'} \circ \Psi_1 = id_{C_1}$$

Similarly from G.5 we know that  $\Psi_1 \circ \Phi_2 = id_{C'}$  and from W.2 we know  $\Psi_2 \circ \Phi_1 = id_{C_2}$

$$\psi \circ \phi = (\Psi_2 \circ \Psi_1) \circ (\Phi_2 \circ \Phi_1) = \Psi_2 \circ (\Psi_1 \circ \Phi_2) \circ \Phi_1 = \Psi_2 \circ id_{C'} \circ \Phi_1 = id_{C_2}$$

□

**Problem:**