Abstract

Un résumé qui parle d interpolation et de restrictions de choix pour ces interpolations a l aide d un invariant pour les isogenies que l on calcule a l aide des volcans d isogenies.

Proposed notation

This section is for internal reference only: erase after the paper has stabilized.

- $\mathbb{F}_{||}$ is the field we are working on
- ℓ is for the ℓ torsion we are working on
- r is the degree of the isogeny we want to compute
- k is the integer such that $\ell^{2k} > 4r + 1$
- we thus work with a tower which has for top level $F_{q^{\ell^k}}$
- E is for ordinary elliptic curves defined over the finite field $\mathbb{F}_q$
- $\mathcal{O}$ (resp. $\mathcal{O}_x$) is the notation for the endomorphism ring associated (up to isomorphism) to E (resp. E_x)
- K is the notation for the imaginary quadratic field in which $\mathcal{O}$ is defined
- d_K is the negative integer such that $K = \mathbb{Z}[d_K]$

1 Reminder on Couveignes's algorithm

Rappel sur l'algorithme de Couveignes, dire que basiquement il interpole un groupe de points sur un autre, puis fait de la reconstruction rationnelle et teste alors si son résultat est correct, si ce n'est pas le cas il change les groupes et recommence.

2 Reminder on isogeny volcanoes

2.1 Endomorphism, Isogenies

Definition 1. Let E, E' two elliptics curve such that there exists an isogeny $\phi : E \to E'$. If E is separable then $deg(\phi) = ker(\phi)$. For ℓ an integer we call an ℓ isogeny, an isogeny of degree ℓ

Definition 2. A volcano of ℓ isogeny is a graph of ℓ isogenies of degree $\ell + 1$.

Definition 3. For E an ordinary elliptic curve defined over $\mathbb{F}_q$ we denote his endomorphism ring (associated up to isomorphism) by $\mathcal{O}$. $\mathcal{O}$ is an order include in a quadratic imaginary field denoted K, we denote $\mathcal{O}_K$ the algebraic integers of K.

Proposition 4. *Let E and E' two elliptic curves defined over $\mathbb{F}_q$, $\phi : E \to E'$ an ℓ-isogeny, with $\ell \neq p$. Then we can denote $[1, \omega]$ a $\mathbb{Z}$ basis of $\mathcal{O}$. For $f = [\mathcal{O} : \mathcal{O}']$ we can denote $[1, f\omega]$ a $\mathbb{Z}$ basis of $\mathcal{O}'$.*

Lemma 5 (Kohel 1996)**.** *Let E and E' two elliptic curves defined over $\mathbb{F}_q$, $\phi : E \to E'$ an ℓ-isogeny, with $\ell \neq p$. Then*

1. *either $\ell | [\mathcal{O} : \mathcal{O}']$ we say then that ϕ is a descending isogeny,*
2. *either $\ell | [\mathcal{O}' : \mathcal{O}]$ we say then that ϕ is an ascending isogeny,*
3. *either $\mathcal{O} = \mathcal{O}'$ we say then that ϕ is an horizontal isogeny.*

Proof. See Kohel cité les deux résultats en un □

Then we can define a top level in a volcano of ℓ-isogeny, we call it the crater.

2.2 Structure of a volcano

Proposition 6. *Let $\mathbb{F}_q$ be a finite field, let $E(\mathbb{F}_q)[\ell^\infty] = \mathbb{Z}/\ell^{h+j}\mathbb{Z} \times \mathbb{Z}/\ell^h\mathbb{Z}$ with $j \geqslant 0$ and $\nu_\ell(q) > h > 1$ a curve on the crater, then $E(\mathbb{F}_{q^\ell})[\ell^\infty]\mathbb{Z}/\ell^{h+j+1}\mathbb{Z} \times \mathbb{Z}/\ell^{h+1}\mathbb{Z}$*

Proof. See lemme 6.5.2 page 67 of Mireille Fouquet [?], the case $l||g$ with $l = 2$ is not treated but it can be proved with an adapted proof of the one quoted here. + Miret Moreno + These Ionica □

Definition 7. We denote by λ_1, λ_2 the 2 eigenvalues of the Frobenius in $\mathbb{Z}_\ell$ and $h_0 = v_2(\lambda_1 - \lambda_2)$.

Remark 8. We then take $k > h_0$.

We will now try to determine a basis $\langle P, Q \rangle = E[\ell^k]$ such that $\pi(P) = \lambda_1 P$ and $\pi(Q) = \lambda_2 Q$.

Proposition 9. *For λ_1, λ_2 the 2 eigenvalues of the Frobenius and $k > v_2(\lambda_1 - \lambda_2)$, the matrix of the Frobenius action on the ℓ^k torsion is only diagonalisable on a cyclic crater of a volcano of ℓ isogeny.*

Proof. We remind that with the notation from [?] [?] we have $d_\pi = g^2 d_K$, with d_K squarefree such that $K = \mathbb{Z}[\sqrt{d_K}]$ and $g = [\mathcal{O}_K : \mathbb{Z}[\pi]]$.
If we have $\left(\frac{d_K}{\ell}\right) = 1$ then we have $x^2 = d_K \bmod \ell$ who has a solution so the characteristic polynomial of the Frobenius has two roots in $\mathbb{Z}_\ell$. If $\left(\frac{d_K}{\ell}\right) = -1$ then we have $x^2 = d_K \bmod \ell$ who has no solution so the characteristic polynomial of the Frobenius has no roots in $\mathbb{Z}_\ell$. If $\left(\frac{d_K}{\ell}\right) = 0$ thus we have $x^2 = d_K \bmod \ell$ who has the trivial solution so the characteristic polynomial of the Frobenius has a unique root in $\mathbb{Z}_\ell$.
We will thus work with $\left(\frac{d_K}{\ell}\right) = 1$. We are obliged to work in $\mathcal{O}_K$ because the eigenvalues of the Frobenius are not defined in $\ell\mathcal{O}_K$ since $\sqrt{d_K}$ is not. □

3 Computing a horizontal basis

When the contrary is not mentioned we work with E on a cyclic crater of a volcano of ℓ isogeny.

3.1 Computing a diagonalized basis

Algorithm 1 Compute the pre image of Q by the multiplication by ℓ.

Require: Q a point on an elliptic curve $E : y^2 = h(x)$ such that E has a ℓ torsion of rank 2.

Ensure: Q/ℓ such that $\ell(Q/\ell) = Q$

$\langle P_1, P_2\rangle = E[\ell] \leftarrow E$

$\phi_1 \leftarrow \{E \rightarrow {}^{E}/_{P_1} = E_1\}$

$\phi_2 \leftarrow \{E_1 \rightarrow E_1/\phi_1(P_2) = E\}$

$x_1, y_1 \leftarrow \phi_2(x_1, y_1) = Q$

$x_2, y_2 \leftarrow \phi_1(x_2, y_2) = (x_1, y_1)$

return $Q/\ell = (x_2, y_2)$

Proposition 10. *Case $\ell = 2$ Algorithm ?? has a complexity of $O(M(2^k)\log(2^k q))$ operations in $\mathbb{F}_q$ or of $O(M(\sqrt{r})(\log(r) + \log(q)))$ in terms of r.*

Proof $\ell = 2$ The 2-isogeny generated by $Q = E(x_Q, y_Q)$ is given by rational functions according to Velu's formulas, thus the computation of a 2 isogeny from its kernel is done in $O(M(2^k))$ operations in $\mathbb{F}_q$, the bottom line is the inversion which is done with this complexity using Newton Raphson's algorithm. The computational complexity could also be expressed as $O(M(2^k)) = O(M(\sqrt{l}))$.
Computing the 2 torsion points of E is done through the calculation of roots of a trinomial. Since we consider the input curves has a two torsion of rank 2 on $\mathbb{F}_q$ we can do the root computation with Cantor Zassenhauss algorithm in a complexity of $O(\log(q))$ operations in $\mathbb{F}_q$. The computation of a square root is done in $O(M(2^k)\log(2^k q))$ operations in $\mathbb{F}_q$ according to [?], thus we have a computational complexity of $O(M(\sqrt{l})(\log(l)+\log(q)))$

$\ell \neq 2$ We have to factorize two times a polynomial of degree ℓ with coefficients in $\mathbb{F}_{q^{\ell k}}$ and for which Cantor-Zassenhauss algorithm is relevant with a complexity of $O(\ell^k log(q)\ell^2) = O(\sqrt{r} log(q)\ell^2)$ operations on $\mathbb{F}_q$.

□

Proposition 11. *Let $\langle P, Q\rangle = E[\ell^{s-1}]$ such that $\pi(P) = \lambda_1 P, \pi(Q) = \lambda_2 Q$. we denote this by:*

$$M(\pi, P, Q) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \bmod \ell^{s-1}$$

For $P/\ell, Q/\ell$ such that $\ell(P/\ell) = P$ and $\ell(Q/\ell) = Q$ we have

$$M(\pi, P/\ell, Q/\ell) = \begin{pmatrix} \lambda_1 + a\ell^{s-1} & b\ell^{s-1} \\ c\ell^{s-1} & \lambda_2 + d\ell^{s-1} \end{pmatrix} \bmod \ell^s$$

with $\{a, b, c, d\} \in \mathbb{Z}/\ell\mathbb{Z}$. For $s > h$ we denote $\lambda_1 - \lambda_2 = k_0\ell^h \bmod \ell^{h+1}$ with $k_0 \wedge \ell = 1$, $r_1 = \frac{-b}{k_0} \bmod \ell$, $r_2 = \frac{c}{k_0} \bmod \ell$. We are able to diagonalise this matrix with the following change of basis:

$$M(\pi, P/\ell + \ell^{s-1-h} r_1 Q/\ell, Q/\ell + \ell^{s-1-h} r_2 P/\ell) = \begin{pmatrix} \lambda_1 + a\ell^{s-1} & 0 \\ 0 & \lambda_2 + d\ell^{s-1} \end{pmatrix} \bmod \ell^s$$

Proof. Proof omitted for lack of space. □

Definition 12. For $P \in E$ a primitive point of ℓ^i-torsion, $i > 0$ and R a ℓ-division point of P of order ℓ^h:

- Either $\pi(R) = \lambda_1 R$ then we say that P is associated to λ_1,
- or $\pi(R) = \lambda_2 R$ then we say that P is associated to λ_2,
- or $\pi(R) \neq \lambda_1 R$ and $\pi(R) \neq \lambda_2 R$ then we say that P is not associated to λ_1 or λ_2.

Proposition 13. *For P a primitive point of ℓ-torsion on E which is on a cyclic crater, with λ_1, λ_2 the two eigenvalues associated to π, then*

- *Either P is associated to λ_1 then the ℓ-isogeny with kernel P is horizontal,*
- *or P is associated to λ_2 then the ℓ-isogeny with kernel P is horizontal,*
- *or P is not associated to λ_1 or λ_2 then the ℓ-isogeny with kernel P is descending.*

Proof. Let denote by $Es_1 = \{P \in E[\ell^h], \ell^{h-1}P \neq 0, \pi(P) = \lambda_1 P\}$ and $Es_2 = \{P \in E[\ell^h], \ell^{h-1}P \neq 0, \pi(P) = \lambda_2 P\}$ and consider ϕ_1(resp. ϕ_2) the ℓisogeny generated by Es_1 (resp. Es_2), this isogeny is unique since those eigenspace are of dimension 1. We have $[\mathcal{O} : \mathcal{O}_K] \wedge \ell = 1$ since we have a cyclic crater, $\left(\frac{d_K}{\ell}\right) = 1$ then (by Proposition 5.11 of [?]) $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathcal{O}_K$ with $Gal(K/\mathbb{Q})$ such as $\mathfrak{p}_1' = \mathfrak{p}_2$ (by theorem 5.9 of [?]). Since Es_1 and Es_2 are also conjugated with $Gal(K/\mathbb{Q})$ we can associate to the isogeny ϕ_1 (resp. ϕ_2) the integral ideal $\mathfrak{p}_1\mathcal{O}_K$ (resp. $\mathfrak{p}_2\mathcal{O}_K$) and the endomorphism ring $\mathfrak{p}_1^{-1}\mathcal{O}_K$ (resp. $\mathfrak{p}_2^{-1}\mathcal{O}_K$) to their codomain. Since we got $\mathfrak{p}_1\mathfrak{p}_2 = p$. The $\ell - 1$ others ℓ isogenies are those associated to the integral ideals $a\mathfrak{p}_1 + \mathfrak{p}_2$ with $a \wedge \ell = 1$ and to the groups which are generated by a linear combination of point of Es_1 and Es_2. □

Definition 14. Let ϕ be a ℓ^r-isogeny with $r > 0$, we say that ϕ is horizontal if it is composed of only horizontal ℓ-isogenies.

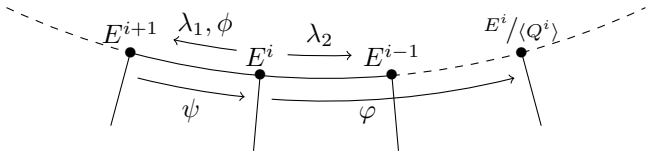


Figure 1: Example for the case $\ell = 2$

Proposition 15. *We denote by E^0 the input curve E of the algorithm located on the cyclic crater of a ℓ-isogenies volcano . For $i \in \mathbb{Z}$, we consider $P \in E^i$ (resp. $Q \in E^i$) a primitive ℓ torsion point associated to λ_1 (resp. λ_2) then the elliptic curve $E^i/\langle P \rangle$ (resp. $E^i/\langle Q \rangle$) is denoted E^{i+1} (resp. E^{i-1}).*

Proof. We have to prove that this notation is well defined, that is $E^{i+1-1} = E^i$. We consider E^i an elliptic curve on the cyclic crater. We denote by P (resp.Q) the ℓ torsion point associated to λ_1 (resp. λ_2), we consider $\phi : E^i \to E^i/\langle P \rangle = E^{i+1}$. On E^{i+1} we denote by Q' the ℓ-torsion point associated to λ_2, then the ℓ-isogeny $\psi : E^i/\langle P \rangle = E^{i+1} \to E^{i+1}/\langle Q' \rangle$ is horizontal by the fact that Q' is associated to λ_2 by 12. The kernel of ψ is $\phi(Q)$ since $\phi(Q)$ is also associated to λ_2, thus we have the composition of ϕ and ψ who annihilates the ℓ torsion of E^i which permits us to conclude that ψ is the dual of ϕ thus that $E^{i+1-1} = E^i$. In a similar way we prove that $E^{i-1+1} = E^i$ □

Proposition 16. *Let E^i be an elliptic curve over a cyclic crater of a volcano of ℓ-isogenies, we consider a primitive ℓ^j torsion point $Q^i \in E^i$ such that $\varphi : E^i \to E^i/\langle Q^i \rangle$ is a horizontal isogeny, we denote V a division point of Q_i of order ℓ^{j+h} such that $\pi(V) = \lambda_2 V$, P a primitive ℓ-torsion point associated to λ_1, ϕ the isogeny: $E^i \to E^{i+1} = E^i/\langle P \rangle$. For R a ℓ division point of Q^i we have $\phi(R)$ such that $E^{i+1} \to E^{i+1}/\langle \phi(R) \rangle$ is a horizontal isogeny and there exists a division point W of $\phi(R)$ of order ℓ^{j+h+1} such that $\pi(W) = \lambda_2 W$.*

Proof. We will first prove that the isogeny $E^{i+1} \to E^{i+1}/\phi(R)$ is horizontal and associated to λ_2.
Since $\ell^j \phi(R) = \phi(\ell^{j-1} Q^i)$ and Q^i is associated to λ_2 then the ℓ-isogeny ψ with kernel $\ell^j \phi(R)$ is the dual isogeny of ϕ because it is the one who anhiliates the ℓ-torsion (here $\langle P, \ell^{j-1} Q^i \rangle$) together with ϕ on E^i. Thus we have proved that ψ is associated to λ_2 and horizontal.
Since we have $\psi(\phi(R)) = Q^i$, this tells us that the isogeny Υ with kernel $\phi(R)$ is the composition of ψ with the isogeny φ of kernel $\langle Q^i \rangle$. Thus the isogeny Υ is horizontal of degree ℓ^{j+1} and associated to λ_2.
Let W a point of order ℓ^{h+j+1} such that $\ell^h W = \phi(R)$, let T a point such that $\phi(T) = W$. From $\ell^h \phi(T) = \phi(R)$ we deduce that $\ell^{h+1} T = Q^i$ and that T is of order ℓ^{j+h+1}. Let denote $\widehat{\phi}$ the dual isogeny of ϕ, since W is a division point of $\phi(Q^i)$, $\widehat{\phi}$ is the ℓ isogeny generated by $\ell^{h+j} W = \ell^j \phi(R) = \ell^{j-1} \phi(Q)$. As $\ell^h \widehat{\phi(W)} = \ell^h \widehat{\phi}(\phi(T)) = \ell^{h+1} T = Q^i$, thus by hypothesis we

have $\pi(\widehat{\phi}(W)) = \lambda_2\widehat{\phi}(W)$. Moreover we have $\widehat{\phi}(\phi(T)) = \widehat{\phi}(W)$ this implies that $\pi(\ell T) = \pi(\widehat{\phi}(W)) = \lambda_2\widehat{\phi}(W) = \lambda_2(\ell T)$. Thus we have for T: $\pi(T) = \lambda_2 T + P$ with a ℓ torsion point P associated to the "eigenspace" of λ_1. Then with the action of ϕ associated to λ_1 we have $\pi(\phi(T)) = \pi(W) = \lambda_2\phi(T) = \lambda_2 W$. □

Proposition 17. *Let Q be a point of ℓ^j torsion with $j > 0$ then there exists a division point R of Q of order ℓ^{h+j} with $\pi(R) = \lambda_2 R$ if and only if the ℓ^j isogeny with kernel $\langle Q\rangle$ is horizontal.*

Proof. In 15, the $\Leftarrow$ has been proved. Now we will prove the other way.
We do a recursive proof. The initial step is the conjecture 12.
Recursive step: we consider that the property is true to the rank $j > 1$, then we will have to prove it for $j+1$. We consider then S a point of order ℓ^{j+1} with T a division point of S of order ℓ^{h+1+j} with $\pi(T) = \lambda_2 T$.We know that the ℓ^j isogeny ϕ generated by $\langle \ell S\rangle$ is horizontal and associated to λ_2. We then have $\phi(S)$ a point of order ℓ and $\phi(T)$ a point of order ℓ^{h+1} with $\pi(\phi(T)) = \lambda_2\phi(T)$. Thus by applying the conjecture 12 we have the isogeny ψ with kernel $\langle\phi(S)\rangle$ horizontal, therefore the isogeny with kernel $\langle S\rangle$ who is equal to the composition of ψ with ϕ is horizontal. □

Proposition 18. *For ϕ: $E \to E'$ a r-isogeny with $r \wedge \ell = 1$ an odd prime, and P a ℓ^i primitive torsion point, with $i > 0$ such that $E \to E/\langle P\rangle$ is horizontal and P is associated to λ_1. Then the isogeny $E' \to E'/\langle\phi(P)\rangle$ is also horizontal.*

Proof. We just have to prove that there exists a ℓ^{h+i} primitive torsion point V dividing $\phi(P)$ such that $\pi(V) = \lambda_1 P$. Since P is a point that generates a horizontal isogeny then there exists a point R of order ℓ^{h+i} dividing P. Since ϕ is a r isogeny then ϕ doesn't change the order of P and R, moreover the frobenius commutes with ϕ (because this one is defined on $\mathbb{F}_q$) then we have $\pi(\phi(R)) = \lambda_1\phi(R)$ which proves the assertion. □

We have thus proved that the image of a ℓ horizontal basis by an r isogeny with $r \wedge \ell = 1$ is still an ℓ horizontal basis. Now we will show how to extend this result for curves not on the crater.

Definition 19. Let ℓ an integer we denote by $C(\ell) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = \ell, a > 0, 0 \leqslant b < d, gcd(a,b,d) = 1\}$

Lemma 20. *Let consider E an elliptic curve defined on $\mathbb{C}$ such that E is not at the crater of the volcano of ℓ-isogeny. We consider the $\mathbb{Z}$ lattice associated (up to isomorphism) to $E : [1,\tau]$. The ascending ℓ-isogeny is the one associated to $M = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ with $M \in C(\ell)$*

Proof. Let consider E_1 on $\mathbb{C}$, we denote by $[1,\tau_1]$ the lattice associated to E_1. For $\sigma \in C(\ell)$, $d[1,\sigma\tau_1]$ is the lattice associated to an ℓ isogenous curve of E_1 (see Theorem 11.23 and Lemma 11.24 [?]).
We consider a $\mathbb{Z}$-basis of the endomorphism ring $[1,\omega_1]$ associated to the elliptic

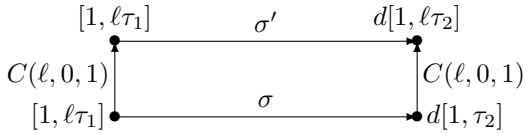
curve $[1, \tau_1]$ since we are not on the crater of the volcano we know that $\ell | \omega_1$.
Let's consider ℓ-isogenous curves of E_1, they are associated to lattices $\ell[1, \frac{\tau_1+k}{\ell}]$ with $k \in [0..\ell-1]$ and the lattice $[1, \ell\tau_1]$. Now we consider $\alpha \in End([1, \tau_1])$ such that $f\mathcal{O}_K = \mathbb{Z}[\alpha]$ we can express $\alpha = a + b\tau_1$ with $a, b \in \mathbb{Z}, a \wedge b = 1$. From the work of Kohel [**?**] we know that α will be included in only one of the ℓ isogenous curve.

1. $\alpha \in \mathsf{End}(\ell[1, \frac{\tau_1+k}{\ell}])$ is equivalent to $\ell | (a - kb)$,
2. $\alpha \in End([1, \ell\tau_1])$ is equivalent to $\ell | b$.

Thus if we have α who belongs to two different sets of $End(\ell[1, \frac{\tau_1+k}{\ell}]), k \in [0..\ell-1] \bigcup End([1, \ell\tau_1])$ then it should belong to all of them. However we know that $\alpha = \ell\alpha'$ since we are not on the crater of the volcano thus the imaginary part of α is divisible by ℓ thus b is divisible by ℓ.
Since we obtain $[1, \ell\tau_1]$ by acting with the matrix $C(\ell, 0, 1) = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ we can conclude. □

Proposition 21. *Let consider E_1 and E_2 two elliptic curve r-isogenous not on the crater of ℓ isogeny volcano with r prime different from ℓ, we denote by E_{1c} (resp. E_{2c}) the elliptic on the crater of the ℓ isogeny volcano of E_1 (resp. E_2) obtained by a composition of only ℓ ascending isogeny. Then E_{1c} and E_{2c} are also r-isogenous.*

Proof. We first consider E_{1u} and E_{2u} curves which are ℓ isogenous to E_1 and E_2 and 1 level above in the volcano, we prove then that E_{1u} and E_{2u} are also r isogenous.
Let consider τ_1 (resp. τ_2) such that $[1, \tau_1]$ (resp. $d[1, \tau_2]$) is associated to E_1 (resp. E_2), with τ_2 such that $\tau_2 = \frac{a\tau_1+b}{d}$ and $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ in $C(r)$.
We denote $C(\ell, 0, 1) = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \in C(\ell)$
By the previous lemma we have the curve E_{1u} associated to $[1, C(\ell, 0, 1)\tau_1]$ and the curve E_{2u} associated to $d[1, C(\ell, 0, 1)\tau_2]$. We want to prove that there exists $\sigma' \in C(r)$ such that $C(\ell, 0, 1)\tau_2 = \sigma' C(\ell, 0, 1)\tau_1$, thus by Theorem 11.23 and Lemma 11.24 of [**?**] we can then conclude that the curve E_{1u} associated to $[1, C(\ell, 0, 1)\tau_1]$ is r isogenous to the curve E_{2u} associated to $d[1, C(\ell, 0, 1)\tau_2]$.
We have $C(\ell, 0, 1)\tau_2 = \frac{\ell a\tau_1+\ell b}{d}$, since $\forall k \in \mathbb{N}\ [1, \frac{\ell a\tau_1+\ell b}{d}] = [1, \frac{\ell a\tau_1+\ell b-kd}{d}]$ we can consider that we have $0 \leqslant \ell b < d$. Let's consider $\sigma' \in C(r)$ then we have $\sigma'(\ell\tau_1) = \frac{a'\ell\tau_1+b'}{d'}$ thus to have $\frac{a'\ell\tau_1+b'}{d'} = \frac{\ell a\tau_1+\ell b}{d}$ we take $a' = a, b' = \ell b, d' = d$ wich defines us $\sigma' \in C(r)$. We can recap this proof in the following commutative diagram :



We can then conclude recursively to obtain the result for curves on the crater. □

Citer les algorithmes de Fouquet-Morain et Ionica-Joux ainsi que Miret-Moreno concernant

Cette partie doit contenir en parallèle de ces définitions et propriétés les algorithmes associés et leurs complexités

4 Interpolating the two bases

Dire que là à l'image de ce qui a été fait par Enge et Morain puis par Luca on va se servir de l'action du Frobenius pour accélérer le calcul de polynomes d'interpolations. Il faut donc avant tout cela faire une introduction des objets que l'on va utiliser.

Definition 22. Let $E(\mathbb{F}_{q^{2^k}})[2^\infty] = \mathbb{Z}/2^{k+j+h}\mathbb{Z} \times \mathbb{Z}/2^{k+h}\mathbb{Z}$ with $j \geqslant 1$, $1 \leqslant h \leqslant \nu_2(q-1)$, we denote by o_{λ_1} and $o_{\lambda 2}$ the multiplicative order of the eigenvaluesλ_1, λ_2 of the Frobenius for the 2^{k+h} torsion defined on the extension field $\mathbb{F}_{q^{2^k}}$.

Proposition 23. $\max(o_{\lambda_1}, o_{\lambda_2}) = 2^k$ *and* $\min(o_{\lambda_1}, o_{\lambda_2}) = 2^{k-j}$

Proof. Let consider a point P of order 2^{k+h} associated to $\max(o_{\lambda_1}, o_{\lambda_2})$, then we will have by definition of o_{λ_1} and o_{λ_2}: $\pi(P)^{\max(o_{\lambda_1}, o_{\lambda_2})} = P$, as P is a point of order 2^{k+h} by the proposition 6 he is defined at least in $\mathbb{F}_{q^{2^{k-j}}}$ and at most in $\mathbb{F}_{q^{2^k}}$ thus we have the results. □