Barcelona University UPC January 2005

Curves over finite fields

By
Christophe RITZENTHALER

These are notes of a course taught at UPC in Barcelona in January 2005. They can be found on `www.math.jussieu.fr/~ritzenth`.
Please send comments and corrections to me at `ritzenth@math.jussieu.fr`.

Conventions.
All fields are assumed perfect.
In the following and unless expressly mentioned a curve will always be a projective smooth absolutely irreducible variety of dimension 1 over a field K.
We will try to keep the notation k for a field of characteristic $p > 0$ (mostly $\mathbb{F}_q$ with q a power of p or an algebraic closed field) and K for any field.
The number l will always be a prime different from the characteristic p of K.

Contents

Chapter 1

Zeta functions of curves over finite fields

1.1 Introduction

We are going to study curves over finite fields. That has two important specificities that we can roughly express as :

1. We are working in characteristic $p \neq 0$: there is no Lefschetz principle to say 'let's say we're working on $\mathbb{C}$'.
2. We can obtain quantitative information because 'things are finite'.

To be a bit more precise, we gather here good and bad aspects of the domain.
Geometry :

- Inseparable morphisms. Here the theory of scheme shows its whole power. For instance if E/k is an elliptic curve, consider the kernel of the map $[m]$. We have $|E[l](\overline{k})| = l^2$ but $|E[p](\overline{k})| = p$ or 1. Looking at $E[p]$ as a scheme one can get back the 'missing points' : indeed in the first case $E[p] = (\mathbb{Z}/p\mathbb{Z}) \times \mu_p$ where $\mu_p = \mathrm{Spec}k[T]/(T^p - 1)$ and in the second case $E[p] = \alpha_p^2$ where $\alpha_p = \mathrm{Spec}k[T]/T^p$. Both last schemes are groups schemes whose underlying set has a single point but with 'multiplicity' p. We will try however to avoid speaking about these difficult notions.
- Differentials : all the problem is that the derivative of x^p is 0. Example of problems : the Hessian of a plane quartic is 0 in characteristic $2, 3$. So we cannot determine easily the flexes (and in fact their behavior is special).
- We cannot apply transcendental methods (or the constructions are much harder). For instance, the description of the fundamental group by loops, the description of abelian varieties as tori.
- Fortunately a lot of things remain true or have direct generalizations : Riemann-Roch theorem, Jacobian ,...

Arithmetic :

- Finite fields are much easier than number fields. As a trivial example, an extension is completely characterized by its degree. Then, actually to study global questions one first has to understand the local question.
- We can compute things : for example there is only a finite number of curves of a given genus up to isomorphism over a fixed finite fields. So if one wants to prove something by brute force attack in such a situation it is (sometimes) possible. It is also easier to construct examples and to test conjectures. One understands why computer softwares play a big role in this area.
- Curves over finite fields and number fields have an exact dictionary. This is a part of it :

$$\begin{array}{ccc} \text{Number fields} & & \text{Algebraic curves} \\ \text{place} & & \text{point} \\ \text{degree} & & \text{number of points} \\ \log|\text{discrim}| & \Longleftrightarrow & \text{genre} \\ \text{class group} & & \text{Jacobian} \end{array}$$

  So more or less when we are studying curves, we are studying number fields. Thus curves over finite fields should be simpler than curves over number fields. In a certain sense, they are even easier than number fields : a lot of conjectures are proved for curves and remain open for number fields (Riemann conjecture).

The main object associated to curves (and to number fields) is the Zeta function. It contains in particular the number of points of the curve over any extension. Zeta functions contain also geometric information. The relations between geometry and arithmetic through this function will be the red line of this part.

Acknowledgments. The results presented in this part are mostly issued of [Sil92] for elliptic curves and [Mil98] for abelian varieties.

1.2 Zeta function of curves over finite fields

In 1949, André Weil made a series of very general conjectures concerning the number of points on varieties defined over finite fields. We restrict to the case of curves.
Let $k = \mathbb{F}_q$ and for all $n \geq 1$, let k_n be the extension of degree n of k. Let C/k be a (projective smooth) curve of genus g over k.

Definition 1.2.1. *The* Zeta function *of C over k is the power series*

$$Z(C/k;T) = \exp\left(\sum_{n=1}^{\infty} |C(k_n)| \frac{T^n}{n}\right).$$

Theorem 1.2.1 (Weil conjectures). *With the above notations, we have the following properties.*

1. *Rationality :*
$$Z(C/k;T) \in \mathbb{Q}(T).$$
2. *Functional equation :*
$$Z(C/k;1/(qT)) = (qT^2)^{1-g} Z(C/k;T).$$
3. *Riemann hypothesis :*
there exists a polynomial $f \in \mathbb{Z}[T]$ of degree $2g$ such that
$$f(T) = \prod_{i=1}^{2g} (1 - T\alpha_i)$$
with $|\alpha_i| = \sqrt{q}$ for all i and such that
$$Z(C/k;T) = \frac{f(T)}{(1-T)(1-qT)}.$$

Corollary 1.2.1. *We have $|C(\mathbb{F}_{q^n})| = 1 + q^n - \sum_{i=1}^{2g} \alpha_i^n$.*

Proof. We have

$$\begin{aligned} \log(Z(C/k;T) = \sum |C(k_n)|T^n/n &= \log(f(T)) - \log(1-T) - log(1-qT) \\ &= \sum \log(1-\alpha_i T) + \sum T^n/n + \sum q^n T^n/n \\ &= \sum_n \left(-\sum_i (\alpha_i^n) + 1 + q^n \right) T^n/n \end{aligned}$$

□

Example 1. *Consider the elliptic curve : $E/\mathbb{F}_7 : y^2 = x^3 + 2$. It has 9 rational points, namely $(0:1:0), (0:3:1), (0:4:1), (3:1:1), (3:6:1), (5:1:1), (5:6:1), (6:1:1), (6:6:1)$. So we must have*

$$Z(E/\mathbb{F}_7;T) = \frac{7T^2 + T + 1}{(1-T)(1-7T)}.$$

In particular the number of points of $E/\mathbb{F}_{49}$ is $1 + 49 - (1^2 - 2 \cdot 7) = 63$ (which can be checked with a computer).

These conjectures were solved by Weil (in the case of curves and abelian varieties). The general case was solved by Deligne in 1973.
The first case $g = 0$ can be done by hand : indeed $|\mathbb{P}^1(k_n)| = q^n + 1$ so

$$Z(\mathbb{P}^1/k;T) = \exp(-\log(1-T) - \log(1-qT)) = \frac{1}{(1-T)(1-qT)}.$$

Now a genus 0 curve C/k is always k-isomorphic to a non degenerate plane conic. Chevalley's theorem shows then that this conic has always a rational point so in fact C is also k-isomorphic to $\mathbb{P}^1$.
The next case, $g = 1$, is the case of elliptic curves. We will prove it in details in the next section. Indeed, a lot of the ideas to attack the general cases are already used there. We will not however give all details for the general proof. In particular the cohomological material will be some kind of black box that we will use without explicit description (see 5.2.4).

1.2.1 The case of elliptic curves

Tate module

Let E/K be an elliptic curve and $m \geq 2$ be an integer prime to the characteristic of K. We know that

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

this isomorphism being one between abstract groups. However the group $E[m]$ comes equipped with more structure. Namely, each element of the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$. We thus obtain a representation

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

This representation is not completely satisfactory because it is generally easier to deal with representations whose matrices have coefficients in a ring of characteristic 0. What we will do is to fit them together :

Definition 1.2.2. *Let E be an elliptic curve and $l \in \mathbb{Z}$ a prime. The (l-adic) Tate module of E is the group*

$$T_l(E) = \varprojlim_n E[l^n],$$

the inverse limit being taken with respect to the natural maps

$$[l] : E[l^{n+1}] \to E[l^n].$$

Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_l$-module.

Proposition 1.2.1. *As a $\mathbb{Z}_l$-module $T_l(E) \simeq \mathbb{Z}_l \times \mathbb{Z}_l$.*

Now the action of $\mathrm{Gal}(\overline{K}/K)$ on each $E[l^n]$ commutes with the multiplication by $[l]$ maps used to form the inverse limit, so $\mathrm{Gal}(\overline{K}/K)$ also acts on $T_l(E)$.

Definition 1.2.3. *The l-adic representation (of $Gal(\overline{K}/K)$ on E), denoted ρ_l, is the map*

$$\rho_l : Gal(\overline{K}/K) \to Aut(T_l(E)).$$

The Tate module is also a useful tool for studying isogenies. If

$$\phi : E_1 \to E_2$$

is an isogeny then it induces a map

$$\phi_l : T_l(E_1) \to T_l(E_2).$$

We thus obtain a homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_l(E_1), T_l(E_2)).$$

It is not hard to show that the above homomorphism is injective (see Prop.1.2.6), but we need the stronger result.

Theorem 1.2.2. *Let E_1 and E_2 be elliptic curves. Then the natural map*

$$\begin{array}{rcl} Hom(E_1, E_2) \otimes \mathbb{Z}_l & \to & Hom(T_l(E_1), T_l(E_2)) \\ \phi & \mapsto & \phi_l \end{array}$$

is injective.

Proof. We start by proving the following statement. Let $M \subset \mathrm{Hom}(E_1, E_2)$ be a finitely generated subgroup and let

$$M^{\mathrm{div}} = \{\phi \in \mathrm{Hom}(E_1, E_2) : [m] \circ \phi \in M \text{ for some integer } m \geq 1\}.$$

Then M^{div} is finitely generated.
To prove this, we extend the degree mapping to the finite dimensional real vector space $M \otimes \mathbb{R}$, which we equip with the natural topology inherited from $\mathbb{R}$. Then the degree mapping is clearly continuous, so the set

$$U = \{\phi \in M \otimes \mathbb{R}, \deg \phi < 1\}$$

is an open neighborhood of 0. Further, since $\mathrm{Hom}(E_1, E_2)$ is torsion-free [Sil92, III.4.2b], there is a natural inclusion

$$M^{\mathrm{div}} \subset M \otimes \mathbb{R}$$

and clearly

$$M^{\mathrm{div}} \cap U = \{0\},$$

since every non-zero isogeny has degree at least 1. Hence M^{div} is a discrete subgroup of the finite dimensional vector space $M \otimes \mathbb{R}$, so it is finitely generated.

We turn now to the proof of the theorem. Let $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l$ and suppose that $\phi_l = 0$. Let

$$M \subset \mathrm{Hom}(E_1, E_2)$$

be a finitely generated subgroup so that $\phi \in M \otimes \mathbb{Z}_l$. Then with the notation above M^{div} is finitely generated, so it is also free (since it is torsion-free). Let $\phi_1, \dots \phi_t$ be a basis of M^{div} and write

$$\phi = \alpha_1\phi_1 + \ldots + \alpha_t\phi_t \text{ with } \alpha_i \in \mathbb{Z}_l.$$

Now choose $a_1, \ldots, a_t \in \mathbb{Z}$ so that $a_i \equiv \alpha_i \pmod{l^n}$. Then the fact that $\phi_l = 0$ implies that the isogeny

$$\psi = [a_1]\phi_1 + \ldots + [a_t]\phi_t$$

annihilate $E_1[l^n]$. It follows that ψ factors through $[l^n]$ so there is an isogeny

$$\lambda \in \mathrm{Hom}(E_1, E_2) \text{ with } \psi = [l^n]\lambda.$$

Further, λ is in M^{div} so there are integers $b_i \in \mathbb{Z}$ such that

$$\lambda = [b_1]\phi_1 + \ldots + [b_t]\phi_t.$$

Then since the ϕ_i's form a $\mathbb{Z}$-basis of M^{div}, we have

$$a_i = l^n b_i$$

hence $\alpha_i \equiv 0 \pmod{l^n}$. Since this holds for all n, it follows that all $\alpha_i = 0$, so $\phi = 0$. $\square$

Remark 1. Be careful : this result cannot be obtained merely by tensoring with $\mathbb{Z}_l$ on the left : indeed we get only that $\mathrm{End}(E_1, E_2) \otimes \mathbb{Z}_l \hookrightarrow M_2(\mathbb{Z}_l) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and this last one is much bigger than $M_2(\mathbb{Z}_l)$.

Corollary 1.2.2. *Let E_1 and E_2 be elliptic curves. Then $Hom(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most* 4.

Proof. Since $\mathrm{Hom}(E_1, E_2)$ is torsion-free, it follows that

$$\mathrm{rank}_{\mathbb{Z}}\mathrm{Hom}(E_1, E_2) = \mathrm{rank}_{\mathbb{Z}_l}(\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l).$$

Now we have the estimate

$$\mathrm{rank}_{\mathbb{Z}_l}\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \leq \mathrm{rank}_{\mathbb{Z}_l}\mathrm{Hom}(T_l(E_1), T_l(E_2)).$$

After having chosen bases we see that

$$\mathrm{Hom}(T_l(E_1), T_l(E_2)) \simeq M_2(\mathbb{Z}_l),$$

which gives the result. $\square$

Remark 2. By definition an isogeny is defined over K if it commutes with the action of $\mathrm{Gal}(\overline{K}/K)$. Similarly, we can define

$$\mathrm{Hom}_K(T_l(E_1), T_l(E_2)) := \mathrm{Hom}(T_l(E_1), T_l(E_2))^{\mathrm{Gal}(\overline{K}/K)}.$$

Then if K is a finite field (or a number field (Faltings)) we have that the natural map

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}_K(T_l(E_1), T_l(E_2))$$

is an isomorphism. This is an important theorem, valid for any abelian variety as we will see in 1.4.

Weil pairing

We want to add structure on the Tate module. This is achieved by the Weil pairing.
Let E/K be an elliptic curve. We fix $m \geq 2$ prime to the characteristic of K.
Let $T \in E[m]$. Then there is a function $f \in \overline{K}(E)$ such that $\mathrm{div}(f) = m(T) - m(O)$.
Letting $T' \in E$ with $[m]T' = T$, there is $g \in \overline{K}(E)$ such that

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$$

(indeed, the degree of the divisor is 0 and $\sum (T' + R) - (R) = \sum T' = m^2 T' = mT = O$ in E).
One verifies that the functions g^m and $f \circ [m]$ have the same divisor :

$$\mathrm{div}(f \circ [m]) = \mathrm{div}([m]^* f) = [m]^* \mathrm{div}(f) = [m]^*(m(T) - m(O)) = m[m]^*((T) - (O)) = \mathrm{div}(g^m).$$

So up to a scalar, $f \circ [m] = g^m$.
Now suppose that $S \in E[m]$, then for any point $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Hence we can define a pairing

$$\overline{e}_m : E[m] \times E[m] \to \mu_m$$

by setting

$$\overline{e}_m(S, T) = g(X + S)/g(X).$$

This pairing is called the *Weil pairing.*

Proposition 1.2.2 ([Sil92, III.8.1]). *The Weil pairing is :*

1. *bilinear :* $\overline{e}_m(S_1 + S_2, T) = \overline{e}_m(S_1, T)\overline{e}_m(S_2, T)$ *and* $\overline{e}_m(S, T_1 + T_2) = \overline{e}_m(S, T_1)\overline{e}_m(S, T_2)$.

2. *alternating :* $\overline{e}_m(S, T) = \overline{e}_m(T, S)^{-1}$.

3. *non-degenerate : if $\overline{e}_m(S,T) = 1$ for all $S \in E[m]$, then $T = 0$.*
4. *Galois-invariant : for all $\sigma \in Gal(\overline{K}/K)$,*
$$\overline{e}_m(S,T)^\sigma = \overline{e}_m(S^\sigma, T^\sigma).$$
5. *compatible : if $S \in E[mm']$ and $T \in E[m]$ then*
$$\overline{e}_{mm'}(S,T) = \overline{e}_m([m']S,T).$$

Corollary 1.2.3. *If $E[m] \subset E(K)$ then $\mu_m \subset K^*$.*

Proof. The image of $\overline{e}_m(S,T)$ as S,T range over $E[m]$ is a subgroup of μ_m, say equal to μ_d. It follows that for all $S,T \in E[m]$,
$$1 = \overline{e}_m(S,T)^d = \overline{e}_m([d]S,T).$$
The non-degeneracy of $\overline{e}_m$ implies that $[d]S = O$, ans since S is arbitrary, we must have $d = m$. Finally if $E[m] \subset E(K)$ then from the Galois invariance of the $\overline{e}_m$ pairing we see that $\overline{e}_m(S,T) \in K^*$ for all S,T. Therefore $\mu_m \subset K^*$. □

The Weil pairing has also a nice interpretation with respect to the dual.

Proposition 1.2.3. *Let $S \in E_1[m], T \in E_2[m]$ and $\phi : E_1 \to E_2$ be an isogeny. Then*
$$\overline{e}_m(S, \hat{\phi}(T)) = \overline{e}_m(\phi(S),T).$$

Proof. Let $\mathrm{div}(f) = m(T) - m(O)$ and $f \circ [m] = g^m$ be as above. Then
$$\overline{e}_m(\phi(S),T) = g(X + \phi(S))/g(X).$$
Choose a function $h \in \overline{K}(E)$ so that
$$\phi^*(T) - \phi^*(O) = \hat{\phi}(T) - (O) + \mathrm{div}(h).$$
Such a function exists because $\hat{\phi}(T)$ is precisely the sum of the points of the divisor of the left-hand side of the equality ([Sil92, III.6.1]). Now
$$\mathrm{div}\left(\frac{f\phi}{h^m}\right) = \phi^*\mathrm{div}(f) - m\mathrm{div}(h) = m(\hat{\phi}(T)) - m(O)$$
and
$$\left(\frac{g\phi}{h[m]}\right)^m = \frac{f[m]\phi}{(h[m])^m} = \left(\frac{f\phi}{h^m}\right)[m].$$
Thus from the definition of $\overline{e}_m$
$$\begin{aligned}
\overline{e}_m(S, \hat{\phi}(T)) &= \frac{(g \circ \phi/h \circ [m])(X+S)}{(g \circ \phi/h \circ [m])(X)} \\
&= \frac{g(\phi(X) + \phi(S))}{g(\phi(X))}\frac{h([m]X)}{h([m]X + [m]S)} \\
&= \overline{e}_m(\phi S, T).
\end{aligned}$$
□

Let l be a prime different from the characteristic of K. We would like to fit together the pairings

$$\overline{e}_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$$

for all n to give an l-adic Weil pairing on the Tate module

$$e_l : T_l(E) \times T_l(E) \to T_l(\mu)$$

where

$$T_l(\mu) = \varprojlim_{n} \mu_{l^n} \simeq \mathbb{Z}_l.$$

We need only to check the compatibility

$$\overline{e}_{l^{n+1}}(S,T)^l = \overline{e}_{l^n}([l]S,[l]T)$$

which follows from Prop.1.2.2 (1) and (5).

Proposition 1.2.4. *There exists a bilinear, alternating, non-degenerate, Galois invariant pairing*

$$e_l : T_l(E) \times T_l(E) \to T_l(\mu)$$

such that if $\phi : E_1 \to E_2$ is an isogeny, ϕ and $\hat{\phi}$ are adjoints for the pairing.

Weil conjectures : $g = 1$

Theorem 1.2.3. *Let k be a field with q elements and E/k be an elliptic curve. Then there is an $a \in \mathbb{Z}$ so that*

$$Z(E/k;T) = \frac{1 - aT + qT}{(1-T)(1-qT)}$$

Further $Z(E:k;1/qT) = Z(E/k;T)$ and

$$1 - aT + qT^2 = (1-\alpha T)(1-\beta T) \textit{ with } |\alpha| = |\beta| = \sqrt{q}.$$

Corollary 1.2.4. *With the notations above, there exists a polynomial (called the* Frobenius polynomial *of E/k)*

$$\chi := T^2 - aT + q = (T-\alpha)(T-\beta)$$

such that $|E(k)| = \chi(1)$ and for every extension k_n of k of degree n, $E(k_n) = (1-\alpha^n)(1-\beta^n)$.

For the proof we will need the following lemma.

Lemma 1.2.1. *Let $\psi \in End(E)$. Then*

$$\det(\psi_l) = \deg(\psi) \textit{ and } tr(\psi_l) = 1 + \deg(\psi) - \deg(1-\psi).$$

Proof. Let v_1, v_2 be a $\mathbb{Z}_l$-basis for $T_l(E)$ and write the matrix of ψ_l for this basis as

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We compute

$$\begin{aligned}
e_l(v_1, v_2)^{\deg(\psi)} &= e_l([\deg(\psi)]v_1, v_2) \\
&= e_l(\hat{\psi}\psi v_1, v_2) \\
&= e_l(\psi v_1, \psi v_2) \\
&= e_l(av_1 + cv_2, bv_1 + dv_2) \\
&= e_l(v_1, v_2)^{ad-bc} \\
&= e_l(v_1, v_2)^{\det(\psi_l)}
\end{aligned}$$

Since e_l is non-degenerate, we conclude that $\deg(\psi) = \det(\psi_l)$. The second part is classical. □

Proof. Let $\pi : E \to E$ be the q-th power of Frobenius endomorphism (review of basic properties of Frobenius is given in Appendix 5.2.1). Since $1 - \pi$ is separable (because the map $(1-\pi)^*$ is the identity on the regular differential and so is not 0), we have

$$|E(k)| = \deg(1 - \pi).$$

Similarly for every $n \geq 1$ and for every extension k_n of degree n, $|E(k_n)| = \deg(1 - \pi^n)$. From the previous lemma, the characteristic polynomial of π_l has coefficients in $\mathbb{Z}$, so we can factor it over $\mathbb{C}$:

$$\det(T - \pi_l) = T^2 - \operatorname{tr}(\pi_l)T + \det(\pi_l) = (T - \alpha)(T - \beta).$$

Further, since for every rational number m/n,

$$\det((m/n) - \pi_l) = \det(m - n\pi_l)/n^2 = \deg(m - n\pi)/n^2 \geq 0,$$

it follows that the quadratic polynomial $\det(T - \pi_l)$ has complex conjugate roots. Thus $|\alpha| = |\beta|$ and

$$\alpha\beta = \det(\pi_l) = \deg(\pi) = q,$$

we conclude that $|\alpha| = |\beta| = \sqrt{q}$.
Finally we note that the characteristic polynomial of π_l^n is given by $(T - \alpha^n)(T - \beta^n)$, so

$$\begin{aligned}
\log Z(E/k; T) &= \sum_{n=1}^{\infty}(|E(k_n)|T^n/n) \\
&= \sum_{n=1}^{\infty}(1 - \alpha^n - \beta^n + q^n)T^n/n \\
&= -\log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - qT)
\end{aligned}$$

which concludes the proof. □

Remark 3. If we let $T = q^{-s}$ then we have

$$\zeta_{E/k}(s) := Z(E/k, q^{-s})$$

and the functional equation reads

$$\zeta_{E/k}(1-s) = \zeta_{E/k}(s),$$

which is an analog for elliptic curve of the Riemman Zeta function for $\mathbb{Q}$. Further if $\zeta_{E/k}(s) = 0$ then $|q^s| = \sqrt{q}$, so $\Re(s) = 1/2$.

The general case follows more or less the same pattern. The main difference is that the elliptic curve is its own Jacobian. Moreover when the dimension is ≥ 2 we have to deal with divisors that are not the sum of points. And the last difference is that the real analogue of an elliptic curve is not only an abelian variety but an abelian variety plus a polarization. All these will prevent us to give a complete proof but we want to introduce the main process and the concepts because there will be also useful in the rest of the course.
For the basic material about abelian varieties and Jacobians we referee to the Appendix 5.1.

1.2.2 Endomorphisms of abelian varieties

We are first going to show that $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$ is a finite dimensional semi-simple algebra over $\mathbb{Q}$. Recall that a finite dimensional K-algebra M is called *semi-simple* if it is isomorphic to a direct sum of simple M-modules (i.e without any non-trivial submodules). For instance, if D is a division algebra then $M_n(D)$ is simple. In fact M is semi-simple iff it is isomorphic to a direct sum of matrix algebras over division algebras. The first result establishes the existence of 'complementaries'.

Proposition 1.2.5. *Let B be an abelian sub-variety of A. Then there exists an abelian variety $B' \subset A$ such that $B \cap B'$ is finite and $B + B' = A$, i.e $B \times B' \to A$ is a isogeny.*

Proof. Choose a polarization λ on A and define B' to be the reduced sub-scheme of the zero component of the kernel of $A \xrightarrow{\lambda} \hat{A} \to \hat{B}$. This is an abelian variety. From the theorem on the dimension of fibers of morphisms, $\dim B' \geq \dim A - \dim B$. The restriction of the morphism $A \to \hat{B}$ to B is the restriction of the polarization λ, which is a polarization on B and so has finite kernel. Therefore $B \cap B'$ is finite and $B \times B' \to A$ is an isogeny. $\square$

Define an abelian variety to be *simple* if it has no proper nonzero abelian sub-varieties. Let $\alpha \in \mathrm{End}(A)$. The connected component of $\ker(\alpha)$ containing 0 is an abelian variety and so it is either A or 0. Hence α is either 0 or an isogeny. In the second case, there is an isogeny $\beta : A \to A$ such that $\beta \circ \alpha = n$ for some $n \in \mathbb{Q}$. This means that α becomes invertible in $\mathrm{End}(A) \otimes \mathbb{Q} = \mathrm{End}^0(A)$. From this it follows that

$\mathrm{End}^0(A)$ is a division algebra (and so is simple).
Now because of the proposition, we know that for every A there exist a decomposition

$$A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}$$

where each A_i is simple and A_i is not isogenous to A_j for $i \neq j$. The above remark shows that

$$\mathrm{End}^0(A) \simeq \prod M_{n_i}(D_i),\ D_i = \mathrm{End}^0(A_i) \text{ a division algebra.}$$

This proves that $\mathrm{End}^0(A)$ is semi-simple.
Reciprocally, if $\mathrm{End}^0(A) \simeq M_1 \times M_2$ let e_i be the 2 idempotents of the decomposition (i.e $e_i(M) = M_i$ and $e_1 + e_2 = 1$). There exists an integer $n > 0$ such that $E_i = ne_i \in \mathrm{End}(A)$. One has the exact sequence

$$0 \to A[n] \to E_1(A) \times E_2(A) \to A \to 0.$$

So A is isogenous to $E_1(A) \times E_2(A)$.
How to find explicitly the numbers involved and the division algebras D_i will be explained in the case of finite fields in 1.4.

Proposition 1.2.6. *For any prime $l \neq Char(K)$, the natural map*

$$Hom(A, B) \to Hom(T_l(A), T_l(B))$$

is injective. In particular $Hom(A, B)$ is torsion free.

Proof. Let $\phi : A \to B$ be a homomorphism such that $\phi_l = 0$; Then $\phi(A[l^n](\overline{K})) = 0$ for all n. For any simple abelian sub-variety A' of A this implies that the kernel of $\phi|A'$ is not finite and so equal to the whole of A'. It follows that $\phi = 0$. □

We have like for elliptic curves even a stronger result (the proof is similar [Mil86, Th.12.5]).

Proposition 1.2.7 ([Mil86, Th.12.5]). *For each prime $l \neq Char(K)$ the natural map*

$$Hom(A, B) \otimes \mathbb{Z}_l \to Hom(T_l(A), T_l(B))$$

is injective with torsion free cokernel. So $Hom(A, B)$ is a free $\mathbb{Z}$-module of finite rank $\leq 4 \dim A \dim B$.

Let $\alpha \in \mathrm{End}(A)$.Now we want to introduce the *characteristic polynomial* of α. By analogy with the complex setting, it is defined as

$$P_\alpha(T) := \det(\alpha - T Id | V_l(A)).$$

It is a monic polynomial of degree $2g$. It seems that it is a polynomial with coefficients in $\mathbb{Q}_l$ so depending on l. However we have the important result.

Theorem 1.2.4 ([Mil86, Prop.12.9]). *P_α is independent of the choice of l and has coefficients in $\mathbb{Z}$. In fact we have for all $r \in \mathbb{Z}$, $P_\alpha(r) = \deg(\alpha - r)$.*

When K is a finite field and $\alpha = \pi$, the Frobenius endomorphism, we write $\chi := P_\pi$ and we call χ *the Frobenius polynomial.* This polynomial will be a fundamental tool in the study of curves over finite fields as we will see in the next section.
For further use, we need at last the following proposition.

Proposition 1.2.8 ([Mil98, Cor.9.24]). *Let $\alpha \in End^0(A)$ and assume that $\mathbb{Q}[\alpha]$ is a product of fields. Let $C_\alpha(X)$ be the characteristic polynomial of α acting on $\mathbb{Q}[\alpha]$ (e.g if $\mathbb{Q}[\alpha]$ is a field, this is the minimum polynomial of α). Then*

$$\{a \in \mathbb{C} | C_\alpha(a) = 0\} = \{a \in \mathbb{C} | P_\alpha(a) = 0\}.$$

1.2.3 Proof of Weil conjectures for curves

We are now going to sketch a proof of Weil conjectures. We will give two proofs for the rationality. The first one is elementary (due to Schmidt, see [Lor96]) and the second one uses the étale cohomology. The second one relates clearly the problem on curves with the study of the Frobenius polynomial. At last, we will prove the Riemann hypothesis and the functional equation thanks to the Rosati involution (note that there exists also a 'elementary' proof due to Bombieri).
In the following C will be a curve over $k = \mathbb{F}_q$ of genus $g \geq 1$. We will denote $J = \mathrm{Jac}(C)$.

Theorem 1.2.5. *We have*

$$Z(C/k; T) = \frac{f(T)}{(1-T)(1-qT)}$$

with $f(T) \in \mathbb{Z}[T]$ a polynomial of degree at most $2g$. Moreover $|Pic^0(C)| = f(1)$.

We first need to give another form to the Zeta function. Let denote

$$Z(T) := \prod_{P \in C(\overline{k})/G} (1 - T^{|G \cdot P|})^{-1} \in \mathbb{Q}[[T]]$$

the formal series where $G = \mathrm{Gal}(\overline{k}/k)$ and $|G \cdot P|$ denote the cardinal of the orbit of P under G.
For every $n \geq 1$ denote $b_n = |\{P \in C(\overline{k})/G,\ |G \cdot P| = n\}$. The integer b_n is well defined because these points are on $C(k_n)$. More precisely they belongs to $C(k_n)$ and not to any $C(k_d)$ for $d|n$. We get actually

$$N_n = \sum_{d|n} d b_d.$$

Now

$$\begin{aligned}
\log(Z(T)) &= \log\left(\prod_d (1-T^d)^{-b_d}\right) \\
&= \sum_d -b_d \log(1-T^d) \\
&= \sum_d b_d \sum_n \frac{T^{dn}}{n} \\
&= \sum_n (\sum_{d|n} b_d d) \frac{T^n}{n} \\
&= \sum_n N_n \frac{T^n}{n}
\end{aligned}$$

So $Z(T) = Z(C/k;T)$.

Proof. Starting with the expression Z we get

$$\begin{aligned}
Z(T) &= \prod_{P \in C(\bar{k})/G} (1-T^{|G\cdot P|})^{-1} \\
&= \sum_{D \in \mathrm{Eff}(C/k)} T^{\deg(D)} \\
&= \sum_{\substack{L \in \mathrm{Pic}(C/k) \\ \deg(L) \geq 0}} \left(\sum_{\substack{D \in \mathrm{Eff}(C/k) \\ (D) \sim L}} T^{\deg(D)} \right)
\end{aligned}$$

where $\mathrm{Eff}(C/k)$ denotes the group of effective divisors of C defined over k. Note that an element $D \in \mathrm{Eff}(C/k)$ is not necessary the sum of points in $C(k)$ (it is enough that it is G-invariant).

Denote

$$E_L := \{D \in \mathrm{Eff}(C/k)/(D) \sim L\}.$$

We want to use Riemman-Roch theorem to compute explicitly the order of this set, at least when the degree of L is large enough. Starting from the last expression

$$Z(T) = \sum_{\substack{L \in \mathrm{Pic}(X/k) \\ 0 \leq \deg(L) \leq 2g-2}} |E_L| T^{\deg(L)} + \sum_{\substack{L \in \mathrm{Pic}(X/k) \\ \deg(L) \geq 2g-1}} |E_L| T^{\deg(L)}.$$

By Riemann-Roch $l(L) = \deg(L) - g + 1 + l(\kappa - L)$ and when $\deg(L) \geq 2g-1$, $l(\kappa - L) = 0$ so we get

$$|E_L| = \frac{q^{\deg(L)+1-g} - 1}{q-1}$$

(note that $E_L = \mathbb{P}(\mathcal{L}(L))$).
To shorten a bit the proof (but the arguments remain the same), we suppose now that $C(k) \neq \emptyset$. Then it is clear that the map deg : $\mathrm{Pic}(C/k) \to \mathbb{Z}$ is surjective and that the kernel $\mathrm{Pic}^0(C/k) = J(k)$ is finite of order h (in the general case, we have to use Riemann-Roch again to prove that the kernel is finite, see [Lor96, VIII.6.1]). Therefore for all $d \in \mathbb{N}$, the set $\mathrm{Pic}^d(C/k)$ has order h. It follows that

$$\sum_{\substack{L \in \mathrm{Pic}(X/k) \\ 0 \leq \deg(L) \leq 2g-2}} |E_L| T^{\deg(L)}$$

is a polynomial in T of order at most $2g-2$. In the same way

$$\sum_{\substack{L \in \mathrm{Pic}(X/k) \\ \deg(L) \geq 2g-1}} |E_L| T^{\deg(L)} = h \cdot \sum_{d \geq 2g-1} \frac{q^{d+1-g} - 1}{q-1} T^d.$$

After an easy computation, one finds for this last expression

$$\frac{h}{q-1} \cdot \sum_{d \geq 2g-1} (q^{d+1-g} - 1) T^d = h \frac{u(T)}{(1-T)(1-qT)} \tag{1.1}$$

where $u(T) \in \mathbb{Z}[T]$ is a polynomial of degree at most $2g$. It follows that

$$Z(C/k; T) = \frac{f(T)}{(1-T)(1-qT)}$$

with $f(T) \in \mathbb{Z}[T]$ a polynomial of degree at most $2g$. Moreover from expression (1.1) we have

$$\lim_{T \to 1} (T-1) Z(C/k; T) = \frac{h}{q-1}.$$

□

Remark 4. Note that we have also $|J(k)| = f(1)$ if $C(k) = \emptyset$.

The second proof uses the Lefschetz fixed-point formula. Let $\pi : C_{\overline{k}} \to C_{\overline{k}}$ the q-Frobenius map. $P \in C_{\overline{k}}$ is a fixed point of π iff $P \in C(k)$. Thus with the notations of 5.2.4, $|C(k_n)| = L(\pi^n, C)$. As C is smooth and projective we can compute these numbers via the Leftschetz fixed-point formula (note that $1 - d\pi^n = 1$ is injective on the regular differentials). We find

$$|C(k_n)| = \mathrm{tr}(\pi^n | H^0(C_{\text{ét}}, \mathbb{Q}_l)) - \mathrm{tr}(\pi^n | H^1(C_{\text{ét}}, \mathbb{Q}_l)) + \mathrm{tr}(\pi^n | H^2(C_{\text{ét}}, \mathbb{Q}_l)).$$

π^n acts on $H^0(C_{\text{ét}}, \mathbb{Q}_l)$ (which is one dimensional) as the identity and on $H^2(C_{\text{ét}}, \mathbb{Q}_l)$ (which is also one dimensional) as q^n. So substituting in the definition of the Zeta function, we have

$$Z(C/k;T) = \underbrace{\exp\left(\sum T^n/n\right)}_{=1/(1-T)} \underbrace{\exp\left(-\sum \mathrm{tr}(\pi^n | H^1(C_{\text{ét}}, \mathbb{Q}_l)) T^n/n\right)}_{=\det(1-\pi T | H^1(C_{\text{ét}}, \mathbb{Q}_l))} \underbrace{\exp\left(\sum q^n T^n/n\right)}_{=1/(1-qT)}.$$

Then we know that $H^1(C_{\text{ét}}, \mathbb{Q}_l)$ is functorially isomorphic to $H^1(\text{Jac}(C)_{\text{ét}}, \mathbb{Q}_l)$ which is functorially isomorphic to $V_l(\text{Jac}(C))^*$. By functoriality we get also that π induces the Frobenius endomorphism of J/k and

$$\det(1 - \pi T | H^1(C_{\text{ét}}, \mathbb{Q}_l)) = T^{2g}\chi(1/T)$$

which proves the rationality.
Thus to prove the functional equation and the Riemann hypothesis it is enough to study the roots of the Frobenius polynomial. Let J the Jacobian of C and λ its canonical (principal) polarization. Note that as the polarization is principal, $\dagger$ defines an involution of $\text{End}(J)$.

Lemma 1.2.2. *We have* $\pi \circ \pi^\dagger = [q]$.

Proof. We can prove that by using the Weil-pairing. Indeed we have for the canonical generator $\sigma \in \text{Gal}(\overline{k}/k) : a \mapsto a^q$ and for all $S, T \in T_l(J)$

$$\begin{aligned} e_l^\lambda(S,T)^\sigma &= e_l^\lambda(S^\sigma, T^\sigma) \text{ Galois invariance} \\ &= e_l^\lambda(\pi(S), \pi(T)) \text{ because the Galois action = geometric action} \\ &= e_l^\lambda(\pi \circ \pi^\dagger(S), T) \text{ see 5.1.4} \end{aligned}$$

Now

$$e_l^\lambda(S,T)^\sigma = e_l^\lambda(S,T)^q = e_l^\lambda([q]S, T)$$

and we have the result because e_l^λ is non-degenerate. □

We see that the morphism $\pi^\dagger$ is in fact the *Verschiebung* (see 5.2.1).

Lemma 1.2.3. *Let* $\psi \in End(J)$ *such that* $\psi^\dagger \circ \psi$ *is an integer* r. *Then* $\mathbb{Q}(\psi)$ *contains no nilpotent element. Moreover for any root* α *of* $P_\psi, |\alpha|^2 = r$. *In particular if* $\psi = \pi$ *we obtain the Riemann hypothesis.*

Proof. Prove the first assertion. Suppose that $\mathbb{Q}(\psi)$ contains an nilpotent element $\beta \neq 0$. Then $\beta' = \beta\beta^\dagger \neq 0$ because $\text{tr}(\beta\beta^\dagger) > 0$ (Th.5.1.3). As $\beta' = \beta'^\dagger$ this implies that $\text{tr}(\beta'^2) > 0$ so $\beta'^2 \neq 0$. Similarly, $\beta'^4 \neq 0$, and so on, which contradicts the nilpotent of β.
We can now prove the second part. Note that $\mathbb{Q}(\psi)$ is stable under $\dagger$. As $\mathbb{Q}(\psi)$ contains no nilpotent elements, it is a product of fields. The tensor product $\mathbb{Q}(\psi) \otimes \mathbb{R}$ is a copy of $\mathbb{R}$ and $\mathbb{C}$. Moreover $\dagger$ extends to an $\mathbb{R}$-linear involution of $\mathbb{Q}(\alpha) \otimes \mathbb{R}$ and $\text{tr}(\beta^\dagger\beta) \geq 0$ for all $\beta \neq 0$ with inequality holding on a dense subset. It follows easily that each factor S of $\mathbb{Q}(\psi) \otimes \mathbb{R}$ is stable under $\dagger$ and that $\dagger$ is the identity map if S is real and is complex conjugation is K is complex. Thus for each homomorphism j of $\mathbb{Q}(\psi)$ into $\mathbb{C}$, $j(\psi^\dagger)$ is the complex conjugate of $j(\psi)$. The hypothesis of the theorem states that $|j(\psi)|^2 = r$. We can then conclude using Prop.1.2.8 because the roots of $P_\psi(X)$ are the same (as a set) as the root of the characteristic polynomial of ψ as an element of $\mathbb{Q}(\psi)$. □

Let us finish with a proof of the functional equation. We first show that if α is a root of χ then $q/\alpha = \overline{\alpha}$ also (in the sense that real roots have an even multiplicity). As χ has integer coefficients, it is clear that if $\chi(\alpha) = 0$ then $\chi(\overline{\alpha}) = 0$. We have then only to concentrate on the case α real. Then $\alpha = \pm\sqrt{q}$. Suppose $\alpha = -\sqrt{q}$. As $\prod_{i=1}^{2g} \alpha_i = \deg \pi = q^g$ there must exist an other negative roots. So real roots come always by pair.
We show now that this property implies the functional equation :

$$\begin{aligned} Z(C/k; 1/(qT)) &= \frac{\prod_{i=1}^{2g}(1-\alpha_i/(qT))}{(1-1/(Tq))(1-1/T)} \\ &= \frac{(qT)^{-2g} \cdot qT^2 \cdot \prod(qT-\alpha_i)}{(Tq-1)(T-1)} \\ &= \frac{q^{-2g+1} \cdot T^{-2g+2} \cdot \prod((\alpha_i\overline{\alpha_i})T-\alpha_i)}{(1-T)(1-qT)} \\ &= q^{2g+1}T^{-2g+2} \cdot \prod(\alpha_i) \cdot \frac{\prod(\overline{\alpha_i}T-1)}{(1-T)(1-qT)}. \end{aligned}$$

And we have the result as we know that $\{\overline{\alpha_i}\} = \{\alpha_i\}$ with multiplicities.

Remark 5. Note that for all n, $1-\pi^n$ is étale (because it is the identity on the tangent space). So its kernel is finite and equal to the degree of the map. So

$$|J(k_n)| = |\ker(1-\pi^n)| = |\deg(1-\pi^n) = \prod(1-\alpha_i^n).$$

In particular $|J(k)| = \chi(1) = f(1)$.

1.3 Hasse-Witt matrix and p-rank

This is part of [Ser58]. In this section X is an (algebraic smooth, projective) curve of genus g defined over an algebraic closed field k of characteristic $p > 0$.

1.3.1 Differentials and Weil differentials

We give a classical interpretation of $H^1(X, \mathcal{O})$ (see also [Sti93, IV.3]). Let $K = k(X)$ seen as a constant sheaf on X with $\mathcal{O}$ as a subsheaf. From the exact sequence

$$0 \to \mathcal{O} \to K \to K/\mathcal{O} \to 0,$$

one deduces the associated cohomology sequence :

$$K \to H^0(X, K/\mathcal{O}) \to H^1(X, \mathcal{O}). \tag{1.2}$$

Let R be the adele of K : an element of R is a family $\{r_x\}_{x \in X}$ where r_x are elements of K belonging to $\mathcal{O}_x$ for all but a finite number of x. The elements for which r_x are all in $\mathcal{O}_x$ generate a subring $R(0)$. One embeds diagonally K in R. One has that

$R/R(0)$ is canonically isomorphic to $H^0(X, K/\mathcal{O})$ and the exact sequence (1.2) gives an isomorphism

$$R/(R(0)+K) \simeq H^1(X,\mathcal{O}). \tag{1.3}$$

The space $R/(R(0)+K$ is called *the space of Weil differentials.* In fact, by duality one knows that $H^1(X,\mathcal{O}) \simeq H^0(X,\Omega^1)^*$. The duality can be expressed with the bilinear form (cup-product) :

$$< r, \omega >= \sum_x \mathrm{res}_x(r_x\omega).$$

Remark 6. If ω is a differential and x a point of the curve, let us write $\omega = P(t)dt$. One can develop P locally in t as a Laurent series $P(t) = \sum a_i t^i \in k((t))$ and $\mathrm{res}_x(\omega) = a_{-1}$ (this is an extension of the usual definition for classical analytic function).

1.3.2 The Hasse-Witt matrix

Let $F : H^1(X,\mathcal{O}) \to H^1(X,\mathcal{O})$ the p-linear operator induced by $F : X \to X$. We want to find 'its matrix'. Note that the identification (1.3) transforms F in the pth power of R. By using the duality $R/(R(0)+K)$ with $H^0(X,\Omega^1)$ one sees that there exist g points $P_1,\ldots,P_g$ such that if $t_1,\ldots,t_g$ are uniformizers at these points, the adeles $r_i = \{r_{i,x}\}$ where $r_{i,x} = 0$ if $x \neq P_i$ and $r_{i,x} = 1/t_i$ if $x = P_i$ are a basis of the k-vector space $R/(R(0)+K)$.
Let $A = (a_{ij})$ the matrix of F relative to this basis. By definition

$$r_i^p \equiv \sum a_{ij} r_j \pmod{R(0)+K}.$$

Definition 1.3.1. *The matrix A is called* the Hasse-Witt *matrix of X.*

We will need some notions of the Jordan reduction of F.

Definition 1.3.2. *Let n be an integer. An additive mapping $F : V_1 \mapsto V_2$ between two k-vector spaces is said to be p^n-*linear *if it satisfies $F(\lambda x) = \lambda^{p^n} F(x)$ for all $\lambda \in k$ and all $x \in V_1$.*

Let F be a p-linear endomorphism of a finite k-vector space V. This operator has no obvious characteristic polynomial attached. But the space V has a canonical decomposition

$$V = V_s \oplus V_n \tag{1.4}$$

where V_s and V_n are stable by F, F being nilpotent on V_n and bijective on V_s. The dimension of V_s and V_n are denoted respectively γ and ν. These numbers remind invariant by a change of basis. One can show also that V_s has a basis $e_1,\ldots,e_\gamma$ such that $F(e_i) = e_i$ for all i. The vectors $v \in V$ such that $F(v) = v$ are linear combinations of the e_i with coefficients in $\mathbb{F}_p$. They form a finite group V^F of order p^γ.
Let V^* the dual of V. The transposition F' of F is a p^{-1}-linear endomorphism defined by the formula :

$$< F(v), v^* >=< v, F'(v^*) >^p .$$

To the decomposition (1.4) corresponds the dual decomposition

$$V^* = V_s^* \oplus V_n^*.$$

If e_i' is the dual of e_i they form a basis of V_s^* and we still have $F'(e_i') = e_i'$ and $F'(v') = v'$ iff v' is a linear combination of e_i' with coefficients in $\mathbb{F}_p$. These v' form a group dual to V^F.
One can apply this to our case.

Definition 1.3.3. *One calls the integer* $0 \leq \gamma \leq g$ *the* p-rank *or* Hasse-Witt invariant *of* X.

Remark 7. One can see that γ is the rank of the matrix $AA^{(p)} \cdots A^{(p^{g-1})}$.

Remark 8. This invariant is only a particular case of invariants one can obtain : see [Kan85].

1.3.3 Cartier operator

Let $t \in k(X)$ be a function which differential dt is not 0. Each function f may be written in a unique way as

$$f = f_0^p + f_1^p t + \ldots f_{p-1}^p t^{p-1}, \; f_i \in k(X).$$

One has easily $f_{p-1}^p = -d^{p-1}f/dt^{p-1}$.
Let $\omega = f dt$ be a differential. We denote

$$C(\omega) := f_{p-1} dt.$$

Definition 1.3.4. *The* p^{-1}*-linear map* C *is called the* Cartier-(Tate) operator.

One can prove that :

1. C does not depend on the choice of t.
2. C acts on the regular differentials.

Proposition 1.3.1. *One has the following properties :*

1. $C(\omega_1 + \omega_2) = C(\omega_1) + C(\omega_2)$.
2. $C(f^p \omega) = f C(\omega)$.
3. $C(df) = 0$.
4. $C(f^{p-1} df) = df$.

The regular differentials df are called *exact differentials*. One has in fact that ω is exact iff $C(\omega) = 0$.
The regular differentials df/f are called *logarithmic differentials*. One has $C(df/f) = C(f^{p-1}df/f^p) = C(f^{p-1}df)/f = df/f$. A theorem of Jacobson shows that w is logarithmic iff $C(w) = w$.
This operator is related to our original problem via the following proposition.

Proposition 1.3.2. *$C : H^0(X, \Omega^1) \to H^0(X, \Omega_1)$ is the transpose F' of F.*

Proof. Let ω be a regular differential and r be an adele. One has to show that

$$< r^p, \omega >=< r, C(\omega) >^p .$$

But this is

$$\sum_x \mathrm{res}_x(r_x^p \omega) = \sum_x \mathrm{res}_x(r_x C(\omega))^p.$$

This is a direct consequence of $\mathrm{res}_x(\pi) = \mathrm{res}_x(C(\pi))^p$, where π is any differential. □

1.3.4 p-torsion

This important operator allows us to get information on the p-torsion part of the Jacobian.

Proposition 1.3.3. *$Jac(X)[p](k)$ is canonically isomorphic to the additive group of regular logarithmic differentials. In particular it is a finite group of order p^γ.*

Proof. We define an application $\vartheta : Jac(X)[p](k) \to H^0(X, \Omega^1)$.
Let $d \in Jac(X)[p](k)$ and D be a divisor in the class of d. Since $pd = 0$ there exists a function $f \neq 0$ such that $pD = (f)$. Let $\omega = df/f$. If one changes D to an equivalent divisor $D + (g)$, one multiples f by g^p and this does not change ω. One can then put $\omega = \vartheta(d)$. If $x \in X$ the equation $pD = (f)$ shows that $f = t^p u$ where u is a unit in $\mathcal{O}_x$ and $df/f = du/u$ shows that df/f is regular in x. So ϑ is well defined.
It is easy to see that ϑ is injective. Let us show that the image of ϑ is the regular logarithmic differentials. Let $\omega = df/f$ be a regular logarithmic differential. As ω is regular, for every point $x \in X$, the order of f at x is divisible by p. This means that $(f) = pD$ and $\omega = \vartheta(d)$ where d is the class of D.
For the last point, we know that ω is logarithmic iff $C(\omega) = \omega$, ϑ is then an isomorphism of $\mathrm{Jac}(X)[p](k)$ onto the fixed points of C. □

We can use this proposition to extend the definition of p-rank to an arbitrary abelian variety. In fact our original definition of the p-rank (and Cartier operator) is also valid for abelian varieties. In particular we confuse the notion of p-rank of X or of its Jacobian. An other important remark is that we know now that the p-rank is invariant by isogenies. Indeed let $\lambda : A \to B$ be an isogeny of degree d. Then we have for all n $\lambda(\ker([p^n])(\overline{k}) \subset \ker([p^n])(\overline{k})$ so $p^{n\gamma_A} = |\ker([p^n])(\overline{k})| \leq d \ker([p^n])(\overline{k}) = dp^{n\gamma_B}$ so $\gamma_A \leq \gamma_B$. As there exists also an isogeny from $B \to A$ we have then $\gamma_A = \gamma_B$. As a consequence, if $A \sim A_1 \times A_2$ then $\gamma_A = \gamma_{A_1} + \gamma_{A_2}$.
Is this invariant related to something else ? In fact we have an easy way to compute it when k is the algebraic closure of a finite field k_0.

Theorem 1.3.1. *Let X (resp. A) be a curve of genus g (resp. an abelian variety of dimension g) defined over $k_0 = \mathbb{F}_{p^n}$. The Hasse-Witt invariant of X (resp. A) is the sum of the multiplicities of the nonzero roots of the reduction modulo p of the Frobenius polynomial of X (resp. A) over k_0.*

Proof. This follows from Manin's formula [Man61]

$$\det(\pi - tId|V_l(A)) \equiv (-1)^g t^g \det(\pi - tId|H^1(A,\mathcal{O})) \pmod{p}$$

where π is the Frobenius endomorphism of A (and A may also be $\mathrm{Jac}(X)$). □

Remark 9. Note that we use π in the formula which is a linear operator on k and not F (and so it has a meaning to speak about characteristic polynomials). One says that π *linearizes* F (see [BG97]).
Manin's formula gives more information than the p-rank : it says that in the case of a curve, the characteristic polynomial modulo p is given by the action of a 'power' of C on a basis of differentials. In particular :

$$|X(k)| \equiv 1 - \mathrm{tr}(C \circ C^{(p)} \cdots C^{(p^{g-1})}) \pmod{p}.$$

This idea has been exploited in [BGS04] to give an algorithm to compute the Frobenius polynomial of a genus 2 curve over $\mathbb{F}_p$.

1.3.5 Examples and applications

Example of elliptic curves

Let E be an elliptic curve. One has $\dim(H^0(E,\Omega_1)) = 1$ so the Hasse-Witt matrix is only a scalar A. If $p \neq 2$ one can write E under the form $E : y^2 = f(x)$. A base for the regular differentials is for instance dx/y. One can distinguish two cases :

1. $A \neq 0$: then we have that $|E[p](k)| = p^1 = p$. We say that the curve is *ordinary.*

2. $A = 0$: then we have that $|E[p](k)| = p^0 = 1$. We say that the curve is *supersingular.* Note that this is equivalent to the fact that the dual isogeny $\hat{\mathrm{Fr}} : E^{(p)} \to E$ is purely inseparable (and also the Verschiebung $V : E \to E$), since the map $[p] : E \to E$ is purely inseparable.

We want to understand when these zeros occur.

Theorem 1.3.2 ([Sil92, V.4.1]). *Let $E : y^2 = f(x)$ be defined over the finite field $k = \mathbb{F}_q$ of characteristic $p > 2$.*

1. *E is supersingular iff the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.*

2. *Let $m = (p-1)/2$ and define the polynomial*

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$

Let $f(x) = x(x-1)(x-\lambda)$. E is supersingular iff λ is a root of H_p.

3. *The polynomial $H_p(\lambda)$ has distinct roots in $\overline{k}$.*

Proof. We are going to prove the first point.
Let $x \in k$. Then the number of points in $E(k)$ with abscissas x is $0, 1$ or 2 and is equal to $f(x)^{(q-1)/2} + 1$ (seen as an integer). So we have the formula

$$|E(k)| = 1 + q + \sum_{x \in k} f(x)^{(q-1)/2},$$

which gives modulo p (or seen in k)

$$|E(k)| = 1 + \sum_{x \in k} f(x)^{(q-1)/2}.$$

We have now easily that

$$\sum_{x \in k} x^i = \begin{cases} -1 \text{ if } q-1 | i \\ 0 \text{ otherwise.} \end{cases}$$

Since f has degree 3, if we multiply out $f(x)^{(q-1)/2}$ and sum over $x \in k$, the only non-zero term comes from x^{q-1}. Hence if we let

$$A_q = \text{coefficient of } x^{q-1} \text{ in } f(x)^{(q-1)/2}$$

then

$$|E(k)| = 1 + A_q = 1 - \operatorname{tr}(\pi)$$

where $\pi : E \to E$ is the Frobenius endomorphism. Now $A_q = 0 \iff \operatorname{tr}(\pi) \equiv 0 \pmod{p}$. But $\hat{\pi} = [\operatorname{tr}(\pi)] - \pi$, so

$$A_q = 0 \iff \hat{\pi} \text{ is inseparable} \iff E \text{ is supersingular.}$$

It remains to show that $A_q = 0$ iff $A_p = 0$. Writing

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2} (f(x)^{(p-1)/2})^{p^r}$$

and equating coefficients (remember f is a cubic) yields

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r}$$

(this reminds us of the strange matrix multiplication of p-linear operators in remark 7) and we have the desired result by induction on r. $\square$

Remark 10. For other characterizations of supersingular elliptic curves, see [Sil92, V.3]. Note that (3) shows that there is roughly $(p-1)/12$ classes of supersingular elliptic curves up to $\overline{\mathbb{F}_p}$-isomorphism.

An important question is the following : let E/K an elliptic curve defined over a number field. For all but a finite number of primes, E has good reduction. How big is the set of primes for which this reduction is supersingular ? When the curve E has complex multiplication, one can prove that this set has density $1/2$. However when E has not complex multiplication, the answer is not known. However When E is defined over $\mathbb{Q}$, Elkies [Elk87] proved that this set is infinite. The answer in higher dimension or genus is even more subtle. One only knows for example [BG97, Prop.5.1]

Proposition 1.3.4. *Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 2$. Then there exists a set of primes with positive density for which $\gamma_{A\otimes\mathbb{F}_p} \geq 2$ for all p in this set.*

Remark 11. There exists a kind of converse proposition to Elkies' theorem [Cha00] : let X be a curve defined over a number field K and ω a differential. One supposes that for almost all prime p, $\omega \pmod p$ is a exact differential (resp. logarithmic). Then ω is an exact differential (resp. there exists an integer $n \geq 1$ such that $n\omega$ is logarithmic). One cannot use this theorem to prove Elkies' : indeed $E \pmod p$ supersingular implies that there exists a regular logarithmic differential but it has not to be dx/y (only a scalar multiple of it, different for each p). But one can use it to prove that there exists an infinite number of p for which the curve is ordinary (because otherwise there would exist a regular exact differential on E/K.

Application to modular curves

In the case of modular curves, the problem of p-rank distribution has been approached in [BG97]. First, thanks to the Eichler-Shimura congruence, there is a nice way to relate the Hecke operators with our problem :

Proposition 1.3.5. *The Hasse-Witt invariant of $X(N)_p := X_0(N)\otimes\mathbb{F}_p$ (p not dividing N) is the sum of the multiplicities of the nonzero roots of the reduction modulo p of the characteristic polynomial of T_p on $S_2(X_0(N))$.*

Moreover

Proposition 1.3.6. *For almost all prime p, $\gamma_{X_0(N)_p} = 0$ implies $T_p = 0$.*
The set of primes for which $\gamma_{X_0(N)_p} = 0$ and $Jac(X_0(N)_p)$ is not $\overline{\mathbb{F}_p}$-isogenous to a supersingular abelian variety is finite (see 1.4 for the definition of supersingular).

Proof. Let us prove the first point.
As the p-rank is invariant by isogeny, we may consider a factor $A = A_f$ of $X_0(N)$ associated to a newform $f \in S_2(N)$. Let $f_1, \ldots, f_g$ be a basis of newforms and $h_1, \ldots, h_g$ be a basis of forms with integral coefficients. Let $M = (m_{ij})$ be the matrix of the change of basis, so that $h_j = \sum m_{ij} f_i$. Let c denote an upper bound of the values $|m_{ij}|$ and let $\mathcal{Q}$ denote the set of primes such that m_{ij} is p-integral, p not dividing N, and $\sqrt{p} > 2gc$. If $f_i = \sum_{n>0} a_i(n)q^n$, $h_i = \sum_{n>0} c_i(n)q^n$, then we get

$$|c_j(p)| = |\sum m_{ij} a_i(p)| \leq c \sum |a_i(p)| < c2g\sqrt{p} < p$$

for all $p \in \mathcal{Q}$. Assume now that $\gamma_p(A) = 0$. If the entries of the matrix M are p-integral, we must have $c_i(p) \equiv 0 \pmod p$ for $1 \leq i \leq g$ (because the eigenvalues of T_p are the $a_i(p)$ and are all congruent to 0 by Prop.1.3.5). If $p \in \mathcal{Q}$, we therefore get $c_i(p) = 0$. Since M is invertible, $a_i(p) = 0$. Then we see that $T_p = 0$. □

We will give some statistics about this problem in the tutorial 6.4.

Application to quartics in characteristic 2

Let X be a curve a genus g over k of characteristic $p = 2$.

Definition 1.3.5. *One calls* theta characteristic *the class of a divisor* ϑ *such that* $2\vartheta = \kappa$ *the canonical divisor.*

Let $t \in k(X)$ be a separating variable (i.e $dt \neq 0$). Then the divisor of the differential dt is of the form $2D_0$ and the class of D_0 does not depend on the choice of t. We call the class of D_0 the *canonical theta characteristic* and denote it by ϑ_0.

Proposition 1.3.7 ([SV87]). *There is a* $\frac{1}{2}$*-linear bijection from the space of regular exact differentials onto* $L(D_0)$.
There is a canonical bijection between the set of regular logarithmic non-zero differentials and the set of non-canonical theta characteristics which sends ω *to the class of* $\frac{1}{2}div(\omega)$.

Proof. Let $f \in k(X)$. Write $f = f_0^2 + f_1^2 t$, then $df = f_1^2 dt$ and df is regular iff $\mathrm{div}(f_1) + D_0 \geq 0$ that is $f_1 \in L(D_0)$.
For the second part : let $\omega = dh/h \neq 0$ be regular. Then, by an easy local computation in characteristic 2, one sees that $\mathrm{div}(\omega) = 2D$ for some divisor D. Since $dh \neq 0$, h is not a square, that is D is not equivalent to the divisor $\frac{1}{2}\mathrm{div}(dh)$, which represents the canonical theta characteristic.
Reciprocally, let D be a divisor which represents a non-canonical theta characteristic. Then $2D$ is equivalent to $2D_0$, say $2D_0 - 2D = \mathrm{div}(h)$ for some $h \in k(X)$. Since $\mathrm{div}(h)$ is divisible by the characteristic, the logarithmic differential dh/h is regular. Since D is not equivalent to D_0, h is not a square, that is $dh \neq 0$. Since $\frac{1}{2}\mathrm{div}(dh)$ is equivalent to D_0, we conclude that $\frac{1}{2}\mathrm{div}(dh/h)$ is equivalent to D. □

Suppose now that X is non-hyperelliptic of genus 3. Then X may be canonically embedded as a plane quartic. Since the positive canonical divisors are exactly the intersection divisors of X with the projective lines, we see that the positive divisors which represent theta characteristics correspond bijectively to the bitangents of the quartic X. By Clifford's theorem, in each theta characteristic there is at most one positive divisor. Thus the number of bitangents of X is $7, 4, 2$ or 1 if $\gamma = 3, 2, 1$ or 0.

Remark 12. When $p \neq 2$, one can show that a smooth quartic has exactly 28 bitangents.

When X is ordinary, by sending 4 of this bitangents to the lines $x = 0, y = 0, z = 0, x + y + z = 0$ one obtain the canonical model

Proposition 1.3.8. *An ordinary quartic is isomorphic over* $\overline{\mathbb{F}}_2$ *to the model*

$$(ax^2 + by^2 + cz^2 + dxy + exz + fyz)^2 = xyz(x + y + z)$$

with

$$abc(a + b + d)(a + c + e)(b + c + f)(a + b + c + d + e + f + 1) \neq 0.$$

Conversely, every curve which satisfies this condition is an ordinary non hyperelliptic curve of genus 3.

Remark 13. In [NR03], models (even rational models) for the other cases of p-rank are given.

1.4 The structure of abelian varieties over finite fields

Let A be an abelian variety defined over a finite field k. We would like to understand the structure of A, for example how it decomposes up to isogeny. These problems are in fact reflected in the endomorphism ring of A. And fortunately for us, a part of this structure is contained in the Frobenius polynomial.
More precisely we are considering the following category :
objects : abelian varieties over k ;
morphisms : $\mathrm{Mor}(A,B) = \mathrm{Hom}(A,B) \otimes \mathbb{Q} := \mathrm{Hom}^0(A,B)$.
This category is called *the category of abelian varieties up to isogeny* over k, $\mathbf{Isab}(k)$, because two abelian varieties become isomorphic in $\mathbf{Isab}(k)$ iff they are isogenous (over k). We already know (Sect. 1.2.2) that every object in $\mathbf{Isab}(k)$ is a direct sum of a finite number of simple objects. In order to describe such a category, it is enough to list the isomorphism classes of simple objects and, for each class, the endomorphism algebra.
Let $\pi_A = \pi$ the Frobenius endomorphism of A. Then π commutes with all endomorphisms of A, so lies in the center of $\mathrm{End}^0(A)$. If A is simple, then $\mathrm{End}^0(A)$ is a division algebra. Therefore, in this case, $\mathbb{Q}(\pi)$ is a field (not merely a product of fields). An isogeny $A \to B$ of simple abelian varieties defines an isomorphism $\mathrm{End}^0(A) \to \mathrm{End}^0(B)$ carrying π_A into π_B and hence mapping $\mathbb{Q}(\pi_A)$ isomorphically onto $\mathbb{Q}(\pi_B)$.
Define a *Weil q-integer* to be an algebraic integer such that, for every embedding $\sigma : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$, $\sigma(\pi) = \sqrt{q}$ and let $W(q)$ be the set of Weil q-integers in $\mathbb{C}$. Say that two elements π and π' are conjugate, $\pi \sim \pi'$ if they have the same minimal polynomial over $\mathbb{Q}$.
For any simple abelian variety A, the image of π_A in $\overline{\mathbb{Q}}$ is a Weil q-integer, well-defined up to conjugacy.

Theorem 1.4.1. *The map $A \mapsto \pi_A$ defines a bijection*

$$\{\textit{simple abelian varieties}/\mathbb{F}_q\}/(\sim) \mapsto W(q)/(\textit{conjugacy}).$$

Proof. The injectivity of the map $A \mapsto \pi_A$ has been proved by Tate [Tat66]. It uses a generalization of the Remark 2 :

$$\mathrm{Hom}(A,B) \otimes \mathbb{Q}_l \simeq \mathrm{Hom}(V_l(A), V_l(B))^{\mathrm{Gal}(\overline{k}/k)}.$$

In fact the canonical generator of $\mathrm{Gal}(\overline{k}/k)$ acts on $V_l(A)$ and $V_l(B)$ as π_A and π_B respectively and these actions are semisimple (i.e over some extension of $\mathbb{Q}_l$ there exists bases of eigenvectors) ; it is an easy exercise in linear algebra to prove that

$$\mathrm{rank}\ \mathrm{Hom}(V_l(A), V_l(B))^{\mathrm{Gal}(\overline{k}/k)} = |\{(i,j) | \alpha_i = \beta_j\}|$$

where $\chi_A(T) = \prod(X - \alpha_i)$ and $\chi_B(T) = \prod(X - \beta_j)$.
The surjectivity was proved by Honda. To construct abelian variety with a given Frobenius polynomial, Honda used the theory of complex multiplication : one constructs (as a torus) an abelian variety over $\mathbb{C}$ with complex multiplication and the classical theorems show that one can reduce it and one has precise control on the Frobenius polynomial. □

Example 2. *A Weil-number whose minimal polynomial has degree d is not necessarily associated to an abelian variety of dimension $d/2$. For instance let $q = p^2$ and $\pi_A = p$. Then its minimal polynomial is $T - p$ but it is indeed associated to the elliptic curve with Frobenius polynomial $(T-p)^2$.*
See however 3.3.3 to have an idea how to recover this bijection in terms of the Frobenius polynomial.

To complete the description of $\mathbf{Isab}(k)$ in terms of Weil-integer, we have to describe the division algebra $\mathrm{End}^0(A)$. Let us recall first some definitions.

Definition 1.4.1. *A* central simple algebra *over a field K is a K-algebra R such that :*

1. *R is finite dimensional over K,*
2. *K is the center of R,*
3. *R is a simple ring (i.e it has no left and right non-trivial ideals).*

If R is also a division algebra, we call it a central division algebra *over K.*

Lemma 1.4.1. *If R and S are central simple algebras over K, then so is $R \otimes_K S$.*

For example, if R is a central simple algebra over K then so is $M_r(R) = R \otimes_K M_r(K)$.

Proposition 1.4.1 (Wedderburn's theorem). *Every central simple algebra R over K is isomorphic to $M_r(D)$ for some $r \geq 1$ and central division algebra D over K.*

The *Brauer group* $Br(K)$ of a field is defined as follow. Its elements are the isomorphism classes of central division algebras over K. If D and D' are two such algebras, then $D \otimes_k D' \simeq M_r(D'')$ and we set $[D] \cdot [D'] = [D'']$. This is a group –the identity element is $[K]$ and $[D]^{-1} = [D^{opp}]$ (the same underlying set and addition, but multiplication is reversed (if $ab = c$ in D, $ba = c$ in D^{opp})).

Theorem 1.4.2. *For any local field K there is a canonical homomorphism*

$$inv : Br(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

If K is nonarchimedian, inv is an isomorphism; if $K = \mathbb{R}$, then the image is $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$; if $K = \mathbb{C}$, then $Br(K) = 0$.

Remark 14. The non-zero element of $Br(\mathbb{R})$ is represented by the Hamilton's quaternion.

Theorem 1.4.3. *For a number field K, there is an exact sequence*

$$0 \to Br(K) \to \oplus_v Br(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Here the sum is over all places of K, the first map sends $[D]$ to $\sum [D \otimes_k k_v]$ and the second map sends (a_v) to $\sum inv(a_v)$. Hence a central division algebra is uniquely determined up to isomorphism by its invariants.

We need one further result.

Theorem 1.4.4. *For a central division algebra D over a number field K, the order of $[D]$ in $Br(K)$ is $\sqrt{[D:K]}$. It is also equal to the least common denominator of the numbers $inv_v(D)$.*

We now state our theorem.

Theorem 1.4.5 ([WM71]). *Let A be a simple abelian variety over $k = \mathbb{F}_q$. Let $D = End^0(A)$ and $\pi \in D$ be the Frobenius element of A. Then :*

1. *The center of D is $\mathbb{Q}(\pi)$; therefore D is a central division algebra over $\mathbb{Q}(\pi)$.*
2. *For a prime v of $\mathbb{Q}[\pi]$ over p, let $i_v = inv_v(D)$. Then*

$$inv_v(D) = \frac{ord_v(\pi)}{ord_v(q)}[\mathbb{Q}(\pi)_v : \mathbb{Q}_p]$$

   ($inv_v(D) = 0$ if v does not divide p or ∞).

3. $2\dim(A) = \sqrt{[D : \mathbb{Q}(\pi)]}[\mathbb{Q}(\pi) : \mathbb{Q}]$.

1.4.1 Some easy consequences

Theorem 1.4.6. *Let A, B be abelian varieties over a finite field k and let χ_A and χ_B be the Frobenius polynomials. Then the following statements are equivalent :*

1. *B is k-isogenous to an abelian sub-variety of A defined over k.*
2. *χ_B divides χ_A.*

Hence, A, B are k-isogenous iff $\chi_A = \chi_B$ iff A, B have the same number of points over every finite extension of k.

We can also study the two extremal cases for the endomorphism ring.

Theorem 1.4.7 ([Tat66]). *Let A be an abelian variety of dimension g over a finite field k. Let π be the Frobenius endomorphism of A and χ be its characteristic polynomial.*

1. *The algebra $F = \mathbb{Q}(\pi)$ is the center of the semisimple algebra $E = End^0(A)$.*
2. *We have*

$$2g \leq [E : \mathbb{Q}] \leq (2g)^2.$$

3. *The following statements are equivalent :*
   - $[E : \mathbb{Q}] = 2g$.
   - *χ has no multiple root.*
   - $E = F$.

- *E is commutative.*

4. *The following statements are equivalent :*
   - $[E:\mathbb{Q}] = (2g)^2$.
   - *χ is a power of a linear polynomial.*
   - $F = \mathbb{Q}$.
   - *E is isomorphic to the algebra of g by g matrices over a quaternion algebra D_p (ramified only at p and ∞).*
   - *A is k-isogenous to the g-th power of a supersingular elliptic curve, all of whose endomorphisms are defined over k.*

   One says that A is supersingular.

5. *A is k-isogenous to a power of a k-simple abelian variety iff χ is a power of a $\mathbb{Q}$-irreducible polynomial P.*

Proof. We are going to prove the second, third and fourth points.
Let

$$\chi(T) = \prod_{i=1}^{s} (T - \alpha_i)^{m_i}$$

with the α_i distinct. Then $\sum m_i = \deg \chi = 2g$ and by Th. 1.4.1 we have $[E:\mathbb{Q}] = \sum m_i^2$ so (2) follows from the obvious inequalities

$$\sum m_i \leq \sum m_i^2 \leq (\sum mi)^2.$$

We have equality on the left of this iff $m_i = 1$ for all i and then the equivalences of the statements follows easily, once we have note that, since π is semisimple, $[F:\mathbb{Q}] = s$.
We have equality on the right iff $s = 1$ and this shows the equivalence of the 3 first statements. If $F = \mathbb{Q}$, then E is a simple algebra with center $\mathbb{Q}$ for which $E_l = E \otimes \mathbb{Q}_l$ is isomorphic to $\mathrm{End}(V_l(A))$. Thus the local invariants of E are 0 at all primes of $\mathbb{Q}$ except possibly at the archimedean prime ∞ and at the prime p. Since the invariant at ∞ is 0 or $\frac{1}{2}$ and the sum of the invariant is 0 (mod 1), the invariant at p is 0 or $\frac{1}{2}$, and we conclude that E is either the algebra $M_{2g}(\mathbb{Q})$ or $M_g(D_p)$. The first possibility is excluded because an abelian variety of dimension g cannot be isogenous to the $2g$th power of an abelian variety. Therefore $E \simeq M_g(D_p)$ and there is a k-isogeny $A \sim B^g$, where B is an elliptic curve with $\mathrm{End}_k(B) \otimes \mathbb{Q} \simeq D_p$. Conversely, if this last is true then $E \simeq M_g(D_p)$ and the center F of E is $\mathbb{Q}$. Thus the last 3 statements are equivalent. □

Remark 15. When A is not simple, its Frobenius polynomial is reducible. The contrary is not true : χ may be reducible and A simple as shows the case of a supersingular elliptic curve. But A is isogenous to a power of a k-simple abelian variety iff χ is the power of a $\mathbb{Q}$-irreducible polynomial.
It is also possible that a Frobenius polynomial relative to k is irreducible but not relative

to an extension. It is the case when A/k is simple but not over an extension. When A is $\overline{k}$-simple one says that it is *geometrically simple.*
One has seen that a supersingular elliptic curve is characterized by the fact that its p-rank is 0. Is it the same in higher dimensions ? It is still the case for dimension 2 but in dimension 3, it is not : for instance the curve

$$(x^2 + y^2 + z^2 + yz)^2 = x(y^3 + x^2 z)$$

has rank 0 but is not supersingular whereas

$$(x^2 + z^2 + xy + xz)^2 = x(y^3 + x^2 z)$$

is supersingular.

Chapter 2

Automorphism group in characteristic p

Given a curve of genus $g \geq 2$ a natural finite group attached to it is its automorphism group. Find explicitly this group is hard in general but at least in characteristic 0 there exists a good bound on the order of this group. This bound is not accurate in positive characteristic anymore. The aim of this part is to show how we can replace it.

2.1 Review of Galois covers

2.1.1 Existence

We want to give here a brief review of Galois covers in a more general setting than for curves. So let X/K be an algebraic variety and G a group acting on X.

Definition 2.1.1. *We say that the set-theoretical quotient X/G is an* algebraic quotient *of X by G if there exist an algebraic variety Y and a surjective morphism $\pi : X \to Y$ such that a morphism $\rho : X \to Z$ factors through π if and only if $\rho(p) = \rho(g(p))$ for all $p \in X(\overline{K})$ and $g \in G$. We call $\pi : X \to Y = X/G$ a* Galois cover.

The condition on the functions prevents us to do something stupid like composing the map π with a purely inseparable map (which is bijective on points).
Algebraic quotient does not always exist : there are examples of algebraic varieties on which $\mathbb{Z}/2\mathbb{Z}$ acts and such that the quotients are not algebraic quotients. The study of when the algebraic quotient exists and when it is projective is a deep one, called *geometric invariant theory.* However in the cases we are interested, everything is fine.

Proposition 2.1.1. [Ser75, III.Prop.18] *Suppose that X is an affine variety with coordinate ring A and G a finite group acting on X. Then X/G in an affine algebraic variety whose coordinate ring is naturally identified with the subring A^G of elements of A fixed by G.*

By patching, one can then prove :

Proposition 2.1.2. *Let X be a quasi-projective variety and G be a finite group acting on X. Then X/G is an algebraic quotient.*

Remark 16. One can prove that if the action of G is defined over K then the quotient is also defined aver K.

If we consider now a curve X and G a finite subgroup G of $\mathrm{Aut}(X)$ the situation is even easier. Consider the field $F = \overline{K}(X)$. Recall that we have the dictionary :

$$\begin{bmatrix} \text{objects :} & \text{curves defined over } K \\ \text{maps :} & \text{non constant morphisms defined over } K \end{bmatrix}$$

$$\leftrightsquigarrow$$

$$\begin{bmatrix} \text{objects :} & \text{extension of } K \text{ of transcendental degree 1 with constant field K} \\ \text{maps :} & \text{field injections fixing } K \end{bmatrix}$$

which links

$$\begin{bmatrix} C/K & \leftrightsquigarrow & K(C) \\ \phi : C_1 \to C_2 & \leftrightsquigarrow & \phi^* : K(C_2) \to K(C_1) \\ P \in C(K) & \leftrightsquigarrow & \text{valuation ring } \mathcal{O}_P \end{bmatrix}$$

By this dictionary G induces a finite subgroup of $\mathrm{Aut}(F)$. Let $F' = F^G$ be the subfield of F of elements invariant by G. The extension F/F' is a Galois extension of group G, so F' has transcendental degree 1 over $\overline{K}$. In particular there exists a curve X' associated to F' and the quotient $X \to X' = X/G$ is algebraic.

Remark 17. One can ask the opposite problem : given a curve X' and a group G, does it exist a curve X such that $X' = X/G$? When G is abelian, this problem can be translated into the existence of isogenies of 'generalized' Jacobians [Ser75]. For instance unramified (see next section for a definition) abelian covers of an algebraic curve are in one-to-one correspondence with isogenies of its Jacobian. This is part of the so called *geometric class field theory* (see [Ser75] or [Sch90]).

2.1.2 Local behavior

In the following K will be algebraically closed (see [Sti73] for a more general treatment).
Let K be an (algebraic closed) field of characteristic $p \geq 0$. Let X be a curve over K of genus g_X. Let G be a finite subgroup of $\mathrm{Aut}(X)$ and P be a point of X. We define *the higher ramification groups* $G_i(P), i \geq -1$ by

$$G_{-1}(P) = \{\sigma \in G |\ \sigma \circ P = P\}$$

and for $i \geq 0$

$$G_i(P) = \{\sigma \in G_{-1}(P) |\ ord_p(\sigma \cdot \pi_P - \pi_P) \geq i + 1\},$$

where π_P is an uniformizer at P. The group $G_{-1}(P)$ is called the *decomposition group* of P and $G_0(P)$ is called the *inertia group* of P.

Remark 18. When K is algebraically closed (as we assume), $G_{-1}(P) = G_0(P)$ because the residue fields at P of the extension defined by $K(X) \to K(X/G)$ are both equal to K.

Remark 19. We want to emphasize that these definitions are local and in fact valid for every Galois extension of local fields with discrete valuation. Indeed, let $\pi : X \to X/G = Y$ be the cover defined by G and let $Q = \pi(P)$. We are looking at properties of the local fields extension $\mathrm{Frac}(\mathcal{O}_{X,P})/\mathrm{Frac}(\mathcal{O}_{Y,P})$. We may even complete the local fields if we want and so we obtain a particular case of the general theory developed in [Ser68, chap.4]. In particular the following results are not restricted to curves.

We have the important proposition.

Proposition 2.1.3 ([Ser68]). *There exist injective homomorphisms*

$$\vartheta_0 : G_0(P)/G_1(P) \to K^*$$

and for $i \geq 1$,

$$\vartheta_i : G_i(P)/G_{i+1}(P) \to K.$$

From this proposition, one can prove the following important properties for the groups $G_i(P)$:

1. $G_0(P) \supset G_1(P) \supset \ldots \supset G_m(P) \supsetneq G_{m+1}(P) = \{1\}$. The subgroups $G_i(P)$ are normal in $G_0(P)$.

2. If $|G_0(P)| = Ep^\alpha$ with $(E,p) = 1$ then $|G_1(P)| = p^\alpha$, $G_0(P)/G_1(P)$ is a cyclic group of order E.

3. $G_0(P)$ is the semi-direct product of $G_1(P)$ by a cyclic group of order E.

4. $\forall s \in G_0(P)$ and $\tau \in G_i(P)/G_{i+1}(P)$, $\vartheta_i(s\tau s^{-1}) = \vartheta_0(s)^i \vartheta_i(\tau)$.

5. Assume $G_0(P)$ abelian and let $e_0(P) = |G_0(P)/G_1(P)|$. If i is an integer not divisible by $e_0(P)$ then $G_i(P) = G_{i+1}(P)$.

We give also the following property, as the proof is instructive.

Lemma 2.1.1. *Let $E = |G_0(P)/G_1(P)|$ and $q_i = |G_i(P)/G_{i+1}(P)|$ ($i \geq 1$) then $E \mid (E,i)(q_i - 1)$. In particular $E \mid i(q_i - 1)$.*

Proof. One may suppose that $p > 0$ (otherwise $q_i = 1$). We follow the notations of Prop. 2.1.3.

Let $\mu_E = Im(\vartheta_0)$ be the group of Eth root of unity and $\zeta = \vartheta_0(s_0)$ be a generator of this cyclic group.

Let $i \geq 1$ and $\mathbb{F}_{q_0}$ be the field generated by $\mu = \zeta^i$ over $\mathbb{F}_p$. Let us prove that $Im(\vartheta_i)$ is a $\mathbb{F}_{q_0}$-vector space. So let $\tau \in G_i(P)/G_{i+1}(P)$ and $\sum a_j \mu^j \in \mathbb{F}_{q_0}$ with $a_j \in \mathbb{F}_p$. It's enough to show that $S = (\sum a_j \mu^j)\vartheta_i(\tau) \in Im(\vartheta_i)$. Now $S = \sum \mu^j \vartheta_i(\tau^{a_j}) = \sum (\zeta^j)^i \vartheta_i(\tau^{a_j}) = \sum \vartheta_i(s_0^j \tau^{a_j} s_o^{-1}) = \vartheta_i(\prod s_0^j \tau^{a_j} s_0^{-j}) \in Im(\vartheta_i)$. Then $q_i = |Im(\vartheta_i)| = q_0^l$ where l is the dimension of $Im(\vartheta_i)$ over $\mathbb{F}_{q_0}$. μ is a $\frac{E}{(i,E)}$-th root of unity so $\frac{E}{(i,E)}$ divides $(q_0 - 1)$. As $q_i - 1 = q_0^l - 1$ it is also a multiple of $\frac{E}{(i,E)}$. $\square$

2.2 Bound on automorphism group orders

2.2.1 Finiteness of the automorphism group

If X/K is a genus 0 curve then it is isomorphic to $\mathbb{P}^1$ and its automorphism group is isomorphic to $\mathrm{PSL}_2(K)$.
If X/K is an elliptic curve then its automorphism group is the direct product of the group of automorphisms which preserve 0 (of order $2, 4, 6, 12$ or 24) and of the group of translations.
When X/K is a genus $g_X \geq 2$ the situation is completely different : indeed we will prove the following proposition.

Proposition 2.2.1. *The automorphism group of a curve X of genus $g_X \geq 2$ is finite.*

To prove this, we first need a lemma.

Lemma 2.2.1. *If g is an automorphism of a curve, it has at most $2g + 2$ fixed points.*

Proof. Let us suppose the contrary, i.e that g has at least $2g + 3$ fixed points, called $P_1, \ldots, P_{2g+3}$. By Riemann-Roch theorem, there exists a non constant function $f \in \mathcal{L}(P_1 + \ldots + P_{g+1})$. f has at most $g + 1$ poles. The function $f - f \circ g$ has then poles inside the set $\{P_1, \ldots, P_{g+1}, g^{-1}(P_1), \ldots, g^{-1}(P_{g+1})\}$ and then has at most $2g + 2$ zeros. But all the P_i, $i = 1, \ldots, 2g + 3$ should be zeros: contradiction. □

Remark 20. We cannot assume less : for example the hyperelliptic involution on an hyperelliptic curve C of genus g has $2g + 2$ fixed points. We then obtain a map of $\mathrm{Aut}(C) \to S_{2g+2}$ which kernel is exactly the hyperelliptic involution.

So if one may find a set of $2g + 3$ points on a curve, globally invariants by all automorphisms, there exists an injective map of $\mathrm{Aut}(X)$ in S_{2g+3} (group of permutations). In particular, the group will be finite. Such sets exists for non hyperelliptic curves, for instance we can take the set of Weierstrass points. In characteristic 0, it is easy to prove that there is always $2g + 6$ such points.
In the following section, we will give (at least in characteristic 0) a way to find a bound for the order of the automorphism group.

2.2.2 Hurwitz theorem

Let G be a finite subgroup of $\mathrm{Aut}(X)$ and consider the Galois cover $\pi : X \to X/G = Y$. The ramification groups contain important information on the cover. For example, if $Q \in Y$, $|\pi^{-1}(Q)| = |G/G_0(P)|$ for P such that $\pi(P) = Q$. So $G_0(P)$ measures the ramification of the point P. Thus, points with non-trivial decomposition group are called *ramified*. When there exists a (resp. no) ramified point on X we say that the *cover is ramified* (resp. *unramified*).
Points with non trivial $G_1(P)$ are of course much more difficult to handle because all the information is not contained in the ramification index. This is reflected in the following definition :

Definition 2.2.1. *Let P be a point on X. We say that it is* wildly ramified *if $G_1(P)$ is not trivial (i.e if $p|e_Q$). Otherwise we say that P is* tamely ramified.

Remark 21. Suppose that p does not divide the order of the group G (in particular $p = 0$). Then all the points of X are tamely ramified (because $G_1(P)$ is a p-group).

Knowing the orders of the higher ramification groups allow to link the genus of X and Y as we will see now.

Theorem 2.2.1. *([Sti73]) : Let $\pi_{X/Y} : X \to Y$ be a Galois cover of degree n. For all $Q \in Y$ we define e_Q and d_Q by : if $G = Gal(X/Y)$ and $P \in X$ such that $\pi_{X/Y}(P) = Q$ then $e_Q = |G_0(P)|$ and $d_Q = \sum_0^\infty(|G_i(P)|-1)$ (as the cover is Galois this is independent of P). We then have :*

$$(2\mathrm{g}_\mathrm{X} - 2)/\mathrm{n} = 2\mathrm{g}_\mathrm{Y} - 2 + \sum_{\mathrm{Q}\in\mathrm{Y}} \frac{\mathrm{d}_\mathrm{Q}}{\mathrm{e}_\mathrm{Q}}.$$

Remark 22. There is a generalization of Hurwitz formula to non-Galois covers. It may be expressed with the degree of a divisor called *the different*. This explains the notation d_Q in the theorem (cf. [Sti73, III.5]).

If p does not divide the order of G, then $G_i(P) = \{0\}$ for $i \geq 1$. So we obtain the tame Hurwitz formula in characteristic 0 :

$$\frac{2g_X - 2}{|G|} = 2g_Y - 2 + \sum_{Q\in Y} \left(1 - \frac{1}{e_Q}\right). \tag{2.1}$$

Example 3. *Let us show how to use this equation to compute the genus of $X(N)$, for N prime, in characteristic 0. We know that $X(N) = \mathbb{H}^*/\Gamma(N)$ and that we have an exact (split) sequence*

$$1 \to \Gamma(N) \to PSL_2(\mathbb{Z}) \to L(N) := PSL_2(\mathbb{Z}/N\mathbb{Z}) \to 1$$

which leads to a Galois cover $X(N) \to X(N)/L(N) = X(1) \simeq \mathbb{P}^1$. This cover is ramified over points representing elliptic curves with extra-automorphisms and over infinity. Over $j = 0$ (6 automorphisms), it is ramified with index 3 and over $j = 1728$ (4 automorphisms) it is ramified with index 2. The infinity represents the class of the cusp $(0 : 1)$. Its stabilizer in $L(N)$ is represented by the matrix $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, so it is of index N. We can now apply Hurwitz formula :

$$\frac{2g_{X(N)} - 2}{|L(N)|} = -2 + (1 - \frac{1}{2}) + (1 - \frac{1}{3}) + (1 - \frac{1}{N}).$$

So, knowing that $|L(N)| = N(N^2 - 1)/2$, we get

$$g_{X(N)} = 1 + \frac{(N^2 - 1)(N - 6)}{24}.$$

When $\mathrm{Char}(K) = 0$ we want to give a bound on the order of the automorphism group of a curve of genus $g \geq 2$. We use equation (2.1) to find it [Har75, ex.4.2.5] :

1. Since $g_X \geq 2$, the left hand side of equation (2.1) is > 0.
2. When $g_Y \geq 0$, $e_Q \geq 2$, it is then easy to prove that the positive minimum of the above equation is reached for $g_Y = 0$ and 3 ramification points with indexes $e_{Q_1} = 2, e_{Q_2} = 3, e_{Q_3} = 7$. So the minimum value is $1/42$.
3. We conclude that if $g_X > 1$, $|G| \leq 84(g_X - 1)$.

We call this bound *Hurwitz bound.*

Remark 23. We can wonder if this bound is optimal. It is in a certain sense : the Hurwitz bound is attained over $\mathbb{C}$ for infinitely many values of g_X [McB61]. The curves which reach the bound are called *Hurwitz curves.*

Example 4. *Let X be the Klein quartic $x^3y + y^3z + z^3x = 0$ over k. If Char$(k) \neq 7$ it is a genus 3 curve so its Hurwitz bound is $84 \cdot 2 = 168$. One knows that $X \simeq X(7)$, so it is now obvious that $G = PSL_2(\mathbb{F}_7)$ is a subgroup of Aut(X). As $|G| = 168$ so $G =$ Aut(X) over $\mathbb{C}$ and the curve is a Hurwitz curve. We will see an explicit approach of the example in the Tutorial 6.4.2.*

In positive characteristic however, a curve may not respect this bound. Let us give the following example :

Example 5 ([Sub75]). *Let $X : (x^p - x)(y^p - y) = 1$ over $\overline{\mathbb{F}_p}$. The curve X is of genus $(p-1)^2$ and it is not difficult to see that $\forall a, b, c \in \mathbb{F}_p, c \neq 0$, $f_{a,b} : (x, y) \mapsto (x + a, y + b)$, $g_c : (x, y) \mapsto (cx, 1/cy)$ and $h : (x, y) \mapsto (y, x)$ are automorphisms of X. Thus X has at least $2p^2(p-1)$ automorphisms. So when $p > 37$, X does not respect the Hurwitz bound. Note that this example is important also because the curves X are ordinary (see 2.2.4). Other less obvious examples are the following :*

- *The Klein curve is isomorphic over $\overline{\mathbb{F}_3}$ to the Fermat curve $x^4 + y^4 + z^4 = 0$ and has $PSU(3, 9) \supsetneq PSL_2(\mathbb{F}_7)$ as automorphism group [Kur82].*
- *The modular curve $X(11)$ over $\overline{\mathbb{F}_3}$ has the Mathieu group M_{11} as automorphism group (and $|M_{11}/PSL_2(\mathbb{F}_{11})| = 12$) [Adl97].*

We then introduce the following definition.

Definition 2.2.2. *We say that a curve X* respects the Hurwitz bound *if the order of its automorphism group is bound by $84(g_X - 1)$.*

2.2.3 Deuring-Šafarevič formula

From now on we assume Char$(K) = p > 0$. So we will denote $K = k$.
We saw in 1.3 that there exists a second important invariant, the p-rank γ_X. We have for it an analogue of the Hurwitz theorem :

Theorem 2.2.2. *[Sub75] If $G = Gal(X/Y)$ is a p-group then*

$$\frac{\gamma_X - 1}{|G|} = \gamma_Y - 1 + \sum_{Q \in Y} (1 - e_Q^{-1}).$$

Remark 24. When G is not a p-group, it is still possible to get some information. For example [Sta04] : Let r the number of fixed points of G on X and let p^n be the p-part of the order of G; then

$$\gamma_X \equiv 1 - r \pmod{p^n}.$$

Thanks to this formula we can obtain an upper bound of the number $m+1$ of non trivial ramification groups (with the convention $m = -1$ if the point is not ramified).

Proposition 2.2.2. $\sum_{i=2}^{\infty}(|G_i(P)| - 1) \leq 2(g_X - \gamma_X)$. *In particular we have the inequality* $m \leq \frac{2(g_X - \gamma_X)}{p-1} + 1$.

Proof. (Following a similar proof by Nakajima [Nak87].)
Let $H = G_1(P)$: it is a p-group. Let us apply Hurwitz and Deuring-Šafarevič formulas to the cover $X \to Z = X/H$:

$$\frac{2g_X - 2}{|H|} = 2g_Z - 2 + \sum_{S \in Z} \frac{d_S}{e_S}$$

and

$$\frac{\gamma_X - 1}{|H|} = \gamma_Z - 1 + \sum_{S \in Z} (1 - e_S^{-1}).$$

We get

$$\frac{2(g_X - \gamma_X)}{|H|} = 2(g_Z - \gamma_Z) + \sum_{S \in Z} \frac{r_S}{e_S}$$

where $r_S = d_S - 2(e_S - 1)$. For $S \in Z$ let $Q \in X$ such that $\pi_{X/Z}(Q) = S$. Then $e_S = |H_0(Q)|$. As H is a p-group, $H_1(Q) = H_0(Q)$ so $r_S = \sum_{i=2}^{\infty}(|H_i(Q)| - 1)$. In particular $r_S \geq 0$. Then

$$r_S \leq (2e_S/|H|)(g_X - \gamma_X) \leq 2(g_X - \gamma_X).$$

Now $r_S \geq (m-1)(p-1)$ which gives the result. □

Remark 25. We notice that when the curve is ordinary then $G_2(P) = \{1\}$ for all $P \in X$ (is the converse true ?).

2.2.4 Other important tools

We list here other important results without any proof.

Roquette's theorem

Theorem 2.2.3 ([Roq70], Roquette). *If $p > g_X + 1$ the cover $X \to X/Aut(X)$ is tamely ramified with one exception : X is isomorphic to the hyperelliptic curve $y^2 = x^p - x$ (so $p = 2g_X + 1$ and $|G| = 2p(p^2 - 1)$). In particular X respects the Hurwitz bound.*

This is particularly useful when one studies the reduction of a curve modulo large primes.

Singh cases

By sharpening the Hurwitz theorem, Singh [Sin74] shows that if $Y = X/G$ is of genus 0 and if we denote by r the number of ramification points of Y and e_i, $1 \leq i \leq r$ the ramification indexes , if the curve does not respect the Hurwitz bound then we have only the following possibilities :

- $r = 4$ and $e_1 = e_2 = e_3 = e_4 = 2$.
- $r = 3$. If we suppose $e_1 \geq e_2 \geq e_3$ then the possibilities are gathered in the following chart.

e_1	3	4	6	5	4	3	e arbitrary
e_2	3	4	3	3	3	3	2
e_3	3	2	2	2	2	2	2

- $r = 1$ and the point is wildly ramified.
- $r = 2$ and one point at least is wildly ramified.

Then Singh gives an upper bound for the automorphism group (in g^3 : compare with Hurwitz bound) :

$$\frac{4pg^2}{p-1}\left(\frac{2g}{p-1} + 1\right).$$

Remark 26. Be careful : there is an article by Henn with a bound $3(2g)^{5/2}$ which has been used after that in other articles. But the proof is wrong.

Remark 27. Much more is known : if $\phi : X \to Y$ is a Galois cover ramified over certain fixed points, Abhyankar's conjecture (proved by Raynaud and Harbater) determines exactly which groups can be the Galois group of ϕ. However it is still an open problem to determine which inertia groups and filtrations of higher ramification groups can be realized (see however [Pri03] for the case of one ramification point).

Lifting

Another possibility is to see if one can lift the problem to characteristic 0. More precisely, suppose that there exist a complete valuation ring R with residue field k and field of fraction K of characteristic 0 (otherwise the lift problem is trivial). Given $\pi : X \to Y = X/G$ a Galois cover over k, a lifting of π is a Galois cover $\mathcal{X} \to \mathcal{Y}$ over R with group G

and special fiber the cover π.
Of course, as not every curve respects the Hurwitz bound, this is not always possible. But we have the following important theorem :

Theorem 2.2.4. *[Gro71, XIII.2.12] If the cover $X \to X/Aut(X)$ is tame, it can be lifted to characteristic* 0.

Remark 28. Generalization of this proposition to the case of wild ramification is a fruitful and very active research. The situation of p-cyclic action is quite well understood now but as far, the general case is beyond one's grasp. For example the famous Oort conjecture (any cyclic cover has a lifting to characteristic 0) is still an open question (see [Liu03] for a survey of these questions).

As a basic application of the results we give the following example.

Proposition 2.2.3. *Let $\mathcal{C}_p : y^3 + x^4 + 1 = 0$ over $\overline{\mathbb{F}_p}$. For $p > 3$ the curve $\mathcal{C}_p$ has an automorphism group of order* 48.

Proof. Let $C/\mathbb{Z}$ be the scheme defined by the equation $y^3 z + x^4 + z^4 = 0$. We denote by $\mathcal{C}$ the projective quartic $C \otimes \overline{\mathbb{Q}}$ and by $\mathcal{C}_p$ the curve $C \otimes \overline{\mathbb{F}_p}$.
The curve $\mathcal{C}$ is a non singular quartic. [KS96] shows that its automorphism group is a group G of order 48.
It is easy to see that when $p = 2$ (resp. $p = 3$) the curve C_p is singular : $y^3 = (x+1)^4$ (resp. $(-y)^3 = x^4 + 1$). A straightforward computation shows that it is smooth if $p > 3$. From now on, we suppose $p > 3$. We want to study the automorphism groups G_p of the curves $\mathcal{C}_p$.

Since we have good reduction $G \subset G_p$ (Prop.5.3.1) and so 48 divides $|G_p|$.But, as many examples have shown, it is not clear that equality holds.
By Roquette's theorem, as $\mathcal{C}_p$ is a non singular quartic, it is not hyperelliptic so we know that the covering $\mathcal{C}_p \to \mathcal{C}_p/G_p$ is tamely ramified. In particular, $|G_p| \leq 168$. So if $G_p \neq G$, the order of G_p is $2 \cdot 48$ or $3 \cdot 48$. We will show that these two cases are not possible.

- Suppose $|G_p| = 96$. The covering $\mathcal{C}_p \to \mathcal{C}_p/G$ is ramified over 3 points with indexes $2, 3, 12$ or $2, 4, 6$. Imitating a classical argument by Serre [Ser96], we see that, since G is normal in G_p, there is an action of G_p on $\mathcal{C}_p/G = \mathbb{P}_1$ which stabilizes the three ramification points (since the indexes are different). So the action is trivial and $G_p = G$.

- Suppose $|G_p| = 144$. Since the cover is tamely ramified, we may lift the curve and the group $|G_p|$ to characteristic 0. Now, following the classification of [Bou98, p. 85], we see that there is no quartic with automorphism group of order 144.

□

Relation with the automorphisms of the Jacobian

Note that thanks to Torelli theorem (Cor. 5.2.2) $|\mathrm{Aut}(X)|$ and $|\mathrm{Aut}(\mathrm{Jac}(X), \Theta)|$ agrees up to a possible factor of 2. So it is very tempting to study this last one. This relation is one of the reasons why usually one suspects curves with big automorphism group to have a supersingular Jacobian (as the endomorphism group of these abelian varieties is bigger).

For a general abelian variety, we have the following proposition :

Proposition 2.2.4. *Let f be a (finite) automorphism of a polarized abelian variety (A, λ) and $n \geq 3$ be an integer prime to the characteristic. If $f|A[n] = 1$ then $f = 1$.*

Proof. Assume the contrary, i.e. $f \neq 1$. As f has finite order, by eventually passing to a power of f we may assume that f is of order q for some prime q. Since the only unipotent automorphism of (A, λ) is the identity (see the beginning of the proof of Lem.1.2.3 and use the fact that for an automorphism f, $f \circ f^\dagger = 1$), there is an eigenvalue ζ of f which is a primitive q-root of unity. By assumption $A[n] \subset \ker(1 - f)$. Hence there is a $g \in \mathrm{End}(A)$ such that $ng = 1 - f$. This implies that there is an algebraic integer η, namely an eigenvalue of g, such that

$$n\eta = 1 - \zeta.$$

Applying the norm of the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ we get

$$n^{q-1} N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\eta) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 - \zeta) = (1 - \zeta) \ldots (1 - \zeta^{q-1}) = q.$$

This is impossible, since q is a prime and $n \geq 3$. $\square$

Remark 29. It can be proved [BL92, 5.1.9] that the automorphism group of a polarized abelian variety is finite. We have thus a representation of $\mathrm{Aut}(A, \lambda)$ in $\mathrm{Aut}(A[n]) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$.

We then get that $|\mathrm{Aut}(A, \lambda)|$ is smaller than $|\mathrm{GL}_{2g}(\mathbb{Z}/3\mathbb{Z})|$ which is exponential in g. So this bound is not very useful in our case. But let us suppose that there exists $n \geq 3$, prime to p such that all n-torsion points of the Jacobian J of X are defined over a finite field k_0. Then each automorphism α of X is defined over k_0 : indeed for all $\sigma \in \mathrm{Gal}(k/k_0)$, $\alpha_J^{-1} \circ \alpha_J^\sigma$ is an automorphism of the polarized abelian variety J fixing the points of order n. So it is the identity and by Torelli theorem we conclude that $\alpha = \alpha^\sigma$ so α is defined over k_0.

If we have a bit more structure on the Jacobian (CM abelian variety, simple, Galois structure,...), even more things can be said. As a trivial example :

Proposition 2.2.5. *Let X be a curve of genus $g > 1$ defined over $k_0 = \mathbb{F}_q$ and let χ be the Frobenius polynomial. Suppose that there exists $n \geq 3$ and prime to p such that the Jacobian of X has all its n-torsion points defined over k_0 and that χ has no multiple root. Then $|Aut(X)| \leq 4g_X + 4$.*

Proof. We have that $\mathrm{Aut}_k(X) = \mathrm{Aut}_{k_0}(X)$ and we have an injection of this group in $E = \mathrm{End}_{k_0}(\mathrm{Jac}(X))$. Since χ has no multiple root we know that E is commutative so is $\mathrm{Aut}(X)$. A general theorem on abelian automorphism groups [Nak87b] gives then the bound. $\square$

Nakajima theorem

We have seen in 2.2.4 that the general bound of Singh is quite high compared with Hurwitz bound. Is it possible with some additional conditions on X to do better ? A great improvement is the following theorem [Nak87].

Theorem 2.2.5 (Nakajima). *Let X be a curve of genus greater or equal to 2 and $G = Aut(X)$. Let H be a p-Sylow subgroup of G.*

1. *If $\gamma_X \geq 2$ then*
$$|H| \leq c_p(\gamma_X - 1)$$
with $c_p = p/(p-2)$ if $p \geq 3$ and $c_2 = 4$.

2. *If $\gamma_X = 1$ and $p \geq 3$ then X respects the Hurwitz bound.*

3. *If $2 \leq \gamma_X \leq p - 2$ ($p \geq 5$) then X respects the Hurwitz bound.*

4. *If $1 \leq g_X - \gamma_X \leq (p-2)/2$ ($p \geq 5$) then X respect the Hurwitz bound.*

5. *If X is ordinary (i.e $\mathrm{g_X} = \gamma_{\mathrm{X}}$) then $G_2(P) = \{1\}$, $\forall P \in X$. Moreover $|G| \leq 84(g_X - 1)g_X$.*

Recall that the ordinary curves are the generic case (i.e they form an open dense subset in the moduli space M_g).
An application of this theorem is given in [Rit02] where the following theorem is proved.

Theorem 2.2.6. *Let $p > 3$ and q be a prime number different from p. If the curve $X(q) \otimes \overline{\mathbb{F}_p}$ is ordinary then its automorphism group is $PSL_2(\mathbb{F}_q)$.*

Remark 30. Michael Zieve has sharpened Nakayama's theorem by showing that for all but finitely many exceptions (for each genus) the bound is in fact in $g_X^{3/2}$ and is optimal in this sense.
Another interesting question is then to go one step further : what can be said about the groups $G_2(P)$? See [Mat04].

Chapter 3

Maximal curves

3.1 Introduction

Recall some results of Chapter 1. If C is a curve of genus g over a finite field $k = \mathbb{F}_q$, there exists a polynomial f of degree $2g$ such that $f(T) = \prod(1 - T\alpha_i)$ with $|\alpha_i| = \sqrt{q}$ and

$$Z(C/k;T) = \frac{f(T)}{(1-T)(1-qT)}.$$

Corollary 1.2.1 says also that $|C(k)| = 1 + q - \sum \alpha_i$. But this implies that

$$||C(k)| - 1 - q| \leq |\sum \alpha_i| \leq \sum |\alpha_i| \leq 2g\sqrt{q}.$$

This has two easy consequences :

1. if q is large enough compared to g, C has always at least one rational point.
2. $|C(k)| \leq 1 + q + 2g\sqrt{q}$. This bound is know as *Weil bound.*

This leads us to introduce the following definition.

Definition 3.1.1. *Let $g \geq 0$ be an integer and q a prime power. We denote by $N_q(g)$ the maximal number of points of a curve of genus g over $\mathbb{F}_q$.*

For several decades, number theorists assumed that the Weil bound was optimal until 1973 when Stark improved the bound by two in a particular case.
Since, there is a (mathematical) world-wide game consisting at finding the exact value of $N_q(g)$. Indeed, except for $g = 1, 2$ this value is not known in general and so things are handle case by case. A chart of the values in characteristic 2 and 3 may be found in [GV03].
There are two strategies to tackle this problem :

1. Decrease the bound : we are going to give in the following some arguments to do that. It is only a small part of the whole picture as the literature on the subject is really extensive.

2. Constructing/proving existence of curves : we are not going to deal with this question (but see Tutorial 6.4). Let us just say that roughly speaking on can distinguish the following approaches :
   - Methods from general class field theory (powerful but not explicit);
   - Methods from class field theory based on Drinfeld modules of rank 1 (explicit);
   - Fiber products of Artin-Shreier curves;
   - Towers of curves with many points;
   - Miscellaneous methods as : formulas for $N_q(1), N_q(2)$, explicit curves, e.g. Hermitian curves, Klein's quartic, modular curves, quotient of curves with many points and curves obtained by computer search.

Except for their own mathematical interest, these researches have also applications in coding theory (which was actually one of the catalyser of this quest). We will see how in 3.4. This leads also to asymptotic problems that we will discuss briefly also in 3.3.2.

Remark 31. This domain is quite new : note that the intuitive fact that $\lim_{q\to\infty} N_q(g) = \infty$ has been proved only in 2002 [KWZ] !

3.2 The case $g = 0, 1$ and 2

The case of genus 0 is trivial : indeed a genus 0 curve with a rational point over $\mathbb{F}_q$ in $\mathbb{F}_q$-isomorphic to $\mathbb{P}^1$ and has then $q+1$ rational points. This gives $N_q(0) = q+1$.
The genus 1 case is alright also. By Th.1.4.1 one sees that we have only to look at what the minimum sum of the trace a of the Frobenius polynomial $T^2 - aX + q$ can be. We have $a \geq -2\sqrt{q}$. So we would like to take $a = -\lfloor 2\sqrt{q} \rfloor$. But the q-Weil integer attached to this polynomial may be associated to an abelian surface with Frobenius polynomial $\chi(T) = (T^2 + \lfloor 2\sqrt{q} \rfloor T + q)^2$. We can check that with Th.1.4.5. This leads to the following cases :

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor \text{ if } \ p|(q+1+\lfloor 2\sqrt{q} \rfloor) \text{ and if } q = p^e \text{ with } e \text{ odd;} \\ q + 1 + \lfloor 2\sqrt{q} \rfloor \text{ otherwise.} \end{cases}$$

We give here for reference the case of genus 2 which is due to Serre.

Theorem 3.2.1 ([Ser85],Serre). *If q is a square different from 4 and 9 then*

$$N_q(2) = q + 1 + 4\sqrt{q}.$$

Moreover $N_4(2) = 10$ and $N_9(2) = 20$.
If q is not a square, we denote $q = p^e$ and $m = \lfloor 2\sqrt{q} \rfloor$. We say that q is special *if one of the following properties is satisfied*

- *$p|m$.*
- *it exists an integer x such that $q = x^2 + 1$.*

- *it exists an integer x such that $q = x^2 + x + 1$.*
- *it exists an integer x such that $q = x^2 + x + 2$.*

If q is non special then

$$N_q(2) = q + 1 + 2m.$$

If q is special then

$$N_q(2) = \begin{cases} q + 2m \text{ if } \{2\sqrt{q}\} \geq \frac{\sqrt{5}-1}{2}; \\ q + 2m - 1 \text{ otherwise} \end{cases}$$

where $\{\}$ denotes the fractional part of the number.

The main ingredients to prove this theorem are Torelli theorem and some study of indecomposable hermitian forms [AN65].

3.3 Decreasing the bound

3.3.1 General arguments

We are going to give general arguments (i.e which are good for $g \gg q$) which follow Serre's idea of 'formules explicites'. Let us start with Serre's original improvement.

Theorem 3.3.1. *For every curve $C/\mathbb{F}_q$ of genus g, on has that*

$$|C(\mathbb{F}_q)| \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

Proof. We have that $|C(\mathbb{F}_q)| = q + 1 - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i})$ where $\overline{\alpha_i}$ denotes q/α_i (see 1.2.3). Put

$$x_i = \lfloor 2\sqrt{q} \rfloor + 1 + \alpha_i + \overline{\alpha_i}.$$

By the Riemann hypothesis, x_i are totally positive algebraic integers. Therefore their product is at least 1. It follows from the arithmetic-geometric mean inequality that

$$\frac{1}{g}\sum_{i=1}^{g} x_i \geq \left(\prod_{i=1}^{g} x_i\right)^{1/g} \geq 1.$$

So we have $\sum x_i \geq g$ which is easily seen to imply the result. $\square$

A second improvement is due to Ihara. Consider C also on $\mathbb{F}_{q^2}$. We have

$$\begin{aligned} |C(\mathbb{F}_q)| \leq |C(\mathbb{F}_{q^2})| &= q^2 + 1 - \sum_{i=1}^{g}(\alpha_i^2 + \overline{\alpha_i}^2) \\ &= q^2 + 1 + 2gq - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i})^2 \\ &\leq q^2 + 1 + 2gq - \frac{1}{g}\left(\sum_{i=1}^{g} \alpha_i + \overline{\alpha_i}\right)^2 \end{aligned}$$

The last inequality is Cauchy-Schwartz (with the vectors $(\alpha_1, \ldots, \alpha_g)$ and $(1, \ldots, 1)$). We conclude that

$$|C(\mathbb{F}_q)| \leq q^2 + 1 + 2qg - \frac{1}{g}(|C(\mathbb{F}_q)| - q - 1)^2.$$

Theorem 3.3.2.

$$|C(\mathbb{F}_q)| \leq q + 1 + (\sqrt{(8q+1)g^2 + 4(q^2 - q)g} - g)/2$$

which is better than Weil bound if $g \geq (q - \sqrt{q})/2$.

Now we come to the best known estimate due to Drinfeld and Vlădut. The proof is an extension of Ihara's argument. It involves a consideration of all finite extensions of $\mathbb{F}_q$. As before we will write b_d for the number of places of C of degree d, i.e b_d is the number of points in $X(\overline{\mathbb{F}_q})$ of degree d up to Galois conjugacy. So we have $|C(\mathbb{F}_{q^m})| = \sum_{d|m} db_d$. Let $\Psi(T) = \sum_{n=1}^{\infty} c_n T^n$ be a polynomial (i.e $c_n = 0$ for n large enough) with non negative coefficients for which

$$\Psi(t) + \Psi(\bar{t}) + 1 \geq 1 \text{ for all } t \in \mathbb{C} \text{ with } |t| = 1. \tag{3.1}$$

By $\Psi_d(T)$ we denote the polynomial $\sum_{n \equiv 0 \pmod d} c_n T^n$.

Theorem 3.3.3. *Let C be a curve over $\mathbb{F}_q$ of genus g and $\Psi(T)$ be a polynomial as above. We have*

$$\sum_{d \geq 1} db_d \Psi_d(q^{-1/2}) \leq g + \Psi(q^{1/2}) + \Psi(q^{-1/2}).$$

Proof. As usual, let α_j denote the zeros of χ. By the Riemann hypothesis, we have $\alpha_j = \sqrt{q}e^{i\vartheta_j}$ with $\vartheta_j \in \mathbb{R}$. Moreover suppose we have ordered the α_j such that $\vartheta_{g+j} = -\vartheta_j$. We have that

$$|C(\mathbb{F}_{q^n})| = q^n + 1 - q^{n/2} \sum_{j=1}^{g} (e^{in\vartheta_j} + e^{-in\vartheta_j}).$$

So

$$\begin{aligned} 0 \leq \sum_{j=1}^{g} (\Psi(e^{i\vartheta_j}) + \Psi(e^{-i\vartheta_j}) + 1) &= g + \sum_{j,n} c_n (e^{in\vartheta_j} + e^{-in\vartheta_j}) \\ &= g + \sum_{n \geq 1} q^{-n/2} c_n (q^n + 1 - |C(\mathbb{F}_{q^n})|) \\ &= g + \Psi(q^{1/2}) + \Psi(q^{-1/2}) - \sum_{d \geq 1} \sum_{n \equiv 0 \pmod d} q^{-n/2} db_d c_n \end{aligned}$$

and the inequality follows. $\square$

The theorem clearly implies that (*Oesterlé's bound*) :

$$|C(\mathbb{F}_q)| - 1 \leq \frac{g + \Psi(q^{1/2})}{\Psi(q^{-1/2})}.$$

If one takes $\Psi(T) = T/2$ one finds Weil bound. On can try also $\Psi = (4T + 3T^2 + 2T^3 + T^4)/5$.

Remark 32. For q and g fixed there is an explicit optimal Ψ (see [Sch90]).

Example 6. *Let fix $g = 3$ and $q = 2$. The Weil bound is approximately 11.48. Serre's bound is 9, Ihara's bound is 8. With our polynomial we can find 7. We can find this bound in another way : we know that a genus 3 non hyperelliptic curve C can be embedded as a plane quartic, so*

$$|C(k)| \leq \max(\underbrace{|\mathbb{P}^2(k)|}_{\textit{non hyperelliptic}}, \underbrace{2|\mathbb{P}^1(k)|}_{\textit{hyperelliptic}}) \leq \max(4+2+1, 2\cdot(2+1)) \leq 7.$$

Moreover we have $N_2(3) = 7$ since the curve

$$y^2z^2 + yz^3 + xy^3 + x^2y^2 + x^3z + xz^3 = 0$$

reaches this bound.

Even with the best optimization there are a lot of examples where the bound is lower. We will see one in section 3.3.3.

3.3.2 Asymptotics

One fixes a finite field $\mathbb{F}_q$. One wants to study the behavior of $N_q(g)$ when g is large. It is classical to study the quotient $N_q(g)/g$, and more precisely the number

$$A(q) := \lim_{g\to\infty} \sup \frac{N_q(g)}{g}.$$

From the work done in 3.3.1, one has the following upper bounds for $A(q)$.

Theorem 3.3.4.
1. *Weil's bound : $A(q) \leq 2\sqrt{q}$.*
2. *Serre's bound : $A(q) \leq \lfloor 2\sqrt{q} \rfloor$.*
3. *Ihara's bound : $A(q) \leq \sqrt{2q} - \frac{1}{2}$.*
4. *Drinfeld and Vlăduț's bound : $A(q) \leq \sqrt{q} - 1$.*

Proof. Only the last point requires some explanations. From Th.3.3.3 we see that

$$A(q) \leq \frac{1}{\Psi(q^{-1/2})}.$$

We must choose our polynomial $\Psi(T)$ in order to get an estimate for $A(q)$. The larger we can take the c_n, the better the estimate will be. However we have that

$$0 \leq \frac{1}{\pi}\int_0^{2\pi}(1+\Psi(e^{i\vartheta})+\Psi(e^{-i\vartheta}))(1-\cos(n\vartheta))d\vartheta = 1-c_n.$$

So $c_n \leq 1$ and we cannot choose all $c_n = 1$ since they should be zero for large n. We will instead choose a sequence of polynomials whose coefficients approach 1. For instance, let us take

$$\Psi(T) = \sum_{i=1}^{N}(1-\frac{i}{N+1})T^i.$$

One verifies that

$$1+\Psi(T)+\Psi(T^{-1}) = \frac{1}{N+1}(1+T+\ldots+T^N)(1+T^{-1}+\ldots+T^{-N})$$

which proves the condition (3.1).
It is easy to see that this gives a decreasing sequence of bounds on $A(q)$, the limit of which is $\sqrt{q}-1$. □

3.3.3 Special arguments

A lot of arguments have been developed. We will give some by K. Lauter and E. Howe. Note that these arguments have been implemented in MAGMA (`htpp://alumnus.caltech.edu/~however/papers/paper25.html`) which allows a fast way to decrease the bound.
We are going to give here two of them : the resultant argument and the descent argument.

Genus 5 over $\mathbb{F}_3$

This is part of an article of Lauter [Lau99].
We want to find the value of $N_3(5)$. Using Oesterlé's bound, on finds that $N_3(5) \leq 14$. We will show now that in fact there is no genus 5 curve with 14 points on $\mathbb{F}_3$.
Let us start in general with a curve of genus g over $\mathbb{F}_q$. We will denote $m = \lfloor 2\sqrt{q} \rfloor$. The first thing to do is to generate all possible zeta functions. We have the following natural definition :

Definition 3.3.1. *A curve $C/\mathbb{F}_q$ of genus g is said to have* a k-defect *if it fails to reach Serre's bound by k, i.e $|C(\mathbb{F}_q)| = q+1+gm-k$.*

We will not look at the Frobenius polynomial $\chi(T) = \prod(T-\alpha_i)$ but rather at $P(X) = \prod(X-(m+1-\alpha_i-\overline{\alpha_i}))$. This polynomial can be easily computed from χ by the formula

$$P(X)^2 = \text{Resultant}(\chi(T), T^2+T(X-m-1)+q).$$

Conversely, one may find back $\chi(T) = T^g P(m+1+T+q/T)$.
It is then a monic polynomial in $\mathbb{Z}[X]$ such that all its root are real and positive. Thus we define the set

$$F_k = \{X^d - a_1 X^{d-1} + \ldots + a_d \in \mathbb{Z}[X], a_1 = d+k \text{ and all roots are real } > 0\}.$$

Let F_k^{irr} be the subset of F_k consisting of irreducible polynomials. It follows from Siegel's theorem that F_k^{irr} is a finite set for $k \geq 0$. For a fixed d, the set of elements of F_k of degree d is also finite and can be listed by taking all products of elements f_j of degree d_j in $F_{k_j}^{\mathrm{irr}}$ such that $\sum k_j = k$ and $\sum d_j = d$.

Definition 3.3.2. *We say that a curve has* Zeta function of type $(x_1, \ldots, x_g)$ *if* $\{\alpha_i, \overline{\alpha_i}\}$ *is the family of g conjugate pairs of eigenvalues of Frobenius acting on the Jacobian of the curve, and* $x_i = -(\alpha_i + \overline{\alpha_i})$.

The $m+1-x_i$ are totally positive algebraic integers, so if

$$\sum x_i = gm - k$$

then

$$P(X) = \prod (X - (m+1-x_i)) \in F_k,$$

since $\deg P = g$ and $a_1 = g+k$.
For $k \leq 1$ we list here the possible types [Lau01].

k	$(x_1, \ldots, x_g)$	g
0	$(m, \ldots, m)$	
1	$(m, \ldots, m, m-1)$	$g \geq 1$
	$(m, \ldots, m, m + \frac{-1+\sqrt{5}}{2}, m + \frac{-1-\sqrt{5}}{2}$	$g \geq 2$

For each pair (q, g), an entry might not correspond to the Zeta function of a curve for a number of possible reasons. Here are three such reasons.

1. Since the eigenvalues of the Frobenius endomorphism have absolute value $\sqrt{q}$, the x_i must satisfy $|x_i| \leq 2\sqrt{q}$.

2. One has $f(T) = \prod(1 + x_i T + qT^2)$ and the Zeta function is

$$Z(C/\mathbb{F}_q; T) = \frac{f(T)}{(1-T)(1-qT)}$$

   As for the Jacobian of a curve, we have seen in 1.2.5

$$\frac{1}{Z(C/\mathbb{F}_q; T)} = \prod (1 - t^i)^{b_i}$$

   one can eliminate entries that does not fullfill the condition $b_i \geq 0$ (it is the number of places of degree i).

3. An entry does not correspond to a curve if the Jacobian admits a non-trivial decomposition into a product of polarized abelian varieties. If $P(X)$ can be factored as $P(X) = r(X)s(X)$ with $r, s \in \mathbb{Z}[X]$ non constant polynomials such that $\text{Resultant}(r, s) = \pm 1$ then P can be eliminated.

We apply now these ideas to the case of genus 5. We suppose that there exists a curve of genus 5 over $\mathbb{F}_3$ with 14 rational points. After listing the possible Zeta functions, we see that argument 1 and 2 eliminate all possibilities except one polynomial which is handled by the last argument.
In Tutorial 6.4 we construct a curve with 13 rational points so $N_3(5) = 13$.

Descent argument

Let k be a finite field and k_1 be an extension. If C_1 is a curve over k_1 , its Jacobian J_1 is defined over k_1. On gives a k-structure on J_1 compatible with the polarization λ_1. It consists in a couple (J, λ) where J is an abelian variety over k, a polarization λ defined over k and an isomorphism f between (J, λ) and (J_1, λ_1). Thanks to Torelli's theorem and some descent theory one can go from the Jacobian to the curve.

Theorem 3.3.5. *Suppose that C_1 is hyperelliptic. There exists an unique k-structure over C_1 compatible with its k_1-structure and whose Jacobian is (J, λ).*

Proof. Using the automorphism $\psi_{J,\sigma}$

$$\begin{tikzcd} J_1 \arrow[rr, "\psi_{J,\sigma}"] & & J_1^\sigma \\ & J \arrow[ul, "f"] \arrow[ur, "f^\sigma"'] & \end{tikzcd}$$

constructed from the generator $\sigma \in \text{Gal}(k_1/k)$, we can descend it to an automorphism $\psi_\sigma : C_1 \to C_1^\sigma$ by Th.5.2.1. This automorphism verifies the cocycle relation verified by $\psi_{J,\sigma}$. This shows that C_1 descends to a curve C/k by Cor.5.2.1. $\square$

In the same way, we can prove.

Theorem 3.3.6. *Suppose that C_1 is non hyperelliptic. There exists then a k-structure C on C_1, compatible with its k_1-structure and a homomorphism $\epsilon : Gal(k_1/k) \to \{\pm 1\}$ such that its Jacobian is isomorphic to the ϵ-twist of (J, λ).*

We are now interested in the following particular case (see also [Lau01, Appendix]).

Proposition 3.3.1. *Let C be a curve over $\mathbb{F}_q$, $q = p^e$, e odd, of genus g, $g \geq 2$, with eigenvalues of Frobenius $\{\pi, \overline{\pi}\}$ repeated g times. If*

$$\pi = \sigma^e \textit{ with } \sigma \in \mathbb{Z}[\pi],$$

then C has a $\mathbb{F}_p$-structure with Frobenius endomorphism σ.

Proof. The idea of the proof is as follows. If the Jacobian of the curve descends to $\mathbb{F}_p$ with its polarization, then the curve also descends by Th. 3.3.5 and 3.3.6 (because k_1/k is of odd degree the twist is trivial). In order to descend the Jacobian, it is necessary and sufficient that σ factors as

$$\sigma = \phi \circ \mathrm{Fr},$$

where Fr is the relative Frobenius map and ϕ is an isomorphism. The fact that σ satisfies this condition if $\sigma \in \mathbb{Z}[\pi]$ with $\pi = \sigma^e$ and $q = p^e$ follows from the following argument : we have $\sigma = a_0 + \ldots + a_n\pi^n$ with $a_i \in \mathbb{Z}$. The tangent map of π is zero. So the tangent application of σ is the homotethy a_0. But the eth power of this application is zero so a_0 is divisible by p so the tangent map of σ is zero. This implies that σ is zero on the kernel of Fr which gives the result by comparison of the degrees.
To show that the principal polarization also descends, it is necessary and sufficient to show that

$$\sigma\sigma^\dagger = p.$$

Indeed the polarization λ_1 is rational over $\mathbb{F}_p$ iff it commutes with σ. Of course it is the case since σ is a polynomial in π (which commutes by hypothesis with λ_1). □

Example 7. *Let C be a curve of genus g over $\mathbb{F}_q$ with 0-defect. Then the eigenvalues are $\{\pi, \overline{\pi}\}$ repeated g times, with*

$$\pi = \frac{-m \pm \sqrt{m^2 - 4q}}{2}.$$

Suppose that $q = 2^3$ then $m = 5$ and $\pi = \frac{-5-\sqrt{-7}}{2} = \sigma^3$ with $\sigma = \frac{1+\sqrt{-7}}{2}$, $\sigma = -\pi - 2$. So we can apply the proposition and we can descend the curve C over $\mathbb{F}_p$. One has

$$|C(\mathbb{F}_2)| = p + 1 - gtr(\sigma) = 2 + 1 - g$$

which is impossible for $g \geq 4$. So there does not exist a curve with 0-defect over $\mathbb{F}_8$ when $g \geq 4$.

3.4 Codes

This is part of [TV91].
Linear codes are a nice domain of applications of the theory we have developed so far.

3.4.1 Definitions

Let A be a finite set of order q, which we call an *alphabet.* The set A^n is equipped with the *Hamming metric* : the distance $d(a, b)$ is the number of coordinates in which a and b differ:

$$d((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = |\{i | a_i \neq b_i\}|.$$

Any non-empty subset $C \subset A^n$ is called a *$q-ary$ code* of length n. The *log-cardinality* is $k = \log_q(|C[)$. The *minimum distance* is defined as

$$d = \min\{d(a,b)|a,b \in C, a \neq b\}.$$

A code with these parameters is called an $[n,k,d]_q$-code. The following relative parameters are also useful : the *rate* $R = k/n$ and the *relative minimum distance* $\delta = d/n$.
Let us briefly explain why codes are called error-correcting. Start with a given message which is long enough and written in the alphabet A. When this message is transmitted over a channel it is distorted by random fluctuations (noise). Here is a way out. Take an $[n,k,d]_q$-code C. Let for simplicity k be an integer. Cut the message into pieces of length k each. Map every word of length k to an element of C, i.e fix an embedding $E : A^k \hookrightarrow C \subset A^n$, and instead of the piece $a \in A^k$ of the message let us transmit the corresponding word $E(a)$ of length n (we encode the message). The transmission is now $1/R$ times slower, which justifies the term rate for R. On the other end of the channel, we obtain a distorted word $E(a)' \in A^n$ and we transform it into the nearest word $E(a)'' \in C$ (i.e we decode the message). If the number of distortions is at most $\lceil (d-1)/2 \rceil$, then $E(a)'' = E(a)$, i.e the decoding is correct.
Therefore, a 'good' code is a code with large n and R, δ as close as possible to 1.
Both for the construction of good codes and for the design of algorithm of coding and decoding, the notion of a code over an arbitrary alphabet is too poor in structure.

Definition 3.4.1. *Let $A = \mathbb{F}_q$ with $q = p^m$. A* linear code *C of length n is a linear subspace $C \subset \mathbb{F}_q^n$. For linear code $k = \dim C$, $d = \min\{|a|, a \in C, a \neq 0\}$ where $|a| = |\{i | a_i \neq 0\}|$ being the* weight *of a.*

Example 8. *$C = \mathbb{F}_q^n$ is an $[n,n,1]_q$-code.*
$C = \{(v_1, \dots, v_n) \in \mathbb{F}_q^n / \sum v_i = 0\}$ is a $[n, n-1, 2]_q$ code.
Let $\mathcal{P} = \{P_1, \dots, P_n\} \subset \mathbb{F}_q$. Consider the linear space $L(a)$ of all polynomials in one variable of degree at most a with coefficients in $\mathbb{F}_q$. We have $\dim(L(a)) = a+1$. For $n > a$ a non-zero polynomial $f(x) \in L(a)$ cannot vanish at all points of $\mathcal{P}$. Moreover it has at least $(n-a)$ non-zero values at points of $\mathcal{P}$. The evaluation map

$$Ev : L(a) \to \mathbb{F}_q^n \ f \mapsto (f(P_1), \dots, f(P_n))$$

is then injective and its image is an $[n, a+1, n-a]_q$-code called a Reed-Solomon code *of degree a.*
As we will see all these codes are a particular case of genus 0 code.

Consider the couples $(\delta(C), R(C))$ for all linear codes C. They form a subset V_q of $[0,1]^2$. We denote U_q the set of limit points of V_q, i.e $(\delta, R) \in U_q$ iff there exists an infinite sequence of *different* (linear) codes C_i such that

$$\lim(\delta(C_i), R(C_i)) = (\delta, R).$$

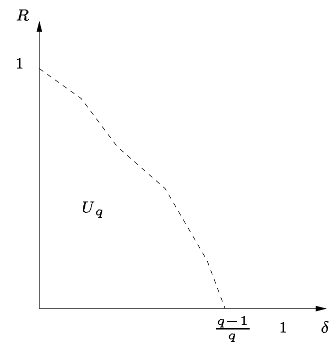
Since there is only a finite number of codes of each length, for each sequence $n(C_i) \to \infty$. If $\delta > 0$ and $R > 0$ such a sequence of codes C_i is called *asymptotically good.*

Theorem 3.4.1. *There exists a continuous function $\alpha_q(\delta)$, $\delta \in [0,1]$ such that*

$$U_q = \{(\delta, R)/0 \leq R \leq \alpha_q(\delta)\}.$$

Moreover $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $(q-1)/q \leq \delta \leq 1$, and α_q decreases on the segment $[0, (q-1)/q]$.

Figure 3.1: Function $\alpha_q(\delta)$



Remark 33. The same result exists for non-linear code.

Almost nothing is now about this function (is it convex, differentiable ?) except some upper and lower bounds which are called asymptotic bounds.

Proposition 3.4.1 (The Singleton bound). *$\alpha_q(\delta) \leq 1 - \delta$.*

Proof. Let $C \subset \mathbb{F}_q^n$ a subspace of dimension k. If d is its minimum distance it means that for all $v \in C$ at most $n-d$ components of v are 0. Suppose that $k > n-d+1$ then there exists a non zero vector in C with $n-d+1$ zero components (by solving the corresponding system). So we get a contradiction and $k \leq n-d+1$. This gives us $R \leq 1 - \delta + 1/n$ so by passing to the limit, we get $\alpha_q(\delta) \leq 1 - \delta$. □

We report also the following lower bound for comparison with the AG-bound.

Proposition 3.4.2 (Gilbert-Varshamov bound). *Let*

$$H_q(x) = x \log_q(q-1) - x \log_q x - (1-x)\log_q(1-x).$$

One has $\alpha_q(\delta) \geq 1 - H_q(\delta)$.

Remark 34. One has also the Hamming upper bound

$$\alpha_q(\delta) \leq 1 - H_q(\delta/2).$$

3.4.2 AG-codes

Algebraic-geometric codes (AG-codes) were discovered by V.D. Goppa and came as a result of many years of thinking over the possible generalization of Reed-Solomon codes. Their success comes from the improvements on the asymptotic problem they give.
Let $X/\mathbb{F}_q$ be a curve such that $X(\mathbb{F}_q) \neq \emptyset$. Let $\mathcal{P} = (P_1, \ldots, P_n) \subset X(\mathbb{F}_q)$ of order n and $D \in \mathrm{Div}(X/\mathbb{F}_q)$. We assume that $\mathrm{Supp}D \cap \mathcal{P} = \emptyset$.
Consider the map

$$Ev : L(D) \to \mathbb{F}_q^n \; f \mapsto (f(P_1), \ldots, f(P_n)).$$

We get a code $C = Ev(L(D))$. We use the notation $C = (X, \mathcal{P}, D)$.
Suppose that D is chosen in such a way that any function $f \in L(D)$ has at most b zeros at $\mathbb{F}_q$-points of X. If $n > b$ then Ev is an embedding, $k = l(D)$ and $d \geq n - b$. The Riemman-Roch theorem makes it possible to estimate the parameters of C.

Theorem 3.4.2. *Let X be a curve of genus g and let $0 \leq \deg(D) = a \leq n = |\mathcal{P}|$. Then $C = (X, \mathcal{P}, D)$ is a $[n, k, d]_q$-code with $k \geq a - g + 1$ and $d \geq n - a$.*

Proof. Let $D = D_1 - D_2$, $D_1 \geq 0, D_2 \geq 0$. A non-zero function $f \in L(D)$ has at most $a_1 = \deg(D_1)$ poles and at least $a_2 = \deg(D_2)$ zeroes in $\mathrm{Supp}D$ since $D + (f)_0 - (f)_\infty \geq 0$. Hence the number of its zeros out of the $\mathrm{Supp}D$ is at most $a_1 - a_2 = a$. We have suppose that $a < n$ so Ev is an embedding. Moreover $Ev(f)$ has at least $n - a$ non-zero coordinates, thus $d \geq n - a$. On the other hand $C \simeq L(D)$, i.e $k = l(D) \geq a - g + 1$ according to the Riemann-Roch theorem. □

Corollary 3.4.1. *Let X be a curve of genus g over $\mathbb{F}_q$ and let $N = |X(\mathbb{F}_q)| > g - 1$. Then for any $n = g + 1, \ldots, N$ and for any $k = 1, \ldots, n - g$ there exists a linear $[n, k, d]_q$-code whose parameters satisfy*

$$k + d = n - g + 1.$$

Example 9. *It is clear that the Reed-Salomon codes are examples of AG-code with $X = \mathbb{P}^1$.*
Consider the cubic $X/\mathbb{F}_2 : y^2 + y = x^3 + x$. It has 5 points over $\mathbb{F}_2$: $(0,0), (0,1), (1,0), (1,1)$ and O. We take $D = 2(O)$; then we have $L(D) = \{0, 1, x, x+1\}$ and evaluating at the remaining 4 points we obtain the following code :

$$\left(\begin{array}{c|cccc} (0,0) & 0 & 1 & 0 & 1 \\ (0,1) & 0 & 1 & 0 & 1 \\ (1,0) & 0 & 1 & 1 & 0 \\ (1,1) & 0 & 1 & 1 & 0 \end{array}\right)$$

an hardly impressing $[4, 2, 2]$-code (a good one can be constructed with the Klein's quartic and some additional tricks of coding theory).

Let us show now why the AG-codes are so important in the asymptotic theory and why we are interesting in curves with a lot of points.

Theorem 3.4.3. *If there exists a family of curves X_i over $\mathbb{F}_q$ of genus $g_i \to \infty$ such that*

$$\gamma = \liminf \frac{g_i}{N_i} < 1$$

where $N_i = |X_i(\mathbb{F}_q)|$, then

$$\alpha_q(\delta) \geq 1 - \gamma - \delta.$$

Proof. According to the last corollary, the codes constructed from X_i have parameters $[n_i, k_i, d_i]_q$, where $n_i = 1, 2, \ldots, N_i$ and $k_i = 0, 1, \ldots, n_i - g_i$ and

$$k_i + d_i = n_i - g_i + 1,$$

i.e $R_i = 1 - \frac{g_i+1}{N_i} - \delta_i$. Passing at the limit one obtains the result. □

Recall that $A(q) = \limsup \frac{N}{g}$ and so $\gamma = 1/A(q)$. So finding curves (asymptotic families) with a lot of points, gives large $A(q)$ so small γ and then good lower bound for α_q.
In fact if q is an even power of a prime then $A(q) = \sqrt{q} - 1$ (in 3.4.3 we will prove that this is the case for $q = p^2$) and so we get

Corollary 3.4.2. *If q is an even power of a prime then*

$$\alpha_q(\delta) \geq 1 - (\sqrt{q} - 1)^{-1} - \delta.$$

Remark 35. This AG-bound was a big revolution in the theory of codes because it improves for a lot of cases the classical Gilbert-Varshamov bound which was so far believed optimal.

3.4.3 Modular codes

We want to construct a family of curves of genus g_i over $\mathbb{F}_{p^2}$ with N_i rational points such that $\limsup N_i/g_i = p - 1$. We are going to do that by using the modular curves $X_0(N)$ (the general case requires Drinfeld modular curves).
Let $N \geq 3$ and let M_N be the moduli problem for the elliptic curves with a cyclic subgroup of order N. M_N is representable and is an affine curve over $\mathrm{Spec}(\mathbb{Z}[1/N])$. One can compactify it in a smooth projective scheme M_N^* over $\mathrm{Spec}(\mathbb{Z}[1/N])$ and $M_N^* \otimes \mathbb{C}$ is isomorphic to the modular curve $X_0(N)$. If p does not divide N then $X_0(N)$ has good reduction and defines a curve $\tilde{X}_0(N)$ over $\mathbb{F}_p$.
We want to give a lower bound on the number $|\tilde{X}_0(N)(\mathbb{F}_{p^2})|$.

Lemma 3.4.1. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. Then $j(E) \in \mathbb{F}_{p^2}$ i.e there exists a model of E over $\mathbb{F}_{p^2}$.*
Moreover there exists one supersingular elliptic curve over $\mathbb{F}_{p^2}$ whose Frobenius endomorphism can be identified with an integer.

Proof. As $Ker([p])(\overline{\mathbb{F}_q}) = \{O\}$ we see that $[p]$ is purely inseparable. It implies that $\hat{\mathrm{Fr}}$ is purely inseparable. It follows that we have the following factorization

$$\begin{tikzcd} E^{(p)} \arrow[rr, "\hat{\mathrm{Fr}}"] \arrow[dr, "\mathrm{Fr}"'] & & E \\ & E^{(p^2)} \arrow[ur, "\psi"'] & \end{tikzcd}$$

where ψ has degree 1 (i.e an isomorphism). So

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}$$

hence $j(E) \in \mathbb{F}_{p^2}$.
Now by Th.1.4.1 there exists an elliptic curve with Frobenius polynomial $(T-p)^2$ over $\mathbb{F}_{p^2}$. By computing the p-rank, it is clear that the curve is supersingular. □

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve whose Frobenius endomorphism acts like $[p]$. For all l prime to p, the cyclic subgroups of E of order l are then all defined over $\mathbb{F}_{p^2}$. Indeed if $P \in E[l] \setminus \{O\}$ then for $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_{p^2}}/\mathbb{F}_{p^2})$ the Frobenius automorphism we get $P^\sigma = [p]P$ so $< P > = < P^\sigma >$. Consider the modular curves $\tilde{X}_0(l)$ such that l satisfies also $l \equiv 11 \pmod{12}$. The genus of such a curve is $(l+1)/12$ and the degree over the j-line is $l+1$. Moreover by the above argument, all the points lying over the supersingular j-invariants are rational over $\mathbb{F}_{p^2}$. Since there are roughly $(p-1)/12$ supersingular j-invariants (Th.1.3.2), there are, up to a slight error due to the cusps and the j-values 0 and 1728, at least $(l+1)(p-1)/12$ rational points on $\tilde{X}_0(l)$. So the ratio

$$\frac{|\tilde{X}_0(l)(\mathbb{F}_p^2)|}{g_{\tilde{X}_0(l)}} \geq p-1.$$

As we have seen that $A(\mathbb{F}_{p^2}) \leq p-1$ we conclude that $A(\mathbb{F}_{p^2}) = p-1$.

Remark 36. In 1996, Garcia and Stichtenoth constructed an explicit tower X_l over $\mathbb{F}_{q^2}$ reaching the bound : start with X_1 the projective line with coordinates x_1 and define Artin-Schreier covers X_l by

$$y_{l+1}^q + y_{l+1} = x_l^{q+1}$$

with $x_l = y_l/x_{l-1}$. Elkies proved that this tower is in fact modular.

Remark 37. When q is not a square, much less is know : one know that there is a constant $c > 0$ such that

$$A(q) \geq c \log_2(q)$$

and one has also

$$A(q^3) \geq 2(q^2-1)/(q+2).$$

Chapter 4

Fast computations of Zeta functions

4.1 Introduction

Cryptography is playing a more and more important role in our society : smart-card, INTERNET payment, online banking.... All these applications needs to protect information. There exists two main strategies. The first one, historically, is called *symmetric key cryptography.* Roughly speaking, it is based on combinatoric tricks and only the owners of the secret key can cipher and decipher. In 1976, Diffie and Hellman introduced the new concept of *public key cryptography.* This protocol solves in particular the important problem (for INTERNET) of a creation of secret key over a non-secure channel (which was not possible with symmetric cryptography). Here is the principle :

1. Goal : Alice and Bob wants to share a secret key (to cipher and decipher after with a traditional symmetric protocol for instance).
2. let G be a group that we can assume to be isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let $g \in G$ be a generator.
3. Alice chooses $a \in \mathbb{Z}$ and sends g^a to Bob.
4. Bob chooses $b \in \mathbb{Z}$ and sends g^b to Alice.
5. Secret shared : g^{ab}.

One sees that the difficulty to break the code is based on the difficulty to compute $a = \log_g(g^a)$ (in fact to compute g^{ab} knowing g^a, g^b but these two problems are believed equivalent). This type of problem is called *discrete logarithm problem.* Does it exist groups for which this problem is difficult (whereas the computation of g^a remains easy of course) ? A problem is said difficult if one cannot solve it in a reasonable time with a good computer. More specifically that means that the number of operations would be greater than 2^{60}.

For a general group G, there is always an attack in $\sqrt{|G|}$, so $|G|$ must have at least 120 bits.
The first concrete example was given in 1978 and is known as RSA (Rivest, Shamir, Adleman). It is based on the group $\mathbb{F}_q^*$. In order to obtain a difficult problem, one has to take q with at least 1024 bits because there exist subexponential attacks.

Remark 38. The complexity of the attack –or of construction, computations– (exponential, subexponential, polynomial) is measured in term of $\log_2 |G|$.

One is of course interested in groups for which the order is small (and then the protocol fast) in other words groups with no subexponential attacks. People have tried with ideal class groups of number fields, but here again there exists a subexponential attack.
Cryptographers are now very interested in the group of rational points of a Jacobian over a finite fields, at least when the dimension g is less than 4. Indeed with this restriction no subexponential attack is known in general. We have to consider curves over $k = \mathbb{F}_{2^N}$ with $N \approx 120/g$ (because the order of the group of rational points on the Jacobian is approximately $|k|^g$).
Note however that nobody has proved that a better attack does not exist and this is of course a big fear of all banks and governments as cryptosystems based on Jacobian (at least elliptic curves) are wide used nowadays.

Remark 39. One has proved that a secure group (where no sub-exponential attack occurs) exists. But nobody is able to construct it.

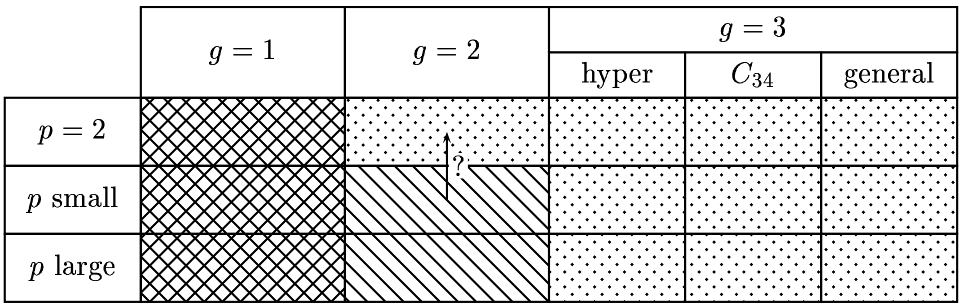
One important practical aspect is the choice of the curve : indeed we need that the order of the group of rational points of its Jacobian is almost a prime (i.e contains a large prime factor). Otherwise it is easy to break the code by working on each factor and using the Chinese Remainder Theorem. One cannot compute this number by brute force (counting points on g extensions). Indeed this method is clearly of exponential complexity and cannot be used with $\mathbb{F}_q$ of cryptographic sizes. Fortunately, two ways exist to obtain this curve :

- One takes random curves of genus g over $\mathbb{F}_q$ and one has a fast way to compute the number of points. These algorithms belongs to four categories :
    1. l-adics methods : for $g = 1$ (Schoof); works in large characteristics.
    2. Cohomological methods : the most used today is Kedlaya's algorithm. It works well when the characteristic is small.
    3. p-adic methods based on the canonical lift : they were introduced by Satoh for elliptic curves in 2000.
    4. Deformation theory : this (for the moment theoretical) method was introduced by Lauder in 2002.
- On construct a curve over a number field whose Jacobian endomorphism ring has a good structure (CM). Then one reduces the curve modulo suitable large prime for which it is easy to compute the order from the structure. These CM methods have been developed for $g = 1, 2$ (and certain $g = 3$) curves.

On can sum up the state of arts in point counting (i.e methods of the first strategy) in the following charts.

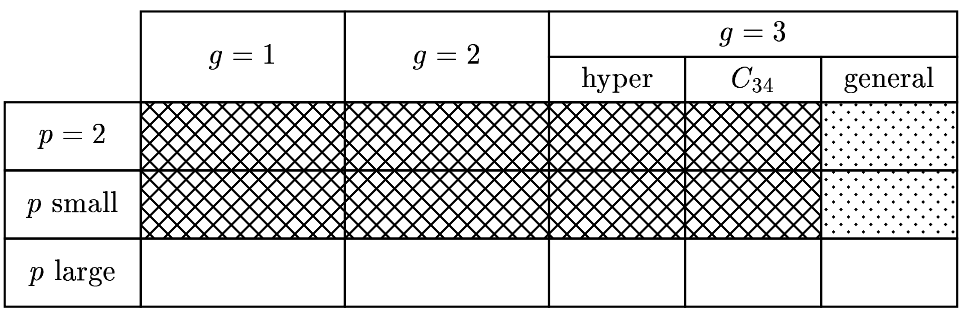
Polynomial time algorithm, possible to deal with crypto sizes
Polynomial time algorithm, impossible to reach crypto sizes
Theoretical polynomial time algorithm, not implemented

l-adic methods



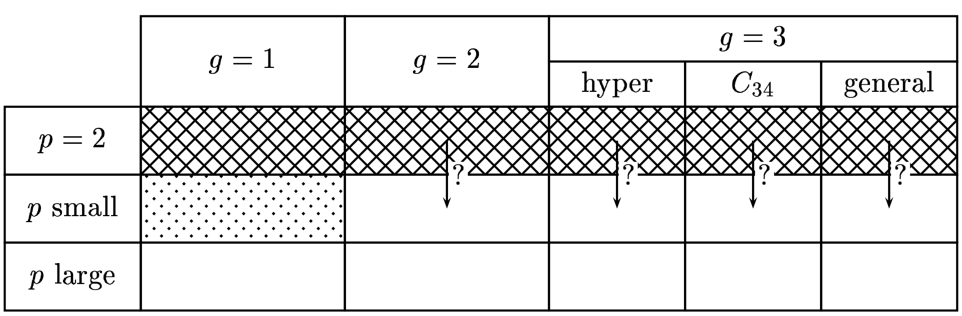
Names: Schoof, Elkies, Atkin, Couveignes, Lercier, Morain, Müller, Dewaghe, Vercauteren, Pila, Cantor, Kampkötter, Huang, Ierardi, Adleman, Harley, Gaudry.

Cohomological methods



Names: Kedlaya, Gürel, Gaudry, Vercauteren.

p-adic methods (canonical lift)



Names: Satoh, Skjernaa, Fouquet, Harley, G., Vercauteren, Mestre, Taguchi, Ritzenthaler, Carls.

Deformation

	$g = 1$	$g = 2$	$g = 3$		
			hyper	C_{34}	general
$p = 2$					
p small					
p large					

Names: Lauder.

All together

	$g = 1$	$g = 2$	$g = 3$		
			hyper	super	general
$p = 2$					
p small					
p large					

One sees that even if this domain is only 30 years old, a lot of techniques have been developed. We will focus on a 2-adic method which is a elegant variant of Satoh's algorithm : the AGM-method for genus 1 curve. This method developed in 2000 by Mestre and implemented by Lercier-Lubicz is nowadays the fastest one in characteristic 2 : a record over $\mathbb{F}_{2^{100002}}$ was obtained. Note that this method was then generalized to hyperelliptic curves [Mes02] and to non hyperelliptic curves of genus 3 [Rit03]. This method is based on formulas coming from the analytic theory and theta functions. We will begin by recalling these classical aspects.

Remark 40. In the Tutorial 6.4.4, we will implement, basically, the genus 1 AGM.

4.2 The complex theory

4.2.1 Computation of periods

It was historically the first case handled : Lagrange [Lag67, t.II,p.253-312] and Gauss [Gau70, t.III,p.352-353,261-403] introduced the *Arithmetic geometric mean* to compute elliptic integrals.

Theorem 4.2.1. *Let a, b be two reals such that $0 < b < a$. We have*

$$\int_0^{\pi/2} \frac{dt}{\sqrt{a^2\cos^2 t + b^2 \sin^2 t}} = \frac{\pi}{2\mathrm{M}(a,b)},$$

where $\mathrm{M}(a,b)$ *(*arithmetic geometric mean *of a and b) is the common limit of*

$$\begin{cases} a_0 = a & a_{n+1} = \frac{a_n+b_n}{2} \\ b_0 = b & b_{n+1} = \sqrt{a_n b_n} \end{cases}$$

Since

$$|a_{n+1} - b_{n+1}| = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} = \frac{(a_n - b_n)^2}{2(\sqrt{a_n} + \sqrt{b_n})^2} \leq \frac{(a_n - b_n)^2}{8b_1}$$

these two sequences are adjacent and the convergence is quadratic. This method is then better than traditional numeric integrations.
The proof is based on a tricky change of variables which transforms the parameters a, b in the integral into a_1, b_1. Taking the limit one has then the theorem.
To understand this change of variables we are going to algebraize our problem. Put $x = e_3 + (e_2 - e_3)\sin^2 t$ with

$$\begin{cases} a_0^2 & = e_1 - e_3 \\ b_0^2 & = e_1 - e_2 \\ 0 & = e_1 + e_2 + e_3 \end{cases}$$

We can reformulate the theorem as :

Theorem 4.2.2.

$$\int_{e_3}^{e_2} \frac{dx}{\sqrt{P(x)}} = \frac{\pi}{2\mathrm{M}(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$

with $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$, $e_3 < e_2 < e_1$.

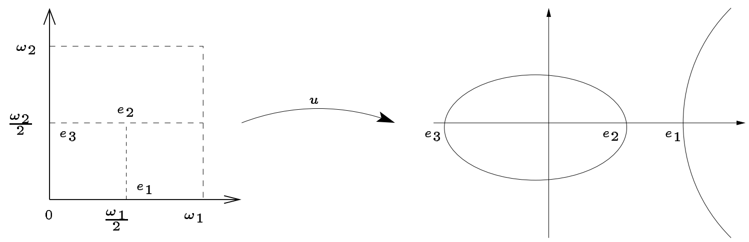
One recognizes the integral of a regular differential form on the elliptic curve $E : y^2 = P(x)$. More precisely, if one denotes by $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ (ω_1 real ω_2 purely imaginary) the complex torus $E(\mathbb{C})$, one has the isomorphism

$$\begin{array}{llll} u: & \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ & [z] & \mapsto & (x = \mathcal{P}(z) : y = \mathcal{P}'(z) : 1) & z \notin \Lambda \\ & [z] & \mapsto & (0 : 1 : 0) & z \in \Lambda \end{array}$$

and (see figure 4.1)

$$\omega_1 = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2\int_{\omega_2/2}^{(\omega_1+\omega_2)/2} \frac{d\mathcal{P}(z)}{\mathcal{P}'(z)} = 2\int_{e_3}^{e_2} \frac{dx}{y} = 2\int_{e_3}^{e_2} \frac{dt}{\sqrt{P(t)}}$$

Figure 4.1: The map u



The problem is now the computation of a period of a differential of the 1st kind on a Riemann surface.
Let $\tau = \omega_2/\omega_1$. In the theory of abelian varieties over $\mathbb{C}$, it is classical to introduce *theta functions*. They can be seen as holomorphic sections of sheaves but we want to give here a more straightforward definition for elliptic curves (see [Ros86] for the general theory).

Definition 4.2.1. *Let* $\tau \in \mathbb{H}$, $\epsilon, \epsilon' \in \{0,1\}$. *One defines the* theta function with characteristic (ϵ, ϵ') *by*

$$\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](z,\tau) = \sum_{n\in\mathbb{Z}} \exp(i\pi(n+\epsilon/2)^2\tau + 2i\pi(n+\epsilon/2)(z+\epsilon'/2))$$

It is an analytic function of the variable z. If $z = 0$, one denotes also $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](0,\tau) = \vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$. When $(\epsilon,\epsilon') \neq (1,1)$, $\vartheta \left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau) \neq 0$ and is called a *theta constant.*
These values have the following properties.

Proposition 4.2.1. *1. Limit :*

$$\lim_{\mathrm{Im}\,\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau) = \lim_{\mathrm{Im}\,\tau\to+\infty} \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau) = 1.$$

2. Thomae's formula :

$$\begin{cases} \omega_1\sqrt{e_1 - e_3} = & \pi\cdot\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \\ \omega_1\sqrt{e_1 - e_2} = & \pi\cdot\vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2 \end{cases}$$

3. Duplication formula :

$$\begin{cases} \vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](2\tau)^2 = & \frac{\vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 + \vartheta\left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2}{2} \\ \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](2\tau)^2 = & \sqrt{\vartheta \left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](\tau)^2 \vartheta \left[\begin{smallmatrix}0\\ 1\end{smallmatrix}\right](\tau)^2} \end{cases}$$

Remark 41. As the theta constants are positive reals (because τ is purely imaginary), the sign of the square roots is always the positive one. When it is no more the case, the choice is a bit more subtle as we will see in 4.2.3.

4.2.2 Proofs

We want to give two proofs of Th.4.2.2. The first one is straightforward. As the duplication formula is exactly the AGM recursion, we can write

$$\begin{cases} a_0 = \vartheta \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\tau)^2 & a_n = \vartheta \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](2^n\tau)^2 \\ b_0 = \vartheta \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](\tau)^2 & b_n = \vartheta \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](2^n\tau)^2 \end{cases}$$

By the limit property, one has

$$\mathrm{M}\left(\vartheta \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\tau)^2, \vartheta \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](\tau)^2\right) = 1.$$

The AGM recursion being homogeneous, one obtains the theorem thanks to Thomae formula :

$$M(a_0, b_0) = M(\frac{\omega_1\sqrt{e_1 - e_3}}{\pi}, \frac{\omega_1\sqrt{e_1 - e_2}}{\pi}) = \frac{\omega_1}{\pi} M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2}) = 1.$$

The second proof will reveal the true geometry behind the result. Consider again the elliptic curve $E : y^2 = P(x)$. This curve is isomorphic to the curve $E_\tau = E_{a_0,b_0}$ defined by

$$\begin{aligned} E_\tau : y_0^2 &= x_0(x_0 - (e_1 - e_3))(x_0 - (e_1 - e_2)) && (4.1)\\ &= x_0\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot\vartheta \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\tau)^4\right)\left(x_0 - \frac{\pi^2}{\omega_1^2}\cdot\vartheta \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right](\tau)^4\right) && (4.2)\\ &= x_0(x_0 - a_0^2)(x_0 - b_0^2), && (4.3) \end{aligned}$$

One can then construct the following diagram.

$$\begin{tikzcd} \mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \arrow[r, "G:z\mapsto z"] \arrow[d, "u_{2\tau}"', "\simeq"] & \mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \arrow[d, "\simeq"', "u_\tau"] \\ E_{2\tau}(\mathbb{C}) \arrow[r, shift left, "g"] & E_\tau(\mathbb{C}) \arrow[l, shift left, "f"] \end{tikzcd}$$

where $E_{2\tau} = E_{a_1,b_1}$ and f, g are 2-isogenies given by (see for instance [BM89]):

$$\begin{aligned} g : (x_1, y_1) &\mapsto \left(x_1(1 + \frac{a_1^2 - b_1^2}{x_1 - a_1^2}), \frac{y_1(x_1^2 - 2x_1a_1^2 + a_1^2b_1^2)}{(x_1 - a_1^2)^2}\right) && (4.4)\\ f : (x_0, y_0) &\mapsto \left(\frac{y_0^2}{4x_0^2} + (\frac{a+b}{2})^2, -\frac{y_0(a^2b^2 - x_0^2)}{8x_0^2}\right) && (4.5) \end{aligned}$$

In particular the kernel of f is $< (0,0) >$.
We can now finish the proof : since $G^*(dz) = dz$ we have $g^*(dx_0/y_0) = dx_1/y_1$. Now

$$\omega_1 = 2\int_{e_1}^{\infty}\frac{dx}{y} = 2\int_0^{-\infty}\frac{-i}{2}\frac{dx_0}{y_0} = \int_0^{-\infty} -i\frac{dx_1}{y_1} = \ldots = \int_0^{-\infty} -i\frac{dx_n}{y_n}.$$

By iteration :

$$E_\tau \to E_{2\tau} \to \ldots \to E_{2^n\tau} \to \ldots \to E_\infty : y^2 = x(x - M(a_0, b_0)^2)^2.$$

But E_∞ is a genus 0 curve which means that there exists a parametrization which gives

$$\omega_1 = \int_0^{-\infty} -i\frac{dx}{\sqrt{x(x - M(a_0,b_0)^2)^2}} = \left[-2\frac{\mathrm{Arctan}(\frac{\sqrt{\mathrm{x}}}{\mathrm{M(a_0,b_0)}})}{\mathrm{M(a_0,b_0)}} \right]_0^{-\infty} = \frac{\pi}{\mathrm{M}(a_0,b_0)}.$$

4.2.3 With complex values

One can wonder what happens when τ is not purely imaginary. The problem was already handled by Gauss (see [Cox84]).
Let $a, b \in \mathbb{C}$ such that $b/a \notin \{0, \pm 1\}$ with $|a| \geq |b|$.

Definition 4.2.2. $b_1 = \pm\sqrt{ab}$ *is called a* good root *if* $|a_1 - b_1| \leq |a_1 + b_1|$ *and if* $|a_1 - b_1| = |a_1 + b_1|$ *one has also* $\Im(b_1/a_1) > 0$.
The AGM sequence (a_n, b_n) *is called good if* b_{n+1} *is a good choice of* $\sqrt{a_n b_n}$ *for all but a finite number of* n.

Proposition 4.2.2. (a_n, b_n) *converges to a common non zero limit iff* (a_n, b_n) *is good.*

One defines then :

Definition 4.2.3. *A number* μ *is called* an arithmetic-geometric mean *of* (a, b) *if there exists a good sequence converging to* μ*. We denotes by* $\{M(a, b)\}$ *the set of these values. The value obtained by doing always a good choice is called* simple value *and denoted* $M(a, b)$.

We have the fundamental result.

Theorem 4.2.3 (Gauss). *Let* $\mu = M(a, b)$ *and* $\lambda = \mathrm{M}(a + b, a - b)$ *then every value* $\mu' \in \{\mathrm{M}(a, b)\}$ *is given by*

$$\frac{1}{\mu'} = \frac{d}{\mu} + \frac{ic}{\lambda}$$

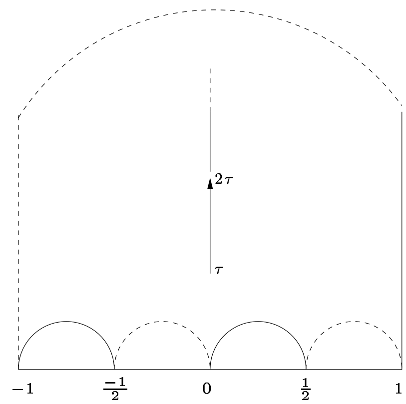
with c, d *coprime such that* $d \equiv 1 \pmod 4$ *and* $c \equiv 0 \pmod 4$.

The proof of this theorem introduces naturally the moduli space $\mathbb{H}/\Gamma^2(4)$

$$\Gamma^2(4) = \{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} | a \equiv d \equiv 1 \pmod 4, c \equiv 0 \pmod 4, b \equiv 0 \pmod 2\}.$$

This moduli space parametrizes elliptic curves with a 2 and a 4 torsion points up to isomorphism. The AGM method may be interpreted as a path to the border of this moduli space (which consists of degenerated curves).

Figure 4.2: Fundamental domain for $\Gamma^2(4)$



Remark 42. One can show that π/μ and $i\pi/\lambda$ are two periods of the curve $E : y^2 = x(x-a^2)(x-b^2)$.
Recently R. Dupont has used the AGM algorithm in the opposite direction : knowing τ he was able to give a quadratic algorithm to compute the theta constants. A generalization to the genus 2 case is a work in progress.

4.3 2-adic method

Let $q = 2^N, k = \mathbb{F}_q$ and $\mathbb{Q}_q$ be the unramified extension of degree N of $\mathbb{Q}_2$, $\mathbb{Z}_q$ its ring of integers, ν its valuation and σ the Frobenius substitution (i.e the unique Galois automorphism of $\mathbb{Q}_q$ such that $\sigma x \equiv x^2 \pmod 2$). The aim of this section is to give an algorithm which we can present as

$$\tilde{E}/\mathbb{F}_q \text{ ordinary e.c.} \overset{\text{lift}}{\longrightarrow} E/\mathbb{Z}_q \underset{\text{cv}}{\overset{\text{AGM}}{\longrightarrow}} \mathcal{E}/\mathbb{Z}_q \text{ canonical lift} \overset{\text{AGM}}{\longrightarrow} \text{Frobenius trace.}$$

Let us detail now the different parts.

4.3.1 Lift

In characteristic 0 we want to use the form $E_{a,b} : y^2 = x(x-a^2)(x-b^2)$. Of course we cannot use this model in characteristic 2. We propose two different solutions to solve this problem.

First solution

Lemma 4.3.1 ([Ver03]). *Let $a, b \in 1 + 4\mathbb{Z}_q$ with $b/a \in 1 + 8\mathbb{Z}_q$. Then*

$$\begin{array}{rcl} E_{a,b} & \tilde{\to} & E : y^2 + xy = x^3 + rx^2 + sx + t \\ (x,y) & \to & \left(\dfrac{x-ab}{4}, \dfrac{y-x+ab}{8}\right) \end{array}$$

for some $r, s, t \in \mathbb{Z}_q$ such that

$$\tilde{E} : y^2 + xy = x^3 + \left(\frac{a-b}{8}\right).$$

We then consider $\tilde{E}$ as $y^2 + xy = x^3 + c$, let $r \in \mathbb{Z}_q$ such that $r \equiv \sqrt{c} \pmod 2$ and take

$$\begin{cases} a_0 = 1 + 4r \\ b_0 = 1 - 4r \end{cases}$$

The advantage of this model is that there is a rational 4 torsion point $(c^{1/4}, c^{1/2})$. This point enables to find the sign of $\pm\mathrm{tr}(\pi)$ that occurs at the end of the algorithm because $\mathrm{tr}(\pi) \simeq 1 \pmod 4$. The drawback is that this model does not represent all cases. Moreover it gives no clue on a possible generalization to higher hyperelliptic cases.

Second solution

Starting with a general ordinary elliptic curve $\tilde{E} : y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$, we can always get rid of the a_6 coefficient. We lift then $\tilde{E}$ naturally and make the transformation

$$Y^2 = (y + \frac{x}{2})^2 = x(x^2 + \frac{4a_2 + 1}{4}x + 1).$$

We can factorize the left member over $\mathbb{Q}_q$ in $x(x-\alpha)(x-\beta)$ with $\nu(\alpha) = -2$ and $\nu(\beta) = 2$. Let $X = x - \alpha$ we have then a model

$$Y^2 = X(X + \alpha)(X + \alpha - \beta).$$

As $\nu(\frac{\alpha-\beta}{\alpha} - 1) = \nu(\frac{\alpha}{\beta}) = 4$, we can take

$$\begin{cases} a_0 = 1 \\ b_0 = \sqrt{\frac{\alpha-\beta}{\alpha}} \in \mathbb{Z}_q \end{cases}$$

and consider the curve

$$Y^2 = X(X-1)(X-b_0^2).$$

Note that this curve is not isomorphic over $\mathbb{Q}_q$ to the original one but is a quadratic twist. However, as we will obtain the trace of the Frobenius only up to a sign, this is not an issue.

Remark 43. We have to get rid of the a_6 coefficient, otherwise we might have to factorize the left member in a ramified extension of $\mathbb{Q}_2$ (it is the case for instance with $y^2 + xy = x^3 + 1$).

4.3.2 Convergence

Let start with a model $E_0 = E_{a_0,b_0}$ over $\mathbb{Z}_q$ lifting $\tilde{E}$. Let denote $E_i = E_{a_i,b_i}$ the elliptic curves obtained by AGM iterations. Let denote also $\tilde{E}^{\uparrow}$ the canonical lift of $\tilde{E}$ which is completely characterized by its j-invariant J. We want to prove that the AGM sequence converges to the Galois cycle associated to the canonical lift. We give two proofs.

First proof

We are going to use the following theorem.

Theorem 4.3.1 ([VPV01, §. 2]). *Let $x \in \mathbb{Z}_q$ such that $x \equiv J \pmod{2^i}$ with $i \in \mathbb{N}$. Then there exists a unique $y \in \mathbb{Z}_q$ such that $y \equiv x^2 \pmod 2$ and $\Phi_2(x, y) = 0$. Moreover $y \equiv j((\tilde{E}^{(2)})^{\uparrow}) = J^{\sigma} \pmod{2^{i+1}}$.*

Recall that Φ_p is the modular polynomial of order p. If E and E' are two elliptic curves that are p-isogenous then $\Phi_p(j(E), j(E')) = 0$.
We have of course $\Phi_2(E_i, E_{i+1}) = 0$ by the complex computations of 4.2. An easy computation shows also the following congruence.

Lemma 4.3.2. $j(E_{i+1}) \equiv j(E_i)^2 \pmod 2$.

By iteration of the AGM we then obtain

$$j(E_n) \equiv j((\tilde{E}^{(2^n)})^{\uparrow}) \pmod{2^{n+1}}.$$

Second proof

The second proof uses a result of Carls. It avoids explicit invariants and is then useful for generalization.

Theorem 4.3.2 ([Car02, Th.3]). *Let A be an abelian variety over $\mathbb{F}_q$, $\mathcal{A}/\mathbb{Z}_q$ be an abelian scheme with special fiber A. One defines a sequence*

$$\mathcal{A} = \mathcal{A}_0 \to \mathcal{A}_1 \to \dots$$

where the kernel of the isogenies are the components $\mathcal{A}_i[2]^{loc}$ (i.e the 2-torsion points in the kernel of the reduction). We have

$$\lim_{n\to\infty} \mathcal{A}_{nN} = A^{\uparrow}$$

i.e for all n, $(\mathcal{A}_{Nn})/\mathbb{Z}_q^{(Nn+1)} = (A^{\uparrow}_{Nn})/\mathbb{Z}_q^{(Nn+1)}$ where $\mathbb{Z}_q^{(i)} = \mathbb{Z}_q/2^i\mathbb{Z}_q \simeq \mathbb{Z}/2^i\mathbb{Z}$. In particular the convergence is linear.

Using 4.2 we see that if we still denote by $f : E_i \to E_{i+1}$ the 2-isogeny induced by the AGM-iteration, then $\ker f =< (0,0) >$ and $(0,0)$ reduces on $\tilde{O}$ (because the kernel corresponds to the point $(\alpha, 0)$ in the reduction, which is of negative valuation). We can then apply the previous theorem.

4.3.3 Trace of the Frobenius

To compute the Frobenius polynomial we only need the trace of the Frobenius on $V_l(\tilde{E})$ for $l \neq p$. But this trace can be already read on regular differentials. We have the classical proposition.

Proposition 4.3.1 (Satoh). *Let E be an elliptic curve over $\mathbb{Q}_q$ having good reduction modulo p and let $f \in End_{\mathbb{Q}_q}(E)$ of degree d. Let ω be a regular differential on E and let $f^*(\omega) = c\omega$ be the action of f on ω then $tr(f) = c + \frac{d}{c}$.*

In particular if f lifts the Frobenius endomorphism, we have $\chi(X) = X^2 - cX + q$.
We need also the following elementary lemma.

Lemma 4.3.3. *Let $E_{a,b} : y^2 = x(x - a^2)(x - b^2)$ et $E_{a',b'} : y'^2 = x'(x' - a'^2)(x' - b'^2)$ with $\frac{a^2}{b^2} \equiv \frac{a'^2}{b'^2} \equiv 1 \pmod 2$. If E and E' are isomorphic then $x = u^2x'$ and $y = u^3y'$ with $u^2 = \frac{a^2+b^2}{a'^2+b'^2}$. Furthermore $\frac{a^2}{b^2} = \frac{a'^2}{b'^2}$ or $\frac{a^2}{b^2} = \frac{b'^2}{a'^2}$.*

Proof. The two curves being isomorphic, there exists $(u, r) \in (\mathbb{Z}_q^* \times Q_q)$ such that $x = u^2x' + r$ and $y = u^3y'$. It is enough to show that $r = 0$. With the usual notations of [Sil92, chap.III,1.2], one has

$$\begin{aligned} -4u^2(a'^2 + b'^2) = b_2' &= b_2 + 12r = -4(a^2 + b^2) + 12r \\ 0 = u^6b_6' &= 4r(r - a^2)(r - b^2) \end{aligned}$$

The first equality shows that $r \equiv 0 \pmod 2$ and the second that $r = 0$ since neither a^2 or b^2 are congruent to 0. The first equality gives also the value of u^2. $\square$

Let $\mathcal{E}_{a_0,b_0}$ be the canonical lift. We can then construct the following diagram

$$\begin{tikzcd}
\mathcal{E}_{a_0^\sigma,b_0^\sigma} \arrow[d, "\phi"'] \arrow[dr, bend left, "\mathrm{Ve}^\uparrow"] & \\
\mathcal{E}_{a_1,b_1} \arrow[r, shift left, "g"] \arrow[d] & \mathcal{E}_{a_0,b_0} \arrow[l, shift left, "f"] \arrow[ul, "\mathrm{Fr}^\uparrow"] \arrow[d] \\
\tilde{E}^{(2)} & \tilde{E} \arrow[l, "\mathrm{Fr}"]
\end{tikzcd}$$

where ϕ is an isomorphism because the two maps have the same kernel $< (0,0) >$. Let $\omega = dx/y$, we then get

$$(\mathrm{Ve}^\uparrow)^*(\omega) = (g \circ \phi)^*(\omega) = \phi^*(\omega) = \frac{\omega}{u^\sigma}$$

with $u^2 = \frac{a_1^2+b_1^2}{(a_0^2)^\sigma+(b_0^2)^\sigma}$ because g acts by identity as we can see on the explicit formula or with the complex interpretation of g as $z \mapsto z$.
We want to simplify a bit the expression of u^2. we have

$$u^2 = \left(\frac{a_1}{a_0^\sigma}\right)^2 \frac{1 + \left(\frac{b_1}{a_1}\right)^2}{1 + \left(\frac{b_0^\sigma}{a_0^\sigma}\right)^2}.$$

Let $\lambda_1 = b_1/a_1$ and $\lambda_0 = b_0/a_0$. By Lem.4.3.3 $\lambda_1^2 = (\lambda_0^2)^\sigma$ or $\lambda_1^2 = \frac{1}{(\lambda_0^2)^\sigma}$. Let us prove that it is the first case which occurs. We can write $\lambda_i = 1 + 8c_i$ with $c_i \in \mathbb{Z}_q$ so the first case occurs iff

$$c_1 \equiv c_0^\sigma \pmod 4.$$

By the AGM iteration, we have

$$1 + 8c_1 = \frac{1 + 4c_0}{\sqrt{1 + 8c_0}} \Rightarrow c_1 \equiv c_0^2 \pmod 4.$$

As after the first iteration c_0 is itself a square α_0^2 modulo 4, we have

$$c_0^\sigma \equiv (\alpha_0^2)^\sigma \equiv \alpha_0^4 \equiv c_0^2 \pmod 4.$$

So we get $c_1 \equiv c_0^\sigma \pmod 4$ which proves

$$u = \pm \frac{a_1}{a_0^\sigma}.$$

The trace of the Frobenius endomorphism is the same as the trace of the Verschiebung. One has

$$\mathrm{tr}(\pi) = \mathrm{tr}(V) = \mathrm{tr}(\mathrm{Ve}^{\sigma^{N-1}} \circ \cdots \circ \mathrm{Ve}) = \pm \left(\frac{1}{N(u)} + 2^N N(u) \right)$$

with $N(u) = \mathrm{Norm}_{\mathbb{Q}_q/\mathbb{Q}_2}(a_1/a_0)$.

4.3.4 Complexity and Conclusion

Since by the Hasse-Weil theorem $\mathrm{tr}(\pi) \leq 2\sqrt{q}$ it is enough to compute the previous norm with $\lceil N/2 \rceil + 2$ bits. Several implementations of this method have been achieved : see [Ver03] for a nice overview and running times. The best complexity obtained is quasi-quadratic in time and quadratic in space.

One of the attractive aspect of the AGM method is the simplicity of the formulas involved. Another one is the natural generalizations one can obtain for hyperelliptic curves and non hyperelliptic curves of genus 3. On the contrary it seems that generalization to other characteristics would be less efficient and less elegant due to the complexity of the new AGM formulas.

Chapter 5

Appendix

5.1 Appendix A : abelian varieties

5.1.1 Definitions

Definition 5.1.1. *A* group variety *over a field K is a variety V over K together with morphisms*

$$m : V \times V \to V \quad \textit{(multiplication)}, inv : V \to V \quad \textit{(inverse)},$$

and a element $\epsilon \in V(K)$ such that the structure on $V(\overline{K})$ defined by m, inv is that of a group with identity ϵ.

A group variety is automatically nonsingular.

Definition 5.1.2. *A complete (i.e proper over K) group variety is called an* abelian variety*.*

Fortunately we get for free that abelian varieties are projective and the group law is commutative.
About morphisms now. Let A, B two abelian varieties. Every morphism $f : A \to B$ is the composite of a homomorphism with a translation. Among them the following ones are more important.

Definition 5.1.3. *Let $f : A \to B$ a homomorphism such that one of the following equivalent properties holds :*

1. $\dim A = \dim B$ *and f is surjective;*
2. $\dim A = \dim B$ *and* $\ker(f)$ *is a finite group scheme;*
3. *f is finite, flat and surjective.*

f is called an isogeny*.*

The *degree* of an isogeny $f : A \to B$ is defined to be the order of the kernel of f (as a finite group scheme). We have $\deg(f \circ g) = \deg(f)\deg(g)$. Let $n = \deg(f)$; then $\ker(f) \subset \ker([n])$ and so $[n]$ factors as $[n] = g \circ f$ with an isogeny g.

Theorem 5.1.1. *Let A be an abelian variety of dimension g and let $n > 0$ be an integer. Then $[n] : A \to A$ is an isogeny of degree n^{2g}; it is étale (i.e séparable) iff the characteristic of K does not divide n.*

Remark 44. If K is separably algebraically closed and n is not divisible by its characteristic, then the theorem says that the kernel of $[n] : A(K) \to A(K)$ has n^{2g} elements. It is then a free $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$. We may then construct (like for elliptic curves)

$$T_l(A) := \lim_{\leftarrow} A[l^n].$$

5.1.2 Dual abelian variety and polarization

Proposition 5.1.1. *Let A be an abelian variety over K. There exists an abelian variety $\hat{A}$ over K such that*

1. *$\hat{A}(K') = Pic^0(A_{K'})$ for all extension K' of K.*
2. *$\hat{\hat{A}} = A$.*
3. *if $f : A \to B$ is an isogeny with kernel N, then there exists an isogeny of the same degree $\hat{f} : \hat{B} \to \hat{A}$ with kernel $\hat{N}$, the Cartier dual of N.*

The statement about the kernels requires explanation. If the degree of f is prime to the characteristic, then N is an algebraic group of dimension zero over k, and the dual is taken in the following sense : if K is separably closed, N can be identified with the abstract group $N(k)$, which is finite and commutative; then

$$\hat{N} = Hom(N, \mu_n(K)),$$

where n is any integer killing N. If K is not separably closed, then $N(K^{sep})$ has an action of $Gal(K^{sep}, K)$ and $\hat{N}(K^{sep})$ has the induced action.

Let $\mathcal{L}$ be an invertible sheaf on A. Then we can define the map $\phi_{\mathcal{L}} : A(K) \to \mathrm{Pic}^0(A)$ which sends $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ where t_a is the translation by a.

Definition 5.1.4. *A* polarization *λ on A is an isogeny $\lambda : A \to \hat{A}$ such that $\lambda_{\overline{K}} = \phi_{\mathcal{L}}$ for some ample invertible sheaf $\mathcal{L}$ on $A_{\overline{K}}$. The degree of a polarization is its degree as an isogeny. An abelian variety together with a polarization is called a* polarized abelian variety. *If λ is an isomorphism then λ is said to be a* principal polarization.

Recall that $\mathcal{L}$ is ample iff there exists a positive integer n such that the map $A \to \mathbb{P}^N$ associated to $\mathcal{L}^n$ is an embedding (one can take $n = 3$).

Remark 45. If λ is a polarization, there need not exist an $\mathcal{L}$ on A. However it is the case if K is finite.

Theorem 5.1.2. *Any abelian variety has a polarization.*

Remark 46. Consider $A/\mathbb{C}$. One can show that $A(\mathbb{C})$ is a complex torus $\mathbb{C}^g/\Lambda$. Reciprocally it is not true that every torus $T = \mathbb{C}^g/\Lambda$, $g \geq 2$ is an abelian variety. Actually T is an abelian variety iff T has a ample sheaf (i.e T has a polarization, i.e T has a projective embedding).

5.1.3 Pairings

If M and N denote the kernels of an isogeny f and its dual $\hat{f}$, then there is a canonical pairing $M \times N \to \mu_m$ which identifies each group scheme with the Cartier dual of the other. In the case that f is the multiplication by m and if m is prime to the characteristic we then obtain a non-degenerate pairing of $\mathrm{Gal}(\overline{K}/K)$-modules

$$\overline{e}_m : A[m] \times \hat{A}[m] \to \overline{K}^*.$$

Remark 47. One can give the same explicit description of this pairing as for elliptic curves (see 1.2.1).

We have also a compatibility relation.

Lemma 5.1.1. *Let m and n be integers prime to the characteristic. Then for all $S \in A[mn]$ and all $T \in \hat{A}[mn]$,*

$$\overline{e}_{mn}(S,T)^n = \overline{e}_m(nS, nT).$$

Thanks to this lemma, we can operate on limits and define a pairing $e_l : T_l(A) \times T_l(\hat{A}) \to T_l(\mu)$.

Proposition 5.1.2. *If $\phi : A \to B$ is a homomorphism then ϕ and $\hat{\phi}$ are adjoints for the pairing.*

Now for $\lambda : A \to \hat{A}$ a polarization we can define

$$e_l^\lambda : T_l(A) \times T_l(A) \to T_l(\mu).$$

This pairing has the same good properties as the Weil pairing for elliptic curves.

Proposition 5.1.3. *The pairing e_l^λ is bilinear, alternating, non-degenerate, Galois invariant.*

5.1.4 Rosati involution

Fix a polarization λ on A. As λ is an isogeny, it has an inverse in $\mathrm{Hom}^0(A, \hat{A})$.

Definition 5.1.5. *The* Rosati involution *on $End^0(A)$ corresponding to λ is*

$$\alpha \mapsto \alpha^\dagger = \lambda^{-1} \circ \hat{\alpha} \circ \lambda.$$

This has the following properties :

$$(\alpha + \beta)^\dagger = \alpha^\dagger + \beta^\dagger,\ (\alpha\beta)^\dagger = \beta^\dagger\alpha^\dagger,\ [a]^\dagger = [a].$$

For any $S, T \in V_l(A)$,

$$e_l^\lambda(\alpha S, T) = e_l(\alpha S, \lambda T) = e_l(S, \hat{\alpha} \circ \lambda T) = e_l^\lambda(S, \alpha^\dagger T).$$

From which it follows that $\alpha^{\dagger\dagger} = \alpha$.

Theorem 5.1.3. *The bilinear form*

$$(\alpha, \beta) \mapsto tr(\alpha \circ \beta^\dagger) : End^0(A) \times End^0(A) \to \mathbb{Q}$$

is positive definite.

5.1.5 Jacobian

A complete book can be devoted (and several have been devoted) to the interactions between a curve and its Jacobian. We will give here a tiny insight of the subject.
Let C/K be a curve of genus $g \geq 1$. If $C(K)$ is not empty, then a choice of a point P^0 in $C(K)$ defines an injection $C(\overline{K}) \hookrightarrow \mathrm{Pic}^0(C_{\overline{K}})$ sending P to the class $(P - P_0)$ (up to linear equivalence). This map is a bijection when $g = 1$, thus allowing us in this case to identify the group $\mathrm{Pic}^0(C_{\overline{K}})$ with the points of an abelian variety.
More generally one can associate to any curve C/K an abelian variety J/K of dimension g called the *Jacobian variety* of C and denoted $\mathrm{Jac}(C)$. However if we want good functorial properties we have to suppose that $C(K) \neq \emptyset$. Then

- if $K \subset K' \subset \overline{K}$, then the set of K'-rational points $J(K')$ is in bijection with $\mathrm{Pic}^0(C/K') := \mathrm{Pic}^0(C_{\overline{K}})^{\mathrm{Gal}(\overline{K}/K')}$.
- Given $P_0 \in C(K)$, there exists a functorial morphism of algebraic varieties $C \to J$, defined over K, that sends P_0 to the 0 of J. This mapping induces on the sets of $\overline{K}$-rational points the map $P \mapsto (P - P_0)$. This mapping is called a *Jacobi map.*
- Universal property : let A/K be an abelian variety then every rational map from C to A factors through J.

Moreover J has a canonical principal polarization which depends only of C. We denote Θ the ample sheaf associated to it.

Remark 48. Analytically, the construction of the Jacobian variety is not very difficult. If C is a curve over $\mathbb{C}$ of genus g, recall that (from topology) C is a g-holed torus and that $H_1(C, \mathbb{Z})$ has a canonical basis $\gamma_1, \ldots, \gamma_{2g}$, roughly speaking each loop γ_i goes once round one hole. If $\omega_1, \ldots, \omega_g$ is a basis of regular differentials, one can then consider the vectors

$$\pi_j = \begin{pmatrix} \int_{\gamma_j} \omega_1 \\ \vdots \\ \int_{\gamma_j} \omega_g \end{pmatrix} \in \mathbb{C}^g$$

called *period vectors*. On can prove that these $2g$ vectors are linearly independent over $\mathbb{R}$ so $\mathbb{C}^g / \sum \mathbb{Z}\pi_i$ is a torus (in a fancy way we can write it as $H_1(C, \Omega^1)^* / H_1(C, \mathbb{Z})$). One can then prove that it is an abelian variety because it has a Riemann form coming from the intersection product (see for example [Ros86]).
One has also an application

$$\mathrm{Div}^0(C) \to \mathrm{Jac}(C) \ , \sum n_i P_i \mapsto (\omega \mapsto \sum n_i \int_P^{P_i} \omega).$$

This map is surjective (Jacobi inversion formula) and its kernel is precisely the group of principal divisor (Abel theorem). We get an isomorphism between $Pic^0(C)$ and $\mathrm{Jac}(C)$.

5.2 Appendix B

5.2.1 Frobenius morphisms and Verschiebung

We define first the *absolute Frobenius morphism* $F : X \to X$ as follow : F is the identity map on the topological space of X and $F^*\mathcal{O} \to \mathcal{O}$ is the pth power map.

Remark 49. F is not a linear map. We have a commutative diagram

$$\begin{tikzcd} X \arrow[r, "F"] \arrow[d] & X \arrow[d] \\ \mathrm{Spec}(k) \arrow[r, "F"] & \mathrm{Spec}(k) \end{tikzcd}$$

where $F : \mathrm{Spec}(k) \to \mathrm{Spec}(k)$ corresponds to the pth power of k.

We define now a new scheme $X^{(p)} = X \otimes_F \mathrm{Spec}(k)$. By definition of the fiber product we can then construct the following diagram

$$\begin{tikzcd} X \arrow[dr, "\mathrm{Fr}"] \arrow[drr, bend left, "F"] \arrow[ddr, bend right] & & \\ & X^{(p)} \arrow[r] \arrow[d] & X \arrow[d] \\ & \mathrm{Spec}(k) \arrow[r, "F"] & \mathrm{Spec}(k) \end{tikzcd}$$

We call Fr the *(relative) Frobenius* morphism.
In the case where X is an affine scheme defined by Spec(M) with $M = k[x_1, \dots, x_n]/(f_i)$ then $X^{(p)}$ is defined by Spec$(M \otimes_F k \simeq k[x_1, \dots, x_n]/(f_i^{(p)})$ where if $f_i = \sum a_I x^I$ then $f_i^{(p)} = \sum a_I^p x^I$. Thus we find the classical definition.
Note that if X/k is a curve then $X^{(p)}$ is the curve with function field $k(X)^p = \{f^p, f \in k(X)\}$.

Proposition 5.2.1. *Let X/k be a variety of dimension n. Then $Fr : X \to X^{(p)}$ is a purely inseparable morphism of degree p^n.*

We can reiterate the process. By abuse of notation one still calls Fr the morphism and $\mathrm{Fr}^n : X \to X^{(p^n)}$.
From now on, let $k = \mathbb{F}_q$, with $q = p^n$ and X/k. One has then that $X^{(q)} = X$. One calls then $\pi = \mathrm{Fr}^n : X \mapsto X$ the *Frobenius endomorphism* of X/k.

Proposition 5.2.2. *Let $\pi : \overline{k} \mapsto \overline{k}, x \mapsto x^q$ the Frobenius automorphism of $\overline{k}/k$. The Galois action induces by the Frobenius automorphism on $X(\overline{k})$ equals the action of the Frobenius endomorphism of X/k.*

When $X = A$ is an abelian variety defined over k, the relative Frobenius $\mathrm{Fr} : A \to A^{(p)}$ is an isogeny. As $\deg(\mathrm{Fr}) = p$, one can write $[p] = \mathrm{Fr} \circ \mathrm{Ve}$ where Ve is an isogeny called the *(relative) Verschiebung* morphism (We can also define the Verschiebung endomorphism denoted V).

Example 10. *If E/k is an elliptic curve then one sees that*

$$\begin{cases} \deg_s([p]) = p \ (resp.\ 1) \\ \deg_i([p]) = p \ (resp.\ p^2) \end{cases}$$

when E is ordinary (resp. supersingular). Then Ve is separable (resp. purely inseparable).
More generally one can prove see that A is ordinary iff Ve is separable.

5.2.2 Descent theory

This is copied from [Ser75, V.4].
Let K_1 be an extension of a field K and let V be an algebraic variety defined over K_1. 'To descend the base field of V from K_1 to K' means to find a variety W/K which is isomorphic to V over K_1. Let us denote $f : W \mapsto V$ an isomorphism.
We suppose from now on that K_1 is a finite Galois extension of K with Galois group G. If $\sigma \in G$ one can apply it to V, W and f. We obtain the diagram

$$\begin{tikzcd} V \arrow[rr, "h_\sigma"] & & V \\ & W \arrow[ul, "f"] \arrow[ur, "f^\sigma"'] & \end{tikzcd}$$

The h_σ are K_1-isomorphisms of V to V^σ ; they satisfy the identity

$$h_{\sigma\tau} = (h_\sigma)^\tau \circ h_\tau. \tag{5.1}$$

We are thus led to make precise the notion of descent of the base field in the following manner : given K_1-isomorphisms $h_\sigma : V \to V^\sigma$ satisfying (5.1), we seek a variety W/K and an isomorphism f satisfying the diagram.

Proposition 5.2.3. *Let V be a quasi-projective variety over K_1. Then the descend of the base field is possible and unique.*

When $K = \mathbb{F}_q$ and $K_1 = \mathbb{F}_{q^n}$, one can simplify the statement.

Corollary 5.2.1. *Let $\sigma : x \mapsto x^q$ be a generator of Gal(K_1/K). The variety V/K_1 can be descend over K iff there exists a K_1-isomorphism $h : V \mapsto V^\sigma$ such that*

$$h^{\sigma^{n-1}} \circ \cdots \circ h^\sigma \circ h = 1.$$

5.2.3 Torelli theorem

Let K be a field. Let X, X' two curves defined over K. We are giving a precise version of Torelli's theorem as Serre does (see Appendix of [Lau01]). Torelli's theorem allows us to relate information on the curve with information on the Jacobian and is used in the part about automorphisms (2.2.4) and about maximal curves (3.3.3).

Theorem 5.2.1. *Let X be a hyperelliptic curve. Then for all isomorphism*

$$F : (Jac(X), \Theta) \to (Jac(X'), \Theta')$$

there exists a unique isomorphism $f : X \to X'$ inducing F.

Theorem 5.2.2. *Let X be a non hyperelliptic curve. Then for all isomorphism*

$$F : (Jac(X), \Theta) \to (Jac(X'), \Theta')$$

there exists a isomorphism $f : X \to X'$ and $e = \pm 1$ such that $F = ef_J$ where f_J is the isomorphism induced by f. The couple (f, e) is uniquely determined by F.

Note that X is hyperelliptic iff there exists an automorphism s of X such that $s_J = -1$.

Corollary 5.2.2.

$$Aut(Jac(X), \Theta) = \begin{cases} Aut(X) & \textit{if } X \textit{ is hyperelliptic} \\ \{\pm 1\} \times Aut(X) & \textit{if } X \textit{ is non hyperelliptic} \end{cases}$$

Relations between the curve and its Jacobian play a crucial role in geometry. It is not a surprised that a lot of interesting conjectures turn around this topic. Let us mention :

- By dimension argument it is not difficult to see that every principally polarized abelian variety is not isomorphic to a Jacobian (the moduli spaces dimensions are respectively $g(g+1)/2$ and $3g-3$). However, the explicit characterization (over $\mathbb{C}$) of Jacobians is a famous problem called *Schottky problem.*
- *Oort's conjecture* : is every abelian variety over $k = \overline{\mathbb{F}_p}$, k-isogenous to a Jacobian ?
- Howe–Maisner–Nart's work : when is an abelian surface over $k = \mathbb{F}_q$, k-isogenous to a Jacobian ?

5.2.4 Cohomology

Let X be a scheme of finite type over k, algebraically closed of characteristic p (X will be for us a curve or an abelian variety). We can associate to X étale cohomology groups, denoted $H^i(X_{\text{ét}}, \mathbb{Z}_l)$. These groups have been created to give good analogues of the standards $H^i(X, \mathbb{Z})$ in characteristic 0. We will not give any details about this construction here and just give the properties needed.

1. the groups $H^i(X_{\text{ét}}, \mathbb{Z}_l)$ are $\mathbb{Z}_l$-modules. They are trivial except in the range $0 \leq i \leq 2n$ where n is the dimension of X. They are known to be finite dimensional if X is proper over k.
2. $H^i(X_{\text{ét}}, \mathbb{Z}_l)$ is a contravariant function in X.
3. Let $X = A$ be an abelian variety.
   - There is a canonical isomorphism $H^1(A_{\text{ét}}, \mathbb{Z}_l) \simeq T_l(A)^*$. If A is defined over a finite field k_0 then this isomorphism is compatible with the $\mathrm{Gal}(k/k_0)$-action.
   - The cup-product pairings define isomorphisms
   $$\Lambda^r H^1(A_{\text{ét}}, \mathbb{Z}_l) \simeq H^r(A_{\text{ét}}, \mathbb{Z}_l).$$
   In particular $H^r(A_{\text{ét}}, \mathbb{Z}_l)$ is a free $\mathbb{Z}_l$-module of rank $\binom{2g}{r}$.
4. Let $X = C$ a curve and $J = \mathrm{Jac}(C)$ then we have a canonical isomorphism $H^1(C_{\text{ét}}, \mathbb{Z}_l) = H^1(J_{\text{ét}}, \mathbb{Z}_l) = T_l(J)^*$.

Moreover we have the fundamental theorem for which these groups were originally introduced :

Theorem 5.2.3 (Lefschetz fixed-point formula). *Let X be smooth and proper over k. Let $f : X \to X$ be a morphism with isolated fixed points, and for each point $x \in X$, assume that the action $1 - df$ on regular differentials in injective. Denote $L(f, X)$ the number of fixed points of f. Then*

$$L(f, X) = \sum (-1)^i tr(f | H^i(X_{\acute{e}t}, \mathbb{Q}_l)).$$

Remark 50. We have the comparison theorem [KL02] : if X is smooth and proper over $\mathbb{C}$ then

$$H^i(X_{\text{ét}}, \mathbb{Z}_l) \otimes \mathbb{C} \simeq H^i(X_{\text{an}}, \mathbb{C}).$$

5.3 Appendix C : reduction and lifting

In the following we fix a discrete valuation field K (e.g. $K = \mathbb{Q}_p$ or $\mathbb{F}_p((x))$), with valuation ν and residue field k. The interested reader will find more in [Liu03].

5.3.1 Reduction

Denote by R the valuation ring of K (e.g. $\mathbb{Z}_p$ or $\mathbb{F}_p[[x]]$), and $p = \mathrm{Char}(k)$. It is not necessary to suppose R complete.
Let us start with the definition of reduction. To give a projective variety X_K is to give some homogeneous polynomials $F_1, \ldots, F_m \in K[T_0, \ldots, T_n]$ with coefficients in K.

Definition 5.3.1. *A* model X *of* X_K *over* R *is a projective scheme over* R *(defined by homogeneous polynomials* $G_1, \ldots, G_m \in R[S_0, \ldots, S_n]$*) such that the projective variety over* K *associated to the* G_i*'s is isomorphic to* X_K*. We require furthermore the technical condition that* X *is a flat scheme over* R*. This condition is satisfied for example if* X *is integral (e.g. the ideal generated by the* G_i*'s is a prime ideal).*

Definition 5.3.2. *Let* $\overline{G_i}$ *be the canonical image of* G_i *in* $k[S_0, \ldots, S_m]$*. Then the* $\overline{G_i}$*'s define a projective variety over* k *denoted by* X_k*. It is called a* reduction *of* X_K*. It depends on the choice of a model of* X_K*. One has* $X_k = X \otimes_R k$*. The flatness hypothesis on* X *insures that* X_k *has the same dimension as* X_K*.*

Remark 51. If X_K is a smooth projective curve of genus $g \geq 1$ then X_K has a so called minimal regular model which is unique.

Definition 5.3.3. *We say that* X_K *has* good reduction *if there exists a model* X *such that* X_k *is smooth. Note that* X_k *is then unique if* X_K *is a curve or an abelian variety. If there exists a finite extension* K'/K *such that the curve* $X_{K'} = X_K \otimes \mathrm{Spec}(K')$ *has good reduction, we will say that* X_K *has* potentially good reduction

Example 11. *Suppose that* $p \neq 3$*. Let* X_K *be the elliptic curve defined by*

$$y^2 z = x^3 + az^3$$

with $1 \leq \nu(a) \leq 5$*. The same equation defines a plane model* P *of* X_K *over* R *whose reduction is a singular curve :*

$$y^2 z = x^3.$$

One can show that actually X_K *cannot have good reduction. However if we enlarge the base field* K *to* $K' = K[\alpha]$ *by including a* 6*-th root* α *of* a*, then*

$$(y/\alpha^3)^2 z = (x/\alpha^2)^3 + z^3$$

defines a model of $X_{K'}$ *with good reduction.*

What happens to the automorphism group when one reduces a curve ?

Proposition 5.3.1 ([DM69, Th.1.11]). *If the curve C_K has good reduction, then $Aut_K(C_K)$ is a subgroup of $Aut_k(C_k)$.*

What happens to the Jacobian of the curve ?

Proposition 5.3.2. *If the curve C_K has good reduction, then its Jacobian J_K also and $Jac(C_k) = J_k$.*

Remark 52. The converse is not true : it is possible that the Jacobian has good reduction but not the curve. For instance, if one consider a genus 2 curves with complex multiplication then its Jacobian has (potentially good reduction) everywhere. But of course for a prime which divides the minimal discriminant the curve has bad reduction. Note that this is reflected by the fact that the Jacobian reduces to a product of two supersingular elliptic curves with the trivial polarization (*superspecial form*) ; it is not then the Jacobian of a curve.

5.3.2 Lifting

We will suppose that R is complete. Let Z be a projective variety over k. We want to lift Z to a smooth projective variety X_K over K, i.e to find a projective scheme X over R with smooth generic fiber such that $X_k \simeq Z$. When such a X exists we say that Z can be *lifted* to K.
One can try to lift naively Z by lifting defining polynomials.

Proposition 5.3.3. *Let Z be a complete intersection in a projective space $\mathbb{P}^n_k$, then Z can be lifted naively to K.*

Remark 53. Note that in general (when Z is not a complete intersection), the naive lifting X may not be flat over R.

Proposition 5.3.4. *Any projective smooth curve or abelian variety over k can be lifted to K.*

By analogy with the lift of covers of curves (see 2.2.4), one would like to lift more than only the abelian variety, namely its endomorphism ring.
Let suppose that $k = \mathbb{F}_q$ and denote by $K = \mathbb{Q}_q$ the unique unramified extension of $\mathbb{Q}_p$ of degree $[k : \mathbb{F}_p]$. We denote by $R = \mathbb{Z}_q$ its ring of integers. We want to lift an abelian variety A/k over K in such a way that we lift also its endomorphism ring. This is not always possible : if A is a supersingular elliptic curve, its endomorphism ring is a quaternion algebra, of rank 4 over $\mathbb{Z}$ when the maximal rank in characteristic 0 is 2.

Theorem 5.3.1 ([Mes72, V, Th.3.3, Cor. 3.4]). *Let A/k be an ordinary abelian variety (see 1.3.4 for ordinary). There exists an unique –up to isomorphism– abelian scheme $A^{\uparrow}$ over Spec(R) such that $A^{\uparrow} \otimes k \simeq A$ and*

$$End_K(A^{\uparrow}) \simeq End_k(A).$$

We call $A^{\uparrow}$ the canonical lift *of A.*

If $f \in \mathrm{End}_k(A)$, we denote $f^{\uparrow} \in \mathrm{End}_K(A^{\uparrow})$ its canonical lift.

Remark 54. This theorem was proved in the case of elliptic curves by par Deuring [Deu41] then generalized by Lubin, Serre and Tate [LST64].

Corollary 5.3.1. *Let $\hat{A}$ be the dual abelian variety of A. Then $(\hat{A})^{\uparrow} \simeq \hat{A^{\uparrow}}$.*
Moreover, all polarization of A defined over k (resp. principal polarization) can be lifted to a polarization of $A^{\uparrow}$ defined over K (resp. principal polarization).

Over the finite field, the Frobenius endomorphism has the same action as the Galois action of the Frobenius automorphism of k. If one denotes by σ the Frobenius substitution of $\mathbb{Q}_q/\mathbb{Q}_p$, which lifts the action of the Frobenius of k, σ is not the lift of the geometric action (because this one has now a non-trivial kernel !). However we have the following corollary.

Corollary 5.3.2 ([Mes72, Appendix, Cor 1.2]). *$A^{\uparrow}$ is the canonical lift of A iff there exists $Fr^{\uparrow} : A^{\uparrow} \to {}^{\sigma}(A^{\uparrow})$ lifting Fr.*

Chapter 6

Tutorials

6.1 My first steps in MAGMA

To start : type magma (and return).

6.1.1 Useful tips

The most important thing is the help. There exist two sorts (three including me) : the html files are the most convenient. They contain, besides the description of each command, examples and even mathematical background. You can access commands by theme (finite groups, commutative algebra, algebraic geometry) or through the index. The second help is online : when you want information about a command, let's say `RandomPrime`, you type `RandomPrime;`.

A last tip before we start : there is a automatic completion with 'tab'. This is useful when you do not remember exactly the name : MAGMA follows very closely the exact definition.

6.1.2 First steps

We will start with some examples that look really similar to MAPLE. To Evaluate an expression you need to end it with `;`. To define an object you write `f:=`.... As you may see it does not display the result. To see it you have to write `f;`.

1. Compute $\frac{123}{10} + \frac{33}{127}$.
2. Compute $2 + \sqrt{3}$. What is the precision ?
3. Compute 200! and factorize this number.
4. Is $2^{1233} + 321$ prime ?

Some examples how to handle sets, sequences, lists :

1. Define the sets $I = \{1, 4, 10\}$, $J = \{2, 4, 8\}$. Do the following operations : $I \cup J$ and $I \cap J$.
2. Define the set $P = \{p \ /p < 100 \text{ prime}\}$. How many elements in P ? Extract the 20th prime.
3. Create a random list of 100 integers between 10 and 2000.

6.1.3 Creation of basic fields and rings

Unlike MATHEMATICA/MAPLE, MAGMA require to define properly where you are working. You cannot open a MAGMA section and write : $f = x^3 + 3;$. MAGMA does not know yet what is x. It is sometimes a bit tedious when you want to work with polynomials in a lot of variables but the counterpart is that it allows much more objects than the two others softwares : polynomials over extensions of finite fields or p-adic fields, matrices with coefficients in function fields .... And it is much more accurate, mathematically speaking !

Start with $\mathbb{Q}, \mathbb{R}, \mathbb{C}$:

1. Define $F = \mathbb{Q}$. Define its ring of integers ($\mathbb{Z}$ of course).
2. Define the real field FR with precision 200. Create π. Compute $s = \exp(\pi\sqrt{163}) - 262537412640768744$ in FR.
3. Compute $s = \sqrt{5} + \sqrt{2} + 7$. Find the possible minimal polynomial.
4. Create $FC = \mathbb{C}$. Compute the j-invariant associated to $(1 + i\sqrt{163})/2$.

Very important fields for us are finite fields :

1. Create the field $F = \mathbb{F}_{23}$.
2. Add 20 and 5 in this field.
3. Create the field $K = \mathbb{F}_{23^5}$. What is a defining polynomial for this field ?

We will see more fields in the next sessions (in particular p-adics).
Now that we have defined some basic fields, we can construct objects on them. The most important ones are the polynomials rings.

1. Create the polynomial ring R with variable x over $\mathbb{F}_5$.
2. Create the polynomial $f = x^6 + 3x + 3$. Evaluate f at 2. Is f irreducible ? What is its splitting field ? Call it $F < w >$.
3. Create the polynomial ring $R2$ with variable y over F. Create the polynomial $g = y^3 + wy + 4$. Compute the resultant of f and g.

4. Create the polynomial ring P with variables u, v over F. Let $s_1 = u^3 + v^3 - 3u^2 + wvu$ and $s_2 = u^5 + w + v^3$. Extract the coefficient of uv in s_1.

5. Compute the resultant r of s_1 and s_2 wrt v. Find its factorization over F. Create the extension of F defined by one of the irreducible factors of degree 4.

Remark 55. You can recall information about the objects you have created : try `Parent(r);` for example.

6.2 Geometry

Now that we have seen the basics objects, we are going to focus on algebraic geometry and more specifically on curves.
Let's start with an easy example :

1. Define the polynomial ring P with variables x, y, z over $\mathbb{F}_{11}$.

2. Define the polynomial $f = x^3y + y^3z + z^3x$.

3. Define the projective space associated to P.

4. Define the curve $C : f = 0$.

5. Is the curve irreducible/absolutely irreducible ?

6. Is the curve singular ?

7. What is the genus of C ?

8. Find the set S of flexes of C.

A less straightforward example is the following.

1. Define the polynomial ring R with variables x, y, z, u, v over the rationals.

2. Define the 3 homogeneous polynomials f_1, f_2, f_3 :

$$\begin{cases} f1 = x^2 + y^2 + z^2 - uv \\ f2 = xu - yv \\ f3 = 2x^2 + 3y^2 - zy + u^2 + v^2 \end{cases}$$

3. Define the projective space associated to R

4. Define the Scheme $C : f_1 = f_2 = f_3 = 0$.

5. What is its dimension ?

6. Is it singular ?

7. What is its genus (caution : MAGMA can only compute genus of plane curves).

Let's finish the geometry part with a singular example.

1. Define the curve $C/\mathbb{Q} : x^4z + 2z^3xy + x^3z^2 - 5xy^3z = 0$.
2. What are the singular points of C over $\mathbb{Q}$ (which multiplicity ?) ? Over $\overline{\mathbb{Q}}$?
3. Reduce the curve modulo 7. Has it more rational singularities ?

There are also particular family of curves for which MAGMA has already more commands available. Among them elliptic curves, hyperelliptic curves and modular curves.

1. Create the elliptic curve $E/\mathbb{Q} : y^2 = x^3 + 3x + 5$.
2. What is its rank ? Find a generator P of the Mordell-Weil group.
3. Compute $3P$.
4. Create the hyperelliptic curves $C_1/\mathbb{Q} : y^2 + (x^2 + 1)y = x^5 + 3x + 1$ and $C_2/\mathbb{Q} : y^2 + (x^2 - 2x + 2)y = x^5 - 5x^4 + 10x^3 - 10x^2 + 8x - 3$.
5. Are they isomorphic over $\mathbb{Q}$?

6.3 Arithmetic

Now we are about to introduce arithmetic over finite fields. The most important thing is to be able to compute the Frobenius polynomial.

1. Take the quartic C defined in the previous section.
2. What is its number of points over $\mathbb{F}_{11}, \mathbb{F}_{11^2}, \mathbb{F}_{11^3}$?
3. Compute the Frobenius polynomial. One may use the following formulas. If $\chi(T) = \sum c_{2g-i}T^i$ is the Frobenius polynomial of a curve $C/\mathbb{F}_q$, define $N_i = |C(\mathbb{F}_{q^i})| - q^i - 1$, then

$$\begin{aligned}
c_0 &= 1, \\
c_1 &= N_1, \\
c_i &= (N_i + \sum_{\substack{j+k=i \\ 1 \leq j,k \leq i-1}} c_k \cdot N_j)/i, \quad i = 2, \ldots, g, \\
c_{2g-i} &= q^{g-i} c_i, \quad i = 0, \ldots, g-1
\end{aligned}$$

4. Define F the function field associated to C. Find again (and quicker) the characteristic polynomial.

5. Is Jac(C) simple ?

6. Consider the singular curve $C/\mathbb{F}_7 : x^4z + 2z^3xy + x^3z^2 - 5xy^3z + y^5 = 0$. What is the genus of a model ? What is its characteristic polynomial ?

7. Is the Jabobian simple/ absolutely simple ?

6.4 More advanced examples

6.4.1 p-rank

- For $11 \leq N \leq 30$ and $2 \leq p \leq 100$ prime not dividing N, give statistics about the repartitions of the p-rank of the reduction modulo p of $X_0(N)$.

- This is a problem by R. Pries. Let $p \geq 7$ a prime number and $E_i/\mathbb{F}_{p^2} : y^2 = x(x-1)(x-\lambda_i)$ the $(p-1)/2$ supersingular elliptic curves. For each triple $\{\lambda_1, \lambda_2, \lambda_3\}$ we define the genus 2 curve $C : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$.

    1. How is the repartition of the p-rank of these curves ?
    2. Is there something interesting to say ?

6.4.2 Automorphisms

Let G, H, M be the following matrices

$$G = \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix},\ H = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\ M = \frac{-1}{\sqrt{7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix},$$

where ζ is a 7th root of unity.
Show that the automorphisms of $\mathbb{P}^2$ given by these matrices are automorphisms of the Klein's quartic $x^3y + y^3z + z^3x = 0$. What is the order of the group generated by these matrices ?

6.4.3 Maximal curves

1. Verify the value of $N_q(g)$ for $g = 1, 2, 3$ and $q = 2, 4, 8, 3, 9$.

2. Construct a genus 5 curve over $\mathbb{F}_3$ with 13 rational points.

6.4.4 Cryptography

1. Implement the genus 1 AGM algorithm to compute the number of points on an elliptic curves over $\mathbb{F}_{2^N}$. Give a bench of times.

2. Create a genus 3 curve C over $k = \mathbb{F}_{17}$. Compute the order N of $J = \mathrm{Jac}(C)(k)$. Take a rational divisor D on C and verify that $N \cdot D \sim 0$.

Bibliography

[Adl97] A. Adler, The Mathieu group M_{11} and the modular curve $X(11)$, Proc. London Math. Soc. **74**, (1997), 1-28.

[AN65] T.H. Ayashida & M. Nishi, existence of curves of genus 2 on a product of two elliptic curves, J. Math. Soc. Japan **17**, (1965), 1-16.

[BM89] J.-B. Bost & J.-F. Mestre, Moyenne Arithmético-géométrique et Périodes des courbes de genre 1 et 2, Gaz. Math., S.M.F. **38** (1989) , 36-64.

[BGS04] A. Boston, P. Gaudry & E. Schost, linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves, Proceedings of Fq7, Springer-Verlag, 2004.

[BG97] P. Bayer and J. González, On the Hasse-Witt invariants of modular curves. Experimental Math. **6** (1997), 57-76.

[BL92] Ch. Birkenhake & H. Lange, *Complex abelian varieties*, Springer-Verlag **302**, Berlin Heidelberg, 1992.

[Bou98] I.I. Bouw, *Tame covers of curves : p-rank and fundamental groups*, PhD thesis, 1998.

[Car02] R. Carls, Approximation of canonical lifts, in preparation, (2002) available on `http://www.math.leidenuniv.nl/~carls/`.

[Cha00] A. Chamberloir, Théorème d'algébricité en géométrie diophantienne, Séminaire Bourbaki **886**, 2000.

[Cox84] D. Cox, The arithmetic-geometric mean of Gauss, Enseign. Math. **30** (1984), 275-330.

[DM69] P. Deligne & D. Mumford, the irreducibility of the space of curves of given genus, Publ. Math. IHES **36**, (1969), 75-110.

[Deu41] M. Deuring, Die Typen der Multiplikatoringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ Hamburg **14** (1941), 197-272.

[Elk87] N.D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over Q, Invent. Math. **89** (1987), 561-567.

[Gau70] C.F. Gauss, *Werke*, Vol. **12**, Göttingen, (1870-1927).

[GV03] G. van der Geer et M. van der Vlugt, New table for the function $N_q(g)$, `http://www.wins.uva.nl/~geer` (2003).

[Gro71] A. Grothendieck & al., Revêtements étales et géométrie algébrique (SGA 1), Lecture Notes in Math. **224**, Springer-Verlag, Heidelberg (1971).

[Har75] R. Hartshorne : *Algebraic geometry*, Providence RI : American Mathematical Society (1975).

[Kan85] E. Kani, relations between the genera and the Hasse-Witt invariants of Galois coverings of curves, Can. Math. Bull. **28**, (1985), 321-327.

[KL02] M. Kisin & G. I. Lehrer, Equivariant Poincaré polynomials and counting points over finite fields, J. of Algebra **247**, (2002), 435-451.

[KS96] M.J. Klassen & E.F. Schaefer, Arithmetic and geometry of the curve $y^3+1=x^4$, Acta Arith. **74**, (1996), 241-257.

[KWZ] A. Kresch, J.L. Wetherell & M.E. Zieve, curves of every genus with many points I. Abelian and toric families, J. Algebra **250** (2002), 353-370.

[Kur82] I. Kuribayashi, On certain curves of genus three with many automorphisms, Tsukuba J. of Math. **6** (1982), 271-288. Verlag, (1972).

[Lag67] J.L. Lagrange, *Oeuvres*, Vol. **14**, Gauthiers-Villars, Paris (1867-1892).

[Lau99] K. Lauter, Non-existence of a curve over $\mathbb{F}_3$ of genus 5 with 14 rational points, Proc. AMS **128**, (1999), 369-374.

[Lau01] K. Lauter Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. With an appendix in French by J.-P. Serre. J. Algebraic Geom. **10** (2001), 19-36.

[Liu03] Q. Liu, reduction and lifting of finite covers of curves, Proceedings of the 2003 workshop on Cryptography and Related Mathematics, Chuo University (2003), 161-180, available at `www.math.u-bordeaux1.fr/~liu`.

[Lor96] D. Lorenzini : *An invitation to arithmetic geometry*, AMS **9**, 1996.

[LST64] J. Lubin & J.-P. Serre & J. Tate, *Elliptic Curves and formal groups*, notes disponibles sur `http://ma.utexas.edu/users/voloch/lst.html`, (1964).

[Man61] Ju. I. Manin, The Hasse-Witt matrix of an algebraic curve. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **25**, 1961, 153-172.

[Mes02] J.-F. Mestre, Algorithmes pour compter des points en petite caractéristique en genre 1 et 2, available at `www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps` (2002).

[McB61] A.M. Macbeath, On a theorem of Hurwitz, Proc. Glascow Math. Assoc. **5** (1961), 90-96.

[Mat04] M. Matignon & al., problems from the workshop on Automorphisms of Curves, Leiden 2004, available on `arxiv.org/abs/math.GR/0411059`.

[Ser96] B. Mazur, *Galois representations* in *Arithmetic Algebraic Geometry*, London Mathematical Society, Lecture Note Series 254, p. 255, (*issu d'une lettre du 26 juin 96 de J.P. Serre*).

[Mes72] W. Messing, *The crystals Associated to Barsotti-Tate Groups : with Applications to Abelian Schemes*, Lect. Notes in Math., **264**, Berin-Heidelberg-New-York, Springer (1972).

[Mil86] J.S. Milne, Abelian varieties, in *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[Mil98] J.S. Milne : *abelian varieties*, available on `www.math.lsa.umich.edu/~jmilne/`, (1998).

[Nak87] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. amer. math. society, **303**, (1987), 595-607.

[Nak87b] S. Nakajima, on abelian automorphism groups of algebraic curves, J. London Math. Soc. **36** (1987), 23-32.

[NR03] E. Nart & C. Ritzenthaler : *Non hyperelliptic curves of genus three over finite fields of characteristic two*, available on `http://front.math.ucdavis/math.NT/0312366`, submitted (2003).

[Pri03] R.J. Pries, conductors of wildly ramified covers III, Pacific J. of Math. **211**, (2003), 163-182.

[Raj98] C.S. Rajan, Automorphisms of $X(11)$ over characteristic 3 and the Mathieu group M_{11}, J Ramanujan Math. Soc. **13** (1998) 63-72.

[Rit02] C. Ritzenthaler, automorphismes des courbes modulaires en caractÚristique p, Manus. math. **109**, 49-62, (2002).

[Rit03] C. Ritzenthaler : *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*, PhD thesis, Université Paris 7 - Denis Diderot, June 2003 available on `http://www.math.jussieu.fr/~ritzenth`.

[Roq70] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern, Math. Z. **117** (1970) 157-163.

[Ros86] M. Rosen, Abelian varieties over $\mathbb{C}$, in *Arithmetic Geometry*, Cornell & Silverman, Springer-Verlag, (1986).

[Sch90] R. Schoof, algebraic curves and coding theory : Abuja 1990, courses notes (1990).

[Ser58] J.-P. Serre, Sur la topologie des variÚtÚs algÚbriques en caractÚristique p, Symp. Int. Top. Alg., Mexico (1958), 24-53 and in *oeuvres* **1**.

[Ser68] J.-P. Serre, *Corps Locaux*, Hermann, Paris, (1968).

[Ser75] J.-P. Serre, *Groupes algÚbriques et corps de classes*, Paris Hermann, 1975.

[Ser85] J.-P. Serre, *Rational points on curves over finite fields*, Notes by F. Gouvea of lectures at Harvard University, 1985.

[Sil92] J.H Silverman, *The Arithmetic of Elliptic Curves*, **106**, Springer, (1992).

[Sin74] B.Singh, On the group of automorphisms of a function field of genus at least two, J. Pure Appl. Algebra **4** (1974), 205-229.

[Sta04] N. Stalder, On p-rank representations, available on `arxiv.org/abs/math.GR/0402434`, (2004).

[Sti93] H. Stichtenoth, *algebraic function fields and codes*, Springer-Verlag Berlin Heidelberg, 1993.

[Sti73] H Stichtenoth, über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, I, II ,Arch. Math. **24** (1973), 527-544, 615-631.

[SV87] K.-0. Stöhr & J.-F. Voloch, A formula for the Cartier operator on plane algebraic Curves, J. für die Reine und Ang. Math., **377**, (1987), 49-64.

[Sub75] D. Subrao, The p-rank of Artin-Schreier curves, Manuscripta Math. **16** (1975), 169-193.

[Tat66] J. Tate, Endomorphisms of abelian varieties over finite fields, Inv. Math. **2**, (1966), 134-144.

[TV91] M.A. Tsfasman & S.G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its application **58**, kluwer academic publishers, 1991.

[Ver03] F. Vercauteren *computing Zeta functions of curves over finite fields*, PhD thesis, Katholicke Universiteit Leuven, 2003.

[VPV01] F. Vercauteren, B. Preneel & J. Vandewalle , A memory efficient version of Satoh's algorithm, Adv. in Cryptology, Eurocrypt (2001) (Innsbruck, Austria, Mai 2001), Lect. Notes in Comput. Sci. **2045**, 1-13, ed. Pfitzmann, Berlin, Heidelberg: Springer-Verlag (2001).

[WM71] W.C. Waterhouse & J.S. Milne, abelian varieties over finite fields, 1969 Number Th. Institute (Proc. Sympos. Pure Math, **XX**, State Univ. New-York, Stony Brook, N.Y.), Amer. Math. Soc., Providence, R.I. 1971, 53-64.