Chapter 2
The Geometry of the Drinfeld Curve

Let $Y$ be the Drinfeld curve

$$Y = \{(x, y) \in A^2(\mathbb{F}) \mid xy^q - yx^q = 1\}.$$

It is straightforward to verify that:

- $G$ acts linearly on $A^2(\mathbb{F})$ (via $g \cdot (x, y) = (ax + by, cx + dy)$ if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$) and stabilises $Y$;
- $\mu_{q+1}$ acts on $A^2(\mathbb{F})$ by homotheties (via $\xi \cdot (x, y) = (\xi x, \xi y)$ if $\xi \in \mu_{q+1}$) and stabilises $Y$;
- the Frobenius endomorphism $F: A^2(\mathbb{F}) \to A^2(\mathbb{F})$, $(x, y) \mapsto (x^q, y^q)$ stabilises $Y$.

Moreover, if $g \in G$ and $\xi \in \mu_{q+1}$, then, as endomorphisms of $A^2(\mathbb{F})$ (or $Y$), we have

$$g \circ \xi = \xi \circ g,$$
$$g \circ F = F \circ g,$$
$$F \circ \xi = \xi^{-1} \circ F.$$

We can therefore form the monoid

$$G \times (\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}})$$

which acts on $A^2(\mathbb{F})$ and stabilises $Y$.

The purpose of this chapter is to assemble the geometric properties of $Y$ and the action of $G \times (\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}})$ which allows us to calculate its $\ell$-adic cohomology (as a module for the monoid $G \times (\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}})$). A large part of this chapter is dedicated to the construction of quotients of $Y$ by the actions of the finite groups $G$, $U$ and $\mu_{q+1}$. 
2.1. Elementary Properties

The following proposition is (almost) immediate.

**Proposition 2.1.1.** The curve $Y$ is affine, smooth and irreducible.

*Proof.* $Y$ is affine because it is a closed subspace of the affine space $\mathbb{A}^2(\mathbb{F})$. It is irreducible because the polynomial $XY^q - YX^q - 1$ in $\mathbb{F}[X, Y]$ is irreducible (see Exercise 2.1). It is smooth because the differential of this polynomial is given by the $1 \times 2$ matrix $(Y^q - X^q)$, which is zero only at $(0, 0) \not\in Y$. $\square$

**Proposition 2.1.2.** The group $G$ acts freely on $Y$.

*Proof.* Let $g \in G$ and $(x, y) \in Y$ be such that $g \cdot (x, y) = (x, y)$. It follows that 1 is an eigenvalue of $g$ and, after conjugating $g$ by an element of $G$, we may assume that there exists an $a \in \mathbb{F}_q$ such that

$$g = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$ 

Then $x + ay = x$ and, as $y \neq 0$ (since $(x, y) \in Y$), we conclude that $a = 0$. $\square$

The next proposition is clear.

**Proposition 2.1.3.** The group $\mu_{q+1}$ acts freely on $\mathbb{A}^2(\mathbb{F}) \setminus \{(0, 0)\}$ and therefore also on $Y$.

Note however, that the group $G \times \mu_{q+1}$ does not act freely on $Y$: the pair $(-I_2, -1)$ acts as the identity. (Even the quotient $(G \times \mu_{q+1})/\langle(-I_2, -1)\rangle$ does not act freely, see Exercise 2.3.)

2.2. Interesting Quotients

We will now describe the quotients of $Y$ by the finite groups $G$, $U$ and $\mu_{q+1}$. In order to construct them we will use the following proposition, a proof of which can be found in [Bor, Proposition 6.6]. (Note that the proposition is far from optimal, but will be sufficient for our needs.)

**Proposition 2.2.1.** Let $V$ and $W$ be two smooth and irreducible varieties, $\varphi : V \to W$ a morphism of varieties, and $\Gamma$ a finite group acting on $V$. Suppose that the following three properties are satisfied:

1. $\varphi$ is surjective;
2. $\varphi(\nu) = \varphi(\nu')$ if and only if $\nu$ and $\nu'$ are in the same $\Gamma$-orbit;
3. There exists $\nu_0 \in V$ such that the differential of $\varphi$ at $\nu_0$ is surjective.

Then the morphism $\bar{\varphi} : V/\Gamma \to W$ induced by $\varphi$ is an isomorphism of varieties.
2.2.1. Quotient by $G$

The map

$$\gamma: \ Y \longrightarrow \mathbb{A}^1(\mathbb{F})$$

$$(x, y) \longmapsto xy^{q^2} - yx^{q^2}$$

is a morphism of varieties. It is $\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}}$-equivariant (for the action of $\mu_{q+1}$ on $\mathbb{A}^1(\mathbb{F})$ given by $\xi \cdot z = \xi^2 z$ and the action of $F$ given by $z \mapsto z^q$). An elementary calculation shows that $\gamma$ is constant on $G$-orbits. Even better, if we denote by $\bar{\gamma}: \ Y / G \rightarrow \mathbb{A}^1(\mathbb{F})$ the morphism of varieties obtained by passing to the quotient, we have the following.

**Theorem 2.2.2.** The morphism of varieties $\bar{\gamma}: \ Y / G \rightarrow \mathbb{A}^1(\mathbb{F})$ is a $\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}}$-equivariant isomorphism.

**Proof.** The $\mu_{q+1} \rtimes \langle F \rangle_{\text{mon}}$-equivariance is evident. In order to show that $\bar{\gamma}$ is an isomorphism we must verify points (1), (2) and (3) of Proposition 2.2.1.

Choose $a \in \mathbb{F}$. To show (1) and (2), it is sufficient to show that $|\gamma^{-1}(a)| = |G|$ (as $G$ acts freely on $Y$ by Proposition 2.1.2). After changing variables $(z, t) = (x, y / x)$, we have a bijection $\gamma^{-1}(a) \sim \mathcal{E}_a$, where

$$\mathcal{E}_a = \{(z, t) \in \mathbb{F}^\times \times \mathbb{F}^\times \mid t^q - t = \frac{1}{z^{q+1}} \text{ and } t^{q^2} - t = \frac{a}{z^{q^2+1}}\}.$$

As $t^{q^2} - t = (t^q - t)^q + (t^q - t)$, we obtain

$$\mathcal{E}_a = \{(z, t) \in \mathbb{F}^\times \times \mathbb{F}^\times \mid t^q - t = \frac{1}{z^{q+1}} \text{ and } \frac{1}{z^{q+1}} + \frac{1}{z^{q^2+q}} = \frac{a}{z^{q^2+1}}\}.$$

Or equivalently

$$\mathcal{E}_a = \{(z, t) \in \mathbb{F}^\times \times \mathbb{F}^\times \mid z^{q^2-1} - az^{q-1} + 1 = 0 \text{ and } t^q - t = \frac{1}{z^{q+1}}\}.$$

The polynomial $z^{q^2-1} - az^{q-1} + 1$ is coprime to its derivative, and therefore has $q^2 - 1$ distinct non-zero roots. For each of these roots, there are $q$ non-zero solutions $t$ to the equation $t^q - t = \frac{1}{z^{q+1}}$. Therefore

$$|\gamma^{-1}(a)| = |\mathcal{E}_a| = (q^2 - 1)q = |G|,$$

as expected.

We now turn to (3). Let $v = (x_0, y_0) \in Y$. The tangent space $\mathcal{T}_v(Y)$ to $Y$ at $v$ has equation $y_0^q x - x_0^q y = 0$ and the differential $d_v \gamma: \mathcal{T}_v(Y) \rightarrow \mathbb{F} = \mathcal{T}_{\gamma(v)}(\mathbb{A}^1(\mathbb{F}))$ is given by

$$d_v \gamma(x, y) = y_0^{q^2} x - x_0^{q^2} y.$$
Therefore, if \((x, y) \in \text{Ker} \ d_v \gamma\), then
\[
y_0^q x - x_0^q y = 0 \quad \text{and} \quad y_0^q x - x_0^q y = 0.
\]
The determinant of this system is
\[
- y_0^q x_0^q + x_0^q y_0^q = \left( x_0 y_0^q - y_0 x_0^q \right)^q = 1,
\]
therefore \(\text{Ker} \ d_v \gamma = 0\).

2.2.2. Quotient by \(U\)

The morphism
\[
\nu : \mathbf{Y} \longrightarrow \mathbf{A}^1(\mathbb{F}) \setminus \{0\}, \quad (x, y) \longmapsto y
\]
is well-defined and is a morphism of varieties. It is \(\mu_{q+1} \rtimes \langle F \rangle\)\_mon\_equivariant (for the action of \(\mu_{q+1}\) on \(\mathbf{A}^1(\mathbb{F}) \setminus \{0\}\) given by \(\xi \cdot z = \xi z\) and the action of \(F\) given by \(z \mapsto z^q\)). An elementary calculation show that \(\nu\) is constant on \(U\)-orbits. Even better, if we denote by \(\tilde{\nu} : \mathbf{Y} / U \to \mathbf{A}^1(\mathbb{F}) \setminus \{0\}\) the morphism of varieties induced by passing to the quotient, we have the following.

**Theorem 2.2.3.** The morphism of varieties \(\tilde{\nu} : \mathbf{Y} / U \to \mathbf{A}^1(\mathbb{F}) \setminus \{0\}\) is a \(\mu_{q+1} \rtimes \langle F \rangle\)\_mon\_equivariant isomorphism.

**Proof.** The \(\mu_{q+1} \rtimes \langle F \rangle\)\_mon\_equivariance is evident. To show that \(\tilde{\nu}\) is an isomorphism, we verify points (1), (2) and (3) of Proposition 2.2.1.

The surjectivity of \(\nu\) is clear. We also have
\[
\nu(x, y) = \nu(x', y') \iff \exists \ u \in U, \ (x', y') = u \cdot (x, y).
\]
Indeed, if \((x, y) \in \mathbf{Y}\) and \((x', y') \in \mathbf{Y}\) are such that \(y = y'\), then
\[
\left( \frac{x}{y} \right)^q - \frac{x}{y} = \left( \frac{x'}{y'} \right)^q - \frac{x'}{y'},
\]
which shows that \(\frac{x' - x}{y} \in \mathbb{F}_q\). Now, if we set \(a = \frac{x' - x}{y}\), then
\[
\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}.
\]
This shows (2). Point (3) is immediate. \(\square\)
2.2.3. Quotient by $\mu_{q+1}$

The morphism

$$\pi: \ Y \longrightarrow \mathbb{P}^1(\mathbb{F}) \setminus \mathbb{P}^1(\mathbb{F}_q)$$

$$(x,y) \longmapsto [x:y]$$

is well-defined and is $G \times \langle F \rangle_{\text{mon}}$-equivariant morphism of varieties (for the action of $G$ induced by the natural action on $\mathbb{P}^1(\mathbb{F})$ and the action of $F$ given by $[x:y] \mapsto [x^q:y^q]$). An elementary calculation show that $\pi$ is constant on $\mu_{q+1}$-orbits. Even better, if we denote by $\bar{\pi}: Y / \mu_{q+1} \rightarrow \mathbb{P}^1(\mathbb{F}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ the morphism of varieties induced by passage to the quotient, we have the following.

**Theorem 2.2.4.** The morphism of varieties $\bar{\pi}: Y / \mu_{q+1} \rightarrow \mathbb{P}^1(\mathbb{F}) \setminus \mathbb{P}^1(\mathbb{F}_q)$ is a $G \times \langle F \rangle_{\text{mon}}$-equivariant isomorphism.

**Proof.** The $G \times \langle F \rangle_{\text{mon}}$-equivariance is evident. To show that $\bar{\pi}$ is an isomorphism, we should verify points (1), (2) and (3) of Proposition 2.2.1, which is straightforward. $\Box$

2.3. Fixed Points under certain Frobenius Endomorphisms

In order to get the most out of the Lefschetz fixed-point theorem (see Theorem A.2.7(a) in Appendix A) we will need the following two results. Firstly, note that, if $\xi \in \mu_{q+1}$, we have

$$(2.3.1) \quad Y^\xi F = \emptyset.$$

Indeed, $(Y/\mu_{q+1})^F = \emptyset$ by Theorem 2.2.4. On the other hand, we have the following.

**Theorem 2.3.2.** Let $\xi \in \mu_{q+1}$. Then

$$|Y^{\xi F^2}| = \begin{cases} 0 & \text{if } \xi \neq -1, \\ q^3 - q & \text{if } \xi = -1. \end{cases}$$

**Proof.** Let $(x,y) \in Y^{\xi F^2}$. We then have

$$x = \xi x^q, \quad y = \xi y^q$$

and

$$xy^q - yx^q = 1.$$

As a consequence,

$$1 = (xy^q - yx^q)^q = x^q y^q - y^q x^q = \xi (x^q y - xy^q) = -\xi.$$

This shows that, if $\xi \neq -1$, then $Y^{\xi F^2} = \emptyset$. 
Therefore suppose that $\xi = -1$. We are looking for the number of solutions to the system

$$\begin{cases} x = -xq^2 & (1) \\ xy^q - yx^q = 1 & (2) \\ y = -yq^2 & (3) \end{cases}$$

However, if the pair $(x, y)$ satisfies (1) and (2), then it also satisfies (3). Indeed, if $(x, y)$ satisfies (1) and (2), then $x \neq 0$, $y = \frac{1 + yx^q}{x}$ and therefore

$$yq^2 = \left(\frac{1 + yx^q}{x}\right)^q = \frac{1 + y^q x^q}{x^q} = \frac{1 - xy^q}{x^q} = -\frac{yx^q}{x^q} = -y.$$ 

It follows that it is sufficient to find the number of solutions to the system given by equations (1) and (2). Now, $x$ being non-zero, there are $q^2 - 1$ possibilities for $x$ to be a solution of (1). As soon as we have fixed $x$, there are $q$ solutions to equation (2) (viewed as an equation in $y$). Indeed, as an equation in $y$, $xy^q - yx^q - 1$ has derivative $-x^q \neq 0$, and so this polynomial does not admit multiple roots. This gives therefore $(q^2 - 1)q$ solutions to equations (1) and (2), and the theorem follows. □

Remark – As $G$ acts freely on $Y$, the set $Y - F^2$ consists of a single $G$-orbit. □

### 2.4. Compactification

We will denote by $[x; y; z]$ homogeneous coordinates on the projective space $P^2(\mathbb{F})$. We view $A^2(\mathbb{F})$ as the open subset of $P^2(\mathbb{F})$ defined by

$$A^2(\mathbb{F}) \simeq \{ [x; y; z] \in P^2(\mathbb{F}) \mid z \neq 0 \}.$$ 

We identify $P^2(\mathbb{F}) \setminus A^2(\mathbb{F})$ with $P^1(\mathbb{F})$ (using the canonical isomorphism $[x; y] \mapsto [x; y; 0]$). The action of $G \times (\mu_{q+1} \rtimes \langle F \rangle)$ on $A^2(\mathbb{F})$ extends uniquely to $P^2(\mathbb{F})$: if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\xi \in \mu_{q+1}$ and $[x; y; z] \in P^2(\mathbb{F})$, then

$$g \cdot [x; y; z] = [ax + by; cx + dy; z],$$

$$\xi \cdot [x; y; z] = [\xi x; \xi y; z]$$

and

$$F[x; y; z] = [x^q; y^q; z^q].$$

Now let $\overline{Y}$ be the projective curve defined by

$$\overline{Y} = \{ [x; y; z] \in P^2(\mathbb{F}) \mid xy^q - yx^q = z^{q+1} \}.$$
The morphism
\[
Y \longrightarrow \mathcal{Y}
\]
\[
(x, y) \longmapsto [x; y; 1]
\]
is an open immersion and allows us to identify \(Y\) with \(\mathcal{Y} \cap A^2(F)\).

**Proposition 2.4.1.** The closed subvariety \(\mathcal{Y}\) of \(P^2(F)\) is the closure of \(Y\) in \(P^2(F)\). It is smooth and stable under the action of \(G \times (\mu_{q+1} \rtimes \langle F \rangle)\). Moreover,
\[\mathcal{Y} \setminus Y \simeq P^1(F_q),\]
with this isomorphism given by \([x; y] \in P^1(F_q) \mapsto [x; y; 0]\).

**Proof.** The only point needing a little work is the smoothness. The points of \(Y\) are smooth by Proposition 2.1.1. As \(G\) acts transitively on \(\mathcal{Y} \setminus Y = P^1(F_q) \simeq G/B\) (as a \(G\)-set), it is enough to show that \([1; 0; 0]\) is a smooth point of \(\mathcal{Y}\). For this, let us consider the open subvariety defined by \(x \neq 0\). In this open set (again isomorphic to \(A^2(F)\), this time via the morphism \((y, z) \mapsto [1; y; z]\)) \(\mathcal{Y}\) is defined by the equation \(y - y^q - z^{q+1} = 0\) and the differential at \((0, 0)\) of this polynomial is the \(1 \times 2\) matrix
\[
\begin{pmatrix}
1 & 0
\end{pmatrix},
\]
which is non-zero. \(\Box\)

We finish with a study of the quotient of \(\mathcal{Y}\) by \(\mu_{q+1}\). Consider the morphism
\[
\pi_0 : \mathcal{Y} \longrightarrow P^1(F)
\]
\[
[x; y; z] \longmapsto [x; y].
\]
It is well-defined, \(G\)-equivariant, and surjective. Moreover, it is constant on \(\mu_{q+1}\)-orbits and therefore induces, after passing to the quotient, a morphism of varieties \(\bar{\pi}_0 : \mathcal{Y}/\mu_{q+1} \rightarrow P^1(F)\).

**Theorem 2.4.2.** The morphism of varieties \(\bar{\pi}_0 : \mathcal{Y}/\mu_{q+1} \rightarrow P^1(F)\) is a \(G \times \langle F \rangle\) mon-equivariant isomorphism.

**Proof.** We omit the proof, as it follows the same arguments as those used in the proof of Theorem 2.2.4. \(\Box\)

### 2.5. Curiosities*

Independent of representation theory, the Drinfeld curve has interesting geometric properties which we discuss briefly here: it has a “large” automorphism group and gives a solution to a particular case of the Abhyankar’s Conjecture [Abh] about unramified coverings of the affine line in positive characteristic.
2.5.1. Hurwitz Formula, Automorphisms*

The group $\mu_{q+1}$ acts trivially on $\overline{Y} \setminus Y = \mathbb{P}^1(F_q)$. Also, as $\mu_{q+1}$ is of order prime to $p$, the morphism $\pi_0$ is tamely ramified: it is only ramified at the points $a \in \mathbb{P}^1(F_q)$ and ramification index at $a$ is $e_a = q + 1$. If we denote by $g(Y)$ the genus of $Y$, then

$$(2.5.1) \quad g(Y) = \frac{q(q-1)}{2}$$

as $Y$ is a smooth plane curve of degree $q + 1$. Note also that $\pi_0$ is a morphism of degree $\deg \pi_0 = q + 1$. We can therefore verify the Hurwitz formula [Har, Chapter IV, Corollary 2.4]

$$2g(\overline{Y}) - 2 = (\deg \pi_0)(2 \cdot g(\mathbb{P}^1(F)) - 2) + \sum_{a \in \mathbb{P}^1(F_q)} (e_a - 1),$$

as $g(\mathbb{P}^1(F)) = 0$.

We will now extend the group $G \times \mu_{q+1}$ to a bigger group $\mathcal{G}$ still acting on $Y$ (or $\overline{Y}$). Set

$$\mathcal{G} = \{ (g, \xi) \in \text{GL}_2(F_q) \times F_q^\times \mid \det(g) = \xi^{q+1} \}.$$

It is then straightforward to verify that,

$$(2.5.2) \quad \text{if } (g, \xi) \in \mathcal{G} \text{ and } (x, y) \in Y, \text{ then } g \cdot (\xi x, \xi y) \in Y.$$

This defines for us an action of $\mathcal{G}$ on $Y$ which extends naturally to an action on $\overline{Y}$. Set

$$\mathcal{D} = \begin{cases} \langle (-l_2, -1) \rangle & \text{if } q \equiv 3 \pmod{4}, \\ \langle (\sqrt{-1} l_2, -\sqrt{-1}) \rangle & \text{if } q \equiv 1 \pmod{4}. \end{cases}$$

Then $\mathcal{D}$ is a central subgroup of $\mathcal{G}$ contained in the kernel of the action on $Y$ (and on $\overline{Y}$). Even better, we have the following.

Lemma 2.5.3. The group $\mathcal{G}/\mathcal{D}$ acts faithfully on $Y$ (and $\overline{Y}$).

Proof. Let $(g, \xi)$ be an element of $\mathcal{G}$ which acts trivially on $Y$. Then $(g, \xi)$ acts trivially on $\overline{Y}$ (as $Y$ is dense in $\overline{Y}$) and, after passing to the quotient by $\{1\} \times \mu_{q+1}$ (which is a central subgroup of $\mathcal{G}$), we conclude that $g$ acts trivially on on $\mathbb{P}^1(F)$ (by Theorem 2.4.2). Therefore $g$ is a homothety: $g = \lambda l_2$, with $\lambda \in F_q^\times$.

Now, if $(x, y) \in Y$, we have $(g, \xi) \cdot (x, y) = (x, y)$, that is $\lambda \xi = 1$. Therefore $\xi = \lambda^{-1}$. On the other hand, $\det(g) = \xi^{q+1}$, which implies that $\lambda^2 = \xi^{q+1}$ or, in other words, $\lambda^{q+3} = 1$. As $\lambda^{q-1} = 1$, we collude that $\lambda^4 = 1$, which finishes the proof. $\Box$

Let $\Delta = \mathcal{D} \cap (G \times \mu_{q+1}) = \langle (-l_2, -1) \rangle$. 

Corollary 2.5.4. The group \((G \times \mu_{q+1})/\Delta\) acts faithfully on \(Y\).

Denote by \(p_1 : \mathcal{G} \to \text{GL}_2(\mathbb{F}_q)\) and \(p_2 : \mathcal{G} \to \mathbb{F}_q^\times\) the canonical projections, and \(i_1 : \mu_{q+1} \to \mathcal{G}, \xi \mapsto (l_2, \xi)\) and \(i_2 : \mathcal{G} \to \mathcal{G}, g \mapsto (g, 1)\). The group \(G \times \mu_{q+1}\) is contained in \(\mathcal{G}\) and we set \(d : \mathcal{G} \to \mathbb{F}_q^\times, (g, \xi) \mapsto \det(g)\). We have a commutative diagram

\[
\begin{array}{ccc}
1 & \mu_{q+1} & 1 \\
\downarrow i_2 & \downarrow i_2 & \downarrow p_2 \\
1 & G \times \mu_{q+1} & \mathcal{G} \\
\downarrow i_1 & \downarrow d & \downarrow p_1 \\
1 & G & \text{GL}_2(\mathbb{F}_q) \\
\end{array}
\]

in which all straight lines of the form \(1 \to \mathcal{G} \to \mathcal{G} \to \mathcal{G} \to 1\) are exact sequences (which follows essentially from the surjectivity of \(N_2\)). In particular,

\[(2.5.5) \quad |\mathcal{G}| = q(q^2 - 1)^2.\]

It follows from Lemma 2.5.3 that

\[|\text{Aut}\mathcal{Y}| \geq \begin{cases} 
\frac{q(q^2 - 1)^2}{2} & \text{if } q \equiv 3 \mod 4, \\
\frac{q(q^2 - 1)^2}{4} & \text{if } q \equiv 1 \mod 4.
\end{cases}\]

In particular, as soon as \(q \geq 7\), we have, by 2.5.1,

\[|\text{Aut}\mathcal{Y}| > 84(g(\mathcal{Y}) - 1) = 42(q - 2)(q + 1).\]

This illustrates the fact that the “Hurwitz bound” [Har, Chapter IV, Exercise 2.5] is not valid in positive characteristic.
2.5.2. Abhyankar’s Conjecture (Raynaud’s Theorem)*

It is not too difficult to show that if a finite group \( \Gamma \) is the Galois group of an unramified covering of the affine line \( \mathbb{A}^1(\mathbb{F}) \), then \( \Gamma \) is generated by its Sylow \( p \)-subgroups. The other implication was conjectured by Abhyankar and shown by Raynaud in a very difficult work [Ray].

**Raynaud’s theorem (Abhyankar’s conjecture).** A finite group \( \Gamma \) is the Galois group of an unramified Galois covering of the affine line \( \mathbb{A}^1(\mathbb{F}) \) if and only if it is generated by its Sylow \( p \)-subgroups.

**Example** – The morphism \( \mathbb{A}^1(\mathbb{F}) \to \mathbb{A}^1(\mathbb{F}), x \mapsto x^q - x \) is an unramified Galois covering of \( \mathbb{A}^1(\mathbb{F}) \) with Galois group \( \mathbb{F}^+ \).

By Proposition 1.4.1 and Lemma 1.2.2, the group \( G = \text{SL}_2(\mathbb{F}_q) \) is generated by its Sylow \( p \)-subgroups. By virtue of Raynaud’s theorem, \( G \) should be the Galois group of an unramified covering of \( \mathbb{A}^1(\mathbb{F}) \). In fact, in this particular case, the construction of such a covering is easy: the isomorphism \( \mathbb{Y}/G \cong \mathbb{A}^1(\mathbb{F}) \) and the fact that \( G \) acts freely on \( \mathbb{Y} \) (see Proposition 2.1.2) tells us that

\[
(2.5.6) \quad \mathbb{Y} \text{ is an unramified Galois covering of } \mathbb{A}^1(\mathbb{F}) \text{ with Galois group } \text{SL}_2(\mathbb{F}_q).
\]

**Exercises**

**2.1.** Show that the polynomial \( XY^q - YX^q - 1 \) in \( \mathbb{F}[X, Y] \) is irreducible. \( \text{Hint:} \) By performing the change of variables \( (Z, T) = (X/Y, 1/Y) \) reduce the problem to showing that \( T^{q+1} - Z^q - Z \) in \( \mathbb{F}[Z, T] \) is irreducible. View this as a polynomial in \( T \) with coefficients \( \mathbb{F}[Z] \) and use Eisenstein’s criterion.

**2.2.** Let \( \mathbb{F}[X, Y] \) a the polynomial ring in two variables, which we identify with the algebra of polynomial functions on \( \mathbb{A}^2(\mathbb{F}) \). If \( g \in G, P \in \mathbb{F}[X, Y] \) and \( v \in \mathbb{A}^2(\mathbb{F}) \), we set \( (g \cdot P)(v) = P(g^{-1} \cdot v) \).

(a) Show that this does indeed give an action of \( G \) via \( \mathbb{F} \)-algebra automorphisms.

(b) Show that \( XY^q - X^q \) and \( Y \) are algebraically independent and that \( \mathbb{F}[X, Y]^U = \mathbb{F}[XY^q - X^q, Y] \).

(c) Show that \( XY^q - YX^q \) divides \( XY^{q^2} - YX^{q^2} \).

(d) Show that \( D_1 = XY^q - YX^q \) and \( D_2 = \frac{XY^{q^2} - YX^{q^2}}{XY^q - YX^q} \) are algebraically independent.

(e) Show that \( \mathbb{F}[X, Y]^G = \mathbb{F}[D_1, D_2] \) (Dickson invariants).

(f) Use this to give another proof of Theorem 2.2.2.
2.3. Denote by $\Delta$ the subgroup of $G \times \mu_{q+1}$ generated by $(-I_2, -1)$. The purpose of this exercise is to show that $(G \times \mu_{q+1})/\Delta$ does not act freely on $Y$. To this end, choose $\xi \in \mu_{q+1} \setminus \{1, -1\}$ and let $v = (x, y) \in A^2(\mathbb{F})$ be an eigenvector of $d'(\xi)$ with eigenvalue $\xi$.

(a) Show that $xy^q - yx^q \neq 0$ (Hint: $xy^q - yx^q = x \prod_{a \in \mathbb{F}_q} (y + ax)$).

(b) Let $\kappa \in \mathbb{F}^\times$ be such that $\kappa^{-1-q} = xy^q - yx^q$. Show that $\kappa v \in Y$.

(c) Show that $(d'(\xi), \xi^{-1})$ stabilises $\kappa v \in Y$.

2.4. Let $Z = \{(x, y) \in A^2(\mathbb{F}) \mid x^{q+1} + y^{q+1} + 1 = 0\}$. We keep the notation $F$ for the restriction to $Z$ of the Frobenius endomorphism $F$ of $A^2(\mathbb{F})$. The purpose of this exercise is to construct an isomorphism of $Y$ and $Z$ which commutes with $F^4$.

(a) Show that $Z^{F^2} \neq \emptyset$. Deduce that there does not exist an isomorphism of varieties $\tau: Y \sim \rightarrow Z$ such that $\tau \circ F^2 = F^2 \circ \tau$.

Let $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $d \in \mathbb{F}$ be such that $d^{q+1} = -\frac{1}{z^q - z}$.

(b) Show that $d \in \mathbb{F}_{q^4}$.

(c) Let $g = \begin{pmatrix} d^q z^q & dz \\ d^q & d \end{pmatrix}$. Show that $g \in \text{GL}_2(\mathbb{F}_{q^4})$ and that $g(Z) = Y$.

2.5. Denote by $\tau: Y/U \rightarrow Y/G$ the canonical projection. Set $\tau' = \bar{\gamma} \circ \tau \circ \bar{\upsilon}^{-1}: A^1(\mathbb{F}) \setminus \{0\} \rightarrow A^1(\mathbb{F})$, so that the diagram

$$
\begin{array}{ccc}
Y/U & \xrightarrow{\tau} & Y/G \\
\downarrow \bar{\upsilon} & & \downarrow \bar{\gamma} \\
A^1(\mathbb{F}) \setminus \{0\} & \xrightarrow{\tau'} & A^1(\mathbb{F})
\end{array}
$$

commutes. Show that $\tau'(y) = y^{-q}(y^{q^2} + y)$.

† The author is indebted to G. Lusztig to whom this exercise is due.
Representations of SL2(F_q)
Bonnafé, C.
2011, XXII, 186 p., Hardcover
ISBN: 978-0-85729-156-1