Invariants of curves and Jacobians in positive characteristic

Re, R.S.G.R.

Link to publication

Citation for published version (APA):

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.
4 Supersingular quotients of Fermat curves

In this chapter we will give methods to construct many supersingular curves over algebraically closed fields of odd characteristic. We know from the preceding chapter, corollary 3.2, that the following Fermat curves over $\overline{\mathbb{F}_p}$ are supersingular:

$$X^{q+1} + Y^{q+1} + Z^{q+1} = 0,$$

with $q = p^n$. We also know that any quotient of a supersingular curve will be supersingular as well. Since the curve given in 6 has a big automorphism group, it will be possible to produce supersingular curves in many genera by taking quotients of this curve by subgroups of the automorphism group.

4.1 Automorphisms of Fermat curves

Let us consider the Fermat curve $F_m$ over an algebraically closed field $k$, with equation

$$X^m + Y^m + Z^m = 0.$$ 

Suppose that $\text{char}(k) = p > 0$ and that $m \geq 4$ is not divisible by $p$. Let $\mu_m$ be the group of $m$-th roots of 1 and $S_3$ be the permutation group of three elements. Then $\mu_m^3$ acts on $F_m$ by

$$(\xi, \eta, \lambda) : (X, Y, Z) \mapsto (\xi X, \eta Y, \lambda Z),$$

and its action factors through the quotient $\mu_m^2$ obtained by dividing by the diagonal subgroup $\mu_m \subset \mu_m^3$. Moreover $S_3$ acts on $F_m$ by permutations of $X, Y, Z$. It follows that the automorphism group $\text{Aut}(F_m)$ contains a subgroup isomorphic to a semidirect product

$$\mu_m^2 \rtimes S_3.$$ 

For $q = p^n$, one can define a "conjugation" in $\mathbb{F}_{q^2}$ by $\bar{x} = x^q$ and introduce the group

$$\text{PGU}(3, q^2) = \{ A \in \text{GL}(3, \mathbb{F}_{q^2}) : A \bar{A} = \lambda I \}/(\mathbb{F}_{q^2})^*.$$ 

If $m = q + 1$, i.e. in the case when $F_m$ is the curve (6), then $\text{PGU}(3, q^2)$ acts on $F_m$. Indeed, for any $A \in \text{PGU}(3, q^2)$, one can define an automorphism $\rho_A$ of the curve (6) in the following way:

$$\rho_A(X, Y, Z) = (X, Y, Z)A.$$ 

We can now state the classification theorem for the automorphism groups of Fermat curves.
Theorem 4.1 ([16]). The group $\text{Aut}(F_m)$ has one of the following forms:

1. If $m \neq p^r + 1$ for any integer $r$ then $\text{Aut}_k(F_m) \cong (\mu_m \times \mu_m) \rtimes S_3$.
2. If $m = p^r + 1 = q + 1$ then $\text{Aut}_k(F_m) = \text{PGU}(3, q^2)$.

The group $A = \text{PGU}(3, q^2)$ has order $q^3(q^2 - 1)(q^3 + 1)$. Its maximal subgroups have been classified by H.H. Mitchell in 1910, cf. [19]. We state the result of Mitchell as follows.

Theorem 4.2 (Mitchell, 1910). The maximal subgroups of $\text{PGU}(3, q^2)$, have the following orders, or are of the following types:

1) $(q + 1)q^3(q - 1)$,
2) $(q + 1)^2q(q - 1)$,
3) $(\mu_m)^2 \rtimes S_3$, as in theorem 4.1, of order $6(q + 1)^2$,
4) $3(q^2 - q + 1)$,
5) $(q - 1)q(q + 1)$,
6) $\text{PGU}(3, q^2)$, if $q = p^m$, $q = p^n$ and $n$ is an odd integer dividing $m$.
7) Finally, there exist exceptional subgroups of orders 216, 168, 360, 720, 2520, or 3 times such orders, appearing in $\text{PGU}(3, q^2)$ for certain given values of $q$.

We warn the reader that the list given on page 241 of [19] refers to subgroups of $\text{PSU}(3, q^2)$, i.e. the set of $A \in \text{PGU}(3, q^2)$ with determinant a cube in $F^*_q$. The list we stated above can easily be deduced from Mitchell’s list.

Quotients of the Fermat curve of degree $q + 1$ by many subgroups of $A = \text{Aut}_k(F_{q+1})$ were computed by Garcia, Stichtenoth and Xing in [8]. In this chapter we will extend and refine some of their results. The motivation for the authors mentioned was to find many maximal curves over $F_{q^2}$, as quotients of the hermitian curve $H \subseteq \mathbb{P}^2$ of equation:

$$H : \quad Y^qZ + YZ^q = X^{q+1}, \quad (7)$$

which is indeed isomorphic to the Fermat curve (6) over $F_{q^2}$.

We will consider also the following two maps from $H$ to $\mathbb{P}^1$.

- The projection $\pi : H \to \mathbb{P}^1$ defined by $\pi(X : Y : Z) = (X : Z)$. We will call $P_\infty$ the center $(0 : 1 : 0)$ of $\pi$. It is a point of $H(F_{q^2})$ and it is also the only ramification point of the map $\pi$.

- The projection $\pi' : H \to \mathbb{P}^1$ defined by $\pi'(X : Y : Z) = (Y : Z)$. We call $Q_\infty = (1 : 0 : 0)$ the center of $\pi'$. This point does not belong to $H$. Since $\text{PGU}(3, F_{q^2})$ acts transitively on $\mathbb{P}^2(F_{q^2})$, the roles of $Q_\infty$ and the projection $\pi'$ can be taken by any point.
in \( \mathbb{P}^2(\mathbb{F}_{q^2}) \) not belonging to \( H \) and the projection onto \( \mathbb{P}^1 \) with center this point, in the remainder of this section.

For the calculations in this chapter, we will not use every possible subgroup of \( \mathcal{A} \). For our purposes it will be enough to consider only some subgroups of the maximal subgroups of \( \mathcal{A} \) as in 1), 2) and 3) of the list in theorem 4.2. We describe more precisely these three types in the remainder of this section.

I. Let \( \mathcal{A}(P_\infty) \) be the stabilizer in \( \mathcal{A} \) of \( P_\infty \in H \). It is a group of order

\[
\text{ord } \mathcal{A}(P_\infty) = q^3(q^2 - 1),
\]

and indeed it is of the type 1) listed in theorem 4.2. A detailed description of this group can be found in [8]. The elements \( \sigma \in \mathcal{A}(P_\infty) \) are those automorphisms which on the affine model of \( H \) given by the equation \( y^q + y = x^{q+1} \) act in the following way:

\[
\sigma(x) = ax + b; \quad \sigma(y) = a^{q+1}y + ab^qx + c,
\]

with given \( a \in \mathbb{F}_{q^2}^* \), \( b \in \mathbb{F}_{q^2} \), and \( c \in \mathbb{F}_{q^2} \) such that \( c^q + c = b^{q+1} \).

\( \mathcal{A}(P_\infty) \) has a unique \( p \)-Sylow subgroup, consisting of those elements \( \sigma \in \mathcal{A}(P_\infty) \) with \( a = 1 \), i.e.

\[
\mathcal{A}_1(P_\infty) = \{ \sigma \in \mathcal{A}(P_\infty) \mid \sigma(x) = x + b, \ \sigma(y) = y + c, \ c^q + c = b \in \mathbb{F}_{q^2} \}.
\]

One can find in [12] an extensive treatment of the hermitian curves \( H \) and their automorphism of the type described above. We recall also that the curve \( H \) has exactly \( q^3 + 1 \) rational points over \( \mathbb{F}_{q^2} \), and these points form the orbit of \( P_\infty \), under the action of \( \text{Aut}(H) = \text{PGU}(3, q^2) \). Therefore the conjugates of \( \mathcal{A}(P_\infty) \) are all the stabilizers of the rational points over \( \mathbb{F}_{q^2} \).

II. Let \( \mathcal{A}(Q_\infty) \subset \mathcal{A} \) be the stabilizer of the point \( Q_\infty \in \mathbb{P}^2 \setminus H \) under the natural action of \( \mathcal{A} \cong \text{PGU}(3, \mathbb{F}_{q^2}) \) on \( \mathbb{P}^2 \). One observes also that \( \mathcal{A}(Q_\infty) \) is the subgroup of \( \text{Aut}(H) \) which fixes the \( g^{11}_{q+1} \) cut on \( H \) by the lines through \( Q_\infty \), which implies that the action of \( \mathcal{A}(Q_\infty) \) descends to \( \mathbb{P}^1 \) through \( \pi' \). Of course, such \( g^{11}_{q+1} \) depends on the choice of \( Q_\infty \), which can be an arbitrary point in \( \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus H \) in what follows. One sees that \( \mathcal{A}(Q_\infty) \) is an extension

\[
(1) \to \mu_{q+1} \to \mathcal{A}(Q_\infty) \to \Gamma \to (1).
\]

38
Here $\mu_{q+1}$ is the automorphism group of the covering $\pi'$, and $\Gamma$ is the automorphism group of $\mathbb{P}^1$ which leaves invariant the set of the ramification points of $\pi'$. Since this set admits a bijection to $\mathbb{P}^1(\mathbb{F}_q)$ induced by a suitable linear transformation over $\mathbb{F}_{q^2}$, one has

$$\Gamma \cong \text{PGL}(2, q).$$

The order of $A(Q_\infty)$ is therefore $(q + 1)^2q(q - 1)$ and so $A(Q_\infty)$ is an example of type (2) in the list of theorem 4.2.

III. Let $(\mu_{q+1})^2 \rtimes S_3$ be the group of the automorphisms of the Fermat curve (6) which admit a lifting to char$= 0$, as introduced in the discussion preceding theorem 4.1. It corresponds to case 3) in theorem 4.2.

In the next sections, we will compute the genera of quotients of the Fermat curves by groups of types I, II and III.

4.2 Groups of type I

Let $G$ be a subgroup of $A(P_\infty)$. The fact that $A=\text{PGU}(3, q^2)$ acts transitively on the set $H(\mathbb{F}_{q^2})$ yields immediately the following characterization of the conjugation class of $G$ in $A$.

**Proposition 4.1.** A subgroup $G \subset A$ fixes a point in $H(\mathbb{F}_{q^2})$ if and only if it is conjugate to a subgroup of $A(P_\infty)$.

Now let us assume $G$ a subgroup of $A(P_\infty)$. The elements $\sigma \in G$ act on $H$ by the formulas (8). Under those notations, one can define an homomorphism $h : G \to Aut(\mathbb{A}^1)$ by setting

$$h(\sigma) = (x \mapsto \sigma(x) = ax + b).$$

We introduce the following notations, similar to those adopted in [8]:

- $U_G = G \cap A_1(P_\infty)$, the only $p-$Sylow subgroup of $G$, with cardinality $|U_G| = p^u$.
  The elements of $U_G$ are those $\sigma \in G$ such that $\sigma(x) = x + b$.

- $V_G = h(U_G)$, with cardinality $|V_G| = p^v$.

- $W_G = \ker(h)$, with cardinality $|W_G| = p^w$.

- $m$ is the positive integer, prime to $p$, such that $|G| = mp^u$. We denote also $d = (m, q + 1)$ and $q = p^n$.  

39
By construction of the groups \( \mathcal{U}_G, \mathcal{V}_G \) and \( \mathcal{W}_G \), it is clear that \( u = v + w \). A formula for genus of the quotient curve \( H/G \) in terms of the parameters \( v, w, m \) and \( n \) has been proved in [8], theorem (4.4), p. 152. The result is the following.

**Proposition 4.2** (cf [8], Thm. (4.4)). The genus of \( H/G \) is given by:

\[
g(H/G) = \frac{(p^n - p^u)(p^n - (d - 1)p^v)}{2mp^u}
\]

In order to compute genera of quotient curves \( H/G \) from this formula, one needs to know for which values of the parameters \( u, v, w, m, d \), a subgroup \( G \subseteq \mathcal{A}(P_\infty) \) as above does exist. This is the problem we are going to study in the remainder of this section, obtaining some refinements of the results of [8].

First of all we observe that \( H/G \) is a quotient of \( H/\mathcal{U}_G \), so we can exclude those values of \( u, v, w \) for which \( g(H/\mathcal{U}_G) = 0 \). In the case \( m = 1 \) the formula (10) gives

\[
g(H/\mathcal{U}_G) = \frac{1}{2}p^{n-v}(p^{n-w} - 1),
\]

hence in order to \( g \) be a positive integer, we must have that

\[
u \leq n \quad \text{and} \quad w \leq n - 1.
\]

So we will assume that these inequalities are satisfied in the remainder of this section. Let us now investigate the relations between \( v, w \) and \( m \). We will use the homomorphism \( h \) from \( G \) to the group of affine transformations of \( \mathbb{A}^1(\mathbb{F}_q) \), defined above. In particular, we want to describe the possible images \( h(G) \). It is well known that any finite group of affine transformations with coefficients in a finite field \( k \), is conjugate over \( k \) to a group of the form \( T \rtimes C_m \), where \( T \) is a group of translations \( x \mapsto x + b \), and \( C_m \) is a cyclic group of order \( m \) generated by a transformation of the form \( x \mapsto ax \). Applying this fact to \( h(G) \), and observing that \( a \in \mathbb{F}_q^* \), it follows that

\[
\text{ord}(a) = m|q^2 - 1.
\]

With little calculation it is easy to see that, up to conjugation in \( \mathcal{A}(P_\infty) \), one may assume that \( G \) contains a transformation \( \sigma \) such that \( \sigma(x) = ax \) and \( \sigma(y) = a^{q+1}y \). Moreover \( \mathcal{T} = \mathcal{V}_G \). If \( \tau(x) = x + b \), then \( (\sigma^{-1}\tau\sigma)(x) = x + ab \), hence \( \mathcal{V}_G \) is invariant by multiplication by \( a \). So

\[
\mathcal{V}_G \quad \text{is a } \mathbb{F}_q[a]-\text{vector space}.
\]

40
One has \( \mathbb{F}_p[a] = \mathbb{F}_{p^r} \), with \( r = \min\{ j : m|p^j - 1 \} \), hence \( r|v \).

If \( r \) is an element of \( \mathcal{W}_G \) defined by \( \tau(x) = x, \tau(y) = y + c \), then one sees that \( \sigma \tau \sigma^{-1}(x) = x \) and \( \sigma \tau \sigma^{-1}(y) = y + a^{q+1}c \). Hence

\[
\mathcal{W}_G \text{ is a } \mathbb{F}_p[a^{q+1}]-\text{vector space.}
\]

We observe that \( \text{ord}(a^{q+1}) = m/d \). Setting \( s = \min\{ j : (m/d)|p^j - 1 \} \), we have that \( \mathbb{F}_p[a^{q+1}] \cong \mathbb{F}_p^s \), so \( s|w \).

Another necessary condition can be found as follows. A simple calculation shows that if \( \tau_1, \tau_2 \in G \) are such that \( \tau_1(x) = x + b_1 \) and \( \tau_2(x) = x + b_2 \), then the commutator \( \tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1} \) is in \( \mathcal{W}_G \), and it is defined by \( x \mapsto x, y \mapsto y + c \), with \( c = b_1^2 b_2 - b_1 b_2^2 \). For the sake of clarity, we will also use the notation

\[
b_1^2 b_2 - b_1 b_2^2 = [b_1, b_2],
\]

and we will write \( [\mathcal{V}_G, \mathcal{V}_G] \) for the \( \mathbb{F}_p \)-vector space generated by the \( [b_1, b_2] \), with \( b_1, b_2 \in \mathcal{V}_G \). Therefore, identifying \( \mathcal{W}_G = \{ \sigma \in G : \sigma(y) = y + c \} \) with the related subset of \( \{ c \in \mathbb{F}_{q^2} : c^d + c = 0 \} \), the desired condition of compatibility between \( \mathcal{V}_G \) and \( \mathcal{W}_G \) is the following:

\[
[\mathcal{V}_G, \mathcal{V}_G] \subseteq \mathcal{W}_G. \tag{11}
\]

Conversely, one can prove the following.

**Proposition 4.3.** Let \( a \) be any element of \( (\mathbb{F}_{q^2})^* \). Let us assume that \( \mathcal{V} \subseteq \mathbb{F}_{q^2} \) is a \( \mathbb{F}_p[a] \)-vector space, and \( \mathcal{W} \subseteq \{ x \in \mathbb{F}_{q^2} : x^d + x = 0 \} \) is a \( \mathbb{F}_p \)-subspace containing \( [\mathcal{V}, \mathcal{V}] \). Then there exists a subgroup \( G \subseteq A(P_{\infty}) \) with order of \( a \) equal to \( m \), \( \gamma \), \( \mathcal{V} \), \( \mathcal{W} \) and \( \mathcal{W}_G \cong \mathcal{W} \).

**Proof.** Let us fix a constant \( \gamma \in \mathbb{F}_{q^2} \) such that \( \gamma^d + \gamma = 1 \). For any \( b \in \mathcal{V} \) we define the element \( \tilde{b} \in A(P_{\infty}) \) by setting \( \tilde{b}(x) = x + b \) and \( \tilde{b}(y) = y + b^d x + \gamma b^{d+1} \). For \( c \in \mathcal{W} \) we define \( \tilde{c} \in A(P_{\infty}) \) by \( \tilde{c}(x) = x \) and \( \tilde{c}(y) = y + c \). Then we consider the subgroup \( \mathcal{U} \) generated by the set \( \{ \tilde{b} : b \in \mathcal{V} \} \cup \{ \tilde{c} : c \in \mathcal{W} \} \).

We know that \( \tilde{b} \tilde{b}_1 = \tilde{c} \tilde{b}_1 \tilde{b}_2 \) with \( c \in [\mathcal{V}, \mathcal{V}] \subseteq \mathcal{W} \), for any \( b_1 \) and \( b_2 \) in \( \mathcal{V} \). Moreover the elements \( \tilde{c} \) belong to the center of \( \mathcal{U} \). It follows that the elements of \( \mathcal{U} \) can be uniquely written in the form \( \tilde{b} \tilde{c} \), with \( b \in \mathcal{V} \) and \( c \in \mathcal{W} \). In particular, given the homomorphism \( h : A(P_{\infty}) \rightarrow \text{Aut}(A^1) \) such that \( h(\sigma) = (x \mapsto \sigma(x)) \), one finds:

\[
\mathcal{U} \cap \ker(h) \cong \mathcal{W} \text{ and } h(\mathcal{U}) \cong \mathcal{V}.
\]
Now let us consider also $\sigma \in A(P_\infty)$ such that $\sigma(x) = ax$ and $\sigma(y) = a^{q+1}y$. For any element $\tau = \bar{b} \in \mathcal{U}$ the conjugate $\sigma \tau \sigma^{-1}$ acts in the following way:

$$\sigma \tau \sigma^{-1}(x) = x + ab, \quad \sigma \tau \sigma^{-1}(y) = y + (ab)^q x + \gamma(ab)^{q+1} + a^{q+1}c.$$ 

Since $\mathcal{V}$ and $\mathcal{W}$ are closed under multiplication by $a$ and $a^{q+1}$, respectively, $\mathcal{U}$ is normal in the group $G$ generated by $\sigma$ and $\mathcal{U}$. Hence $G$ is a semi-direct product of $\mathcal{U}$ and the cyclic group of order $m$ generated by $\sigma$, and it is the subgroup of $A(P_\infty)$ we are looking for. \(\square\)

The algebraic conditions given above allow us to find some sufficient conditions on the parameters $m$, $v$ and $w$ for the existence of such subgroups $G$. Let $a \in (\mathbb{F}_q)^*$ be an element of order $m$, and let $\mathcal{V}$, $\mathcal{W}$, $v$, $w$, $d$ as above. We fix the following notations.

- $r' = \text{degree of } \mathbb{F}_p[a]$ over $\mathbb{F}_p = \min\{j : m|p^j - 1\}$.
- $r = \text{degree of } \mathbb{F}_p[a] \cap \mathbb{F}_q$ over $\mathbb{F}_p$. If $\mathbb{F}_p[a] \subseteq \mathbb{F}_q$, then $r' = r$. If $\mathbb{F}_p[a] \not\subseteq \mathbb{F}_q$, that is, if $r'$ does not divide $n$, then $r' = 2r$.
- Since $\mathcal{V}$ is a $\mathbb{F}_p[a]$-vector space, we can write $v = r't$. We see that $t \leq n/r$.
- $t' = \min\{j : j \geq t \text{ and } rj|n\}$.
- $s = \text{degree of } \mathbb{F}_p[a^{q+1}]$ over $\mathbb{F}_p = \min\{j : (m/d)|p^j - 1\}$. Note that $s|r$, since $\mathbb{F}_p[a^{q+1}]$ is contained in $\mathbb{F}_{p^t} = \mathbb{F}_p[a] \cap \mathbb{F}_q$.

The following result is an improvement on the results in [8], pp. 153-154.

**Theorem 4.3.** Under the notations above, there exists a group $G$ with parameters $m$, $v$ and $w$ if one of the following two conditions is satisfied:

1. $m|q - 1$, $r = r'$, $v = rt \leq n$, $w = is$, $0 \leq i \leq n/s$,

2. $m|q - 1$, $r = r'/2$, $v = 2rt$, $w = r \min(2t - 1, t') + is$, $w \leq n$, $i \geq 0$.

**Proof.** Case 1). Since $m|q - 1$, we have $\mathbb{F}_p[a] \subseteq \mathbb{F}_q$. In this case we can take $\mathcal{V}$ any $\mathbb{F}_p[a]$-vector space of dimension $t \leq n/r$ contained in $\mathbb{F}_q$. Since $[\mathcal{V}, \mathcal{V}] = (0)$, one has $[\mathcal{V}, \mathcal{V}] \subseteq \mathcal{W}$, for any $\mathbb{F}_p[a^{q+1}]$-vector space $\mathcal{W} \subseteq \{c : c^q + c = 0\}$ of dimension over $\mathbb{F}_p[a^{q+1}]$ equal to $i \leq n/s$. Therefore, by proposition 4.3, we can find a group $G$ for any choice of the parameters as in case 1.

Case 2). Since $m|q - 1$, we have $\mathbb{F}_p[a] \cong \mathbb{F}_{p^r}$ and we may write $\mathbb{F}_p[a] = \mathbb{F}_{p^r} \oplus c\mathbb{F}_{p^r}$, with $c$ an element, not belonging to $\mathbb{F}_q$, such that $c^2$ is not a square in $\mathbb{F}_{p^r}$. Then $c^2$ is not a square in $\mathbb{F}_q$ either, since $\mathbb{F}_{p^r} = \mathbb{F}_p[a] \cap \mathbb{F}_q$. One then immediately sees that $c^2 + c = 0$. 

42
Now let us take a field $\mathbb{F}_{p^{t'}} \subseteq \mathbb{F}_q$, which we write $\mathbb{F}_{p^{t'}} = \mathbb{F}_p[\beta] = \mathbb{F}_p \oplus \mathbb{F}_p \beta \oplus \cdots \mathbb{F}_p \beta^{t'-1}$. Let us consider the vector space $V$ over $\mathbb{F}_{p^{t'}}$ generated by $1, \beta, \cdots, \beta^{t'-1}$. The dimension of $V$ over $\mathbb{F}_{p^{t'}}$ is exactly $t$. Indeed, $1, \beta, \cdots, \beta^{t'-1}$ belong to $\mathbb{F}_q$ and they are independent over $\mathbb{F}_{p^t}$, whence it is easy to see that they are independent also over $\mathbb{F}_{p^{t'}} = \mathbb{F}_p \oplus c\mathbb{F}_p$. Now we observe that $[\mathbb{F}_p, \mathbb{F}_{p^t}] = [c\mathbb{F}_p, c\mathbb{F}_{p^t}] = (0)$, and that if $\gamma \in \mathbb{F}_p$ and $c\delta \in c\mathbb{F}_p$, then $[\gamma, c\delta] = 2c\gamma \delta = -[c\delta, \gamma]$. From this fact it follows that $[V, V] = c\mathbb{F}_p + c\beta \mathbb{F}_{p^t} + \cdots + c\beta^{2t-2} \mathbb{F}_{p^t}$, hence it has dimension over $\mathbb{F}_{p^{t'}}$ equal to $\min(2t - 1, t')$. Finally, we take any $\mathbb{F}_{p^t} = \mathbb{F}_p[a^{t'+1}]$-vector space $\mathcal{W}$ contained in $c\mathbb{F}_q = \{ x : x^q + x = 0 \}$, such that $\mathcal{W}$ contains $[V, V]$. We observe that the dimension over $\mathbb{F}_p$ of such a space $\mathcal{W}$ can assume any value $w = r \min(2t - 1, t') + is \leq n$, with $i \geq 0$. By proposition 4.3, we deduce the existence of a group $G$ with the requested properties.

**Remark.** We do not know if the sufficient conditions given in the theorem above are also necessary, under the assumption $v \leq n$. Looking at the construction in proposition 4.3, one sees that the necessity would follow if one could prove that

$$\dim_{\mathbb{F}_{p^t}} [V, V] \geq \min(2t - 1, t')$$

for $V$ an arbitrary $\mathbb{F}_p[a]$-vector space. We suspect this to be true, but we do not have a proof for it.

### 4.3 Groups of type II

Now we want to study the quotients $H/G$ with $G$ a subgroup of $\mathcal{A}(Q_\infty)$. Instead of considering the curve $H$, it is more convenient to consider the following curve:

$$H_1 : \quad Y^{q+1} = X^q Z - XZ^q. \quad (12)$$

It is isomorphic over $\mathbb{F}_p^2$ to the curve (7) by the linear transformation $(X, Y, Z) \rightarrow (Y, \gamma X, \gamma Z)$, with $\gamma \in \mathbb{F}_p^2$ such that $\gamma^{q-1} = -1$. We keep the notations of the preceding section, namely, $\pi'$ is the projection from $H_1$ onto $\mathbb{P}^1$ given by $\pi'(X : Y : Z) = (X : Z)$, $Q_\infty = (0 : 1 : 0)$ is the center of the projection $\pi'$, and $\mathcal{A}(Q_\infty)$ is the group of automorphisms of $H_1$ whose linear action on $\mathbb{P}^2$ fixes $Q_\infty$. We are interested in the case $G$ a subgroup of $\mathcal{A}(Q_\infty)$. This latter lies in an extension as (9), where now the term $\text{PGL}(2, \mathbb{F}_q)$ has the clear geometrical interpretation of being the subgroup of $\text{Aut}(\mathbb{P}^1)$ which fixes the set of ramification points $\mathbb{P}^1(\mathbb{F}_q)$. Then $G$ is an extension

$$0 \rightarrow G' \rightarrow G \rightarrow \overline{G} \rightarrow 0, \quad (13)$$

43
with $G' = G \cap \mu_{q+1}$ and $\overline{G}$ the image of $G$ in $\text{PGL}(2, \mathbb{F}_q)$.

In principle, for any subgroup $\overline{G} \subseteq \text{PGL}(2, \mathbb{F}_q)$, one could study the possible $G \subseteq \mathcal{A}(Q_\infty)$ covering it, and determine the curves $H_1/G$. For simplicity, we will report only our analysis of the following list of subgroups of $\overline{G} \subset \text{PGL}(2, \mathbb{F}_q)$. On the basis of our calculations, the cases left out do not seem to add new genera to our list of genera of supersingular curves.

1. $\overline{G}$ conjugate to a group of affine transformations $\sigma(x) = ax + b$, for $x$ the affine coordinate $x = X/Z$, $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$.

2. $\overline{G}$ cyclic of order $\mu$ any divisor of $q + 1$. This type of subgroup of $\text{PGL}(2, \mathbb{F}_q)$ can be realized as follows. There is an action of the cyclic group $\mathbb{F}_q^*/\mathbb{F}_q^*$, of order $q + 1$, permuting cyclically the $q + 1$ points of $\mathbb{P}^1(\mathbb{F}_q)$. This action can be obtained by representing $\mathbb{P}^1(\mathbb{F}_q)$ as $\mathbb{F}_q^*/\mathbb{F}_q^*$ and letting this latter act on itself by multiplication. Any non-trivial subgroup $\overline{G}$ of $\mathbb{F}_q^*/\mathbb{F}_q^*$ is cyclic of order $\mu$, with $\mu$ a divisor of $q + 1$, and it acts freely on $\mathbb{P}^1(\mathbb{F}_q)$.

3. $\overline{G}$ dihedral of order $2\lambda$, with $\lambda$ any divisor of $q - 1$. More precisely, we assume $\overline{G}$ generated by an affine transformation $\sigma(x) = ax$, with $a \in \mathbb{F}_q^*$ and $\text{ord}(a) = \lambda$, and an involution $\tau(x) = c/x$, with $c \in \mathbb{F}_q^*$.

4. $\overline{G}$ dihedral of order $2\mu$, with $\mu$ any divisor of $q + 1$. We will restrict our attention to those $\overline{G}$ which contain as normal subgroup of index 2 a cyclic group of order $\mu$ as in case 2. More precisely, these dihedral groups are generated by an element $\sigma$ of order $\mu$, with $\mu$ a divisor of $q + 1$ as in case 2, and an involution $\tau$ which permutes the fixed points of $\sigma$, which are two distinct points lying in $\mathbb{P}^1(\mathbb{F}_{q^2}) \setminus \mathbb{P}^1(\mathbb{F}_q)$.

Case 1. A group of affine transformations $x \mapsto \alpha x + \beta$ fixes the point at infinity $(1 : 0) \in \mathbb{P}^1$. So any lift $G \subset \mathcal{A}(Q_\infty)$ of $\overline{G}$ fixes the point $(1 : 0 : 0) \in H_1$, the unique point of $H_1$ over $(1 : 0)$. Since this point is rational over $\mathbb{F}_{q^2}$, we see that $G$ is conjugate to a subgroup of type I, by proposition 4.1. For our purpose of computing a table of supersingular genera, we will not need to compute the genus of $H_1/G$, since these genera are already obtained by method I.

Cases 2 and 4. We notice that there exist isomorphisms between the curve $H_1 : Y^{q+1} = X^qZ - XZ^q$ and the curve (6): $Y^{q+1} = -X^{q+1} - Z^{q+1}$. Moreover one can obtain such an isomorphism by a suitable linear transformation of $X, Z$, defined over $\mathbb{F}_{q^2}$. Let $\sigma \in \text{PGL}(2, \mathbb{F}_q)$ be an element of order $\mu | q + 1$ as in case 2, and $\tau \in \text{PGL}(2, \mathbb{F}_q)$ an
involution permuting the two fixed points of $\sigma$, as discussed about in Case 4. It is not
difficult to prove that, via a suitable choice of such an isomorphism, any lift of $\sigma$ to an
automorphism of $H_1$ can be read off from (6) as the automorphism $Y \mapsto Y, X \mapsto \eta X, Z \mapsto Z$, with $\eta$ a primitive $m$-th root of 1. Moreover, the involution $\tau$ can b lifted to an
automorphism of 6 of the form: $Y \mapsto Y, X \mapsto \xi Z, Z \mapsto X$, with $\xi$ any $(q + 1)$-th root of
1. Therefore we see that a group $G$ with $\overline{G}$ equal to $\langle \sigma \rangle$ or $\langle \sigma, \tau \rangle$ is isomorphic to a group
of automorphisms of (6) extendable to char= 0, see theorem 4.1, hence of type III, which
case will be completely worked out in the next section.

Case 3. $\overline{G}$ is generated by an affine transformation $\sigma(x) = ax$, with $a \in \mathbb{F}_q^*$ and ord $(a) = \lambda$, and an involution $\tau(x) = c/x$, with $c \in \mathbb{F}_q^*$. The group $G$ is the extension of $\overline{G}$
with a subgroup $G' \subseteq \mu_{q+1}$, as in (13). Therefore, the quotient map $H_1 \to H_1/G$ is the
composition of the quotient map $H_1 \to Y = H_1/G'$, followed by a quotient $Y \to Y/G''$, with $G'' \cong \overline{G}$. The curve $Y$ has an equation of the form:

$$Y : \quad y^m = x^q - x, \quad (14)$$

with $m$ a divisor of $q + 1$. The map $\pi : Y \to \mathbb{P}^1$ given by $\pi(x, y) = x$ is a Galois covering
with Galois group equal to $\mu_m$, and $Y$ has a group of automorphisms $A_Y$ equal to an
extension:

$$0 \to \mu_m \to A_Y \to \text{PGL}(2, q) \to 0.$$

So we will analyze all the possible quotients of such a curve $Y$ with a subgroup $G''$ of $A_Y$
such that $G'' \cong \overline{G} \cong D_{2\lambda} \subseteq \text{PGL}(2, q)$. The general lifts of $\sigma$ and $\tau$ to elements $\tilde{\sigma}$ and $\tilde{\tau}$
of $A_Y$ are defined by:

$$\tilde{\sigma}(x) = ax, \quad \tilde{\sigma}(y) = \beta y, \quad \text{with} \quad \beta^m = a,$$

$$\tilde{\tau}(x) = c/x, \quad \tilde{\tau}(y) = \gamma y/x^{(q+1)/m}, \quad \text{with} \quad \gamma^m = -c.$$

The relations defining $\overline{G}$ are $\text{ord}(\sigma) = \lambda$, $\text{ord}(\tau) = 2$ and $\tau \sigma \tau = \sigma^{-1}$. Therefore, in order
to ensure that $G'' \cong \overline{G}$, we have to impose that the group $G''$ is generated by $\tilde{\sigma}$ and $\tilde{\tau}$ and
that these elements satisfy the same relations as $\sigma$ and $\tau$. A little calculation shows that
the stated relations are equivalent to:

$$b^m = a, \quad (m, \lambda) = 1, \quad b^2 = a^{\frac{q+1}{m}},$$

$$\gamma^m = -c, \quad \gamma^2 = c^{\frac{q+1}{m}}. \quad (15)$$

It is also easy to prove that the every element in $G''$ commutes with every element in
$\mu_m = \text{Gal}(Y/\mathbb{P}^1)$. Hence the composition of Galois coverings $Y \to \mathbb{P}^1 \to \mathbb{P}^1/\overline{G}$ is Galois,
with Galois group equal to $\mu_m \cdot G''$. We have a diagram of Galois coverings:

$$
\begin{array}{ccc}
Y & \xrightarrow{q} & Y/G'' \\
\downarrow & & \downarrow \\
P^1 & \xrightarrow{p} & P^1/\overline{G},
\end{array}
$$

(16)

where $\pi$ and $\pi'$ have Galois group equal to $\mu_m$ and $p$, $q$ have Galois group isomorphic to $D_{2n}$. For a point $P \in Y$ let us denote $P' = \pi(P)$, $Q = q(P)$ and $Q' = p(P') = \pi'(Q)$. We will also denote by $r_{P/Q}$, $r_{P'/P'}$, $r_{Q/Q'}$ and $r_{P'/Q'}$ the ramification orders of the maps $q$, $\pi$, $\pi'$ and $p$ respectively, at the indicated points. We represent all this in the diagram:

$$
\begin{array}{ccc}
P & \xrightarrow{q} & Q \\
\downarrow & & \downarrow \\
P' & \xrightarrow{p} & Q', \\
\end{array}
$$

(17)

Then the following relation holds:

$$
r_{P/Q} \cdot r_{Q/Q'} = r_{P'/P'} \cdot r_{P'/Q'}.
$$

(18)

Now, the isomorphism $h \mapsto \tilde{h}$ between the Galois groups of $q$ and $p$ induces an injection between the inertia groups of $P$ and $P'$, since, for any $h \in G''$ such that $h(P) = P$ it holds $P' = \pi(P) = \pi(h(P)) = \tilde{h}(\pi(P)) = P'$. So we find that

$$
r_{P/Q} \mid r_{P'/Q'} \mid 2\lambda.
$$

Hence, by (17) we also have:

$$
r_{P'/P'} \mid r_{Q/Q'} \mid m.
$$

This means that $Q$ is a ramification point for $\pi'$ if $P$ is a ramification point for $\pi$. Since we know that $\pi$ is ramified above the set $P^1(\mathbb{F}_q)$ only and, over this set, the ramification is total, we find that:

$\pi'$ is ramified over $P^1(\mathbb{F}_q)/\overline{G}$, with total ramification, and maybe over some other point of $P^1/\overline{G}$.

We now consider separately the two cases according whether $m$ is odd or even.

1) $m$ odd. First of all, we need to observe that, for $m$ odd, the equations (15) have a unique solution $(b, \gamma) \in (\mathbb{F}_q^*)^2$ for any choice of $(a, c) \in (\mathbb{F}_q^*)^2$, with $\operatorname{ord}(a) = \lambda$. By (15)
we know that /.

Hence also \((m, 2\lambda) = 1\). So, from (18) and the observation that \(r_{P/Q}\) and \(r_{P'}\), \(2\lambda\) and \(r_{Q/Q'}, \tau_{P/P'}\) divide \(m\), we can deduce

\[
\frac{r_{P/Q}}{r_{P'/Q'}} = \frac{r_{P'}}{r_{Q/Q'}}. 
\]

Hence in case \(m\) odd, the Galois covering \(\pi'\) is ramified only over \(P^1(\mathbb{F}_q)/\overline{G}\), with total ramification. Therefore we will be able to compute the genus of \(Y/G''\) if we know the cardinality of \(P^1(\mathbb{F}_q)/\overline{G}\).

Lemma 4.1. Under the notations above, for \(m\) odd and prime to \(\lambda\), the cardinality of \(P^1(\mathbb{F}_q)/\overline{G}\) is equal to:

\[
|P^1(\mathbb{F}_q)/\overline{G}| = \frac{q - 1}{2\lambda} + \begin{cases} 
2 & \text{if } (q - 1)/\lambda \text{ is even} \\
1 & \text{if } (q - 1)/\lambda \text{ is odd}
\end{cases} 
\] (19)

Proof. One orbit for the action of \(\overline{G}\) on \(P^1(\mathbb{F}_q)\) is \(\{0, \infty\}\). A point \(x \in \mathbb{F}_q^* \cong P^1 \setminus \{0, \infty\}\) belongs to an orbit of \(\lambda\), or \(2\lambda\), elements according whether it is stabilized by one element of \(\overline{G}\) of the form \(\sigma^i\tau\), or not. If \(\sigma^i\tau(x) = x\) then \(x^2 = a^i c\). If \(a\) is a square in \(\mathbb{F}_q\), which happens if and only if \((q - 1)/\lambda\) is even, then there are \(2\lambda\) such points \(x\), or no such \(x\), according whether \(c\) is a square, or not. If there are \(2\lambda\) such points, then they are divided into two orbits with respect to the action of \(\overline{G}\). Therefore the total number of orbits for \((q - 1)/\lambda\) even and \(c\) a square is \(1 + (q - 1 - 2\lambda)/2\lambda + 2 = 2 + (q - 1)/2\lambda\). Similarly, for \((q - 1)/\lambda\) even and \(c\) not a square, one has \(1 + (q - 1)/2\lambda\) orbits. This proves the part of the stated formula when \((q - 1)/\lambda\) is even. Now let us suppose that \(a\) is not a square in \(\mathbb{F}_q\). This is equivalent to \((q - 1)/\lambda\) odd, so in particular \(\lambda\) is even. In this case just half of the \(\lambda\) elements \(a^i c\) are squares, precisely the ones with \(i\) even if \(c\) is a square, or the ones with \(i\) odd, if \(c\) is not a square. Since \(\lambda\) is even, the elements \(\sigma^i\tau\) form two conjugation classes in \(\overline{G}\), according to the parity of \(i\). So we see that the \(\lambda\) elements \(x\) such that \(x^2 = a^i c\) form just one orbit in this case. Therefore one has a number of orbits equal to \(1 + (q - 1 - \lambda)/2\lambda + 1 = 3/2 + (q - 1)/2\lambda\) for \((q - 1)/\lambda\) odd.

From the preceding lemma the following result follows:

Theorem 4.4. The genus of the quotient curve \(Y/G''\), for \(m\) odd, is the following:

\[
g(Y/G'') = \frac{(m - 1)(q - 1 - \epsilon)}{4\lambda}, \tag{20}
\]

with

\[
\epsilon = \begin{cases} 
0 & \text{if } (q - 1)/\lambda \text{ is even} \\
2\lambda & \text{if } (q - 1)/\lambda \text{ is odd}
\end{cases}
\]

47
Proof. We apply the Riemann-Hurwitz formula to the covering \( \pi' : Y/G'' \to P^1/G \). As we observed before, for \( m \) odd this covering is a cyclic covering of order \( m \) with ramification only over \( P^1(F_q)/G \), and total ramification over this set. Therefore we see:

\[
2g(Y/G'') - 2 = -2m + (m - 1)|P^1(F_q)/G|.
\]

By applying the formulas (19) for \( |P^1(F_q)/G| \), one can find the stated formulas for \( g(Y/G'') \).

\( \square \)

(ii) \( m \) even. By (15), in this case \( \lambda \) is odd. We already know that \( \pi' \) is ramified over \( P^1(F_q)/G \) with total ramification. However, in the present case, there might be also other ramification points for \( \pi' \). The relations (15), for \( m = 2s \), are easily seen to be compatible if and only if \( a \) is a square in \( F_q \) and \( c \) is not a square, i.e \( c^{(q-1)/2} = -1 \). In this case one sees that \( b \) is uniquely determined, while \( \gamma \) is determined up to the sign. To get all the other possible ramification points for \( \pi' \), we have to look at points \( P' \in P^1 \setminus P^1(F_q) \). For any such point one has \( r_{P/P'} = 1 \). Since we want to impose \( r_{Q/Q'} > 1 \) and \( P' \) is not a ramification point for \( \pi \), by 18 we have to impose that \( r_{P'/Q'} > 1 \), and therefore the inertia group of \( P' \) in \( G \) must necessarily be generated by an element of the form \( \sigma^\tau \), which means \( r_{P'/Q'} = 2 \). So, by (18), we have \( r_{P/Q}r_{Q/Q'} = 2 \), and finally we impose \( r_{P/Q} = 1 \) to get \( r_{Q/Q'} = 2 > 1 \). Points \( P' \in P^1 \) with these properties correspond to \( x \in F_q^* \) such that \( x^2 = \bar{a}^i \), for some \( i \), but \( \gamma \bar{b}^i/x^{(q+1)/m} = -1 \). These conditions ensure that \( \sigma^\tau(P') = P' \), but \( \bar{\sigma}^\tau(P) \neq P \). Since the order of \( \bar{\sigma} \) is odd, and hence \( \bar{\sigma} = \bar{\sigma}^{2k} \), for suitable \( k \), one can prove that the set of the \( x \) as above, is in bijection with the set of the \( z \) such that \( z^2 = c \) and \( \gamma/z^{(q+1)/m} = -1 \), by setting \( z = \bar{\sigma}^{-ik}(x) \). Now let us consider the two square roots \( \pm z \) of \( c \). If \( (q + 1)/m \) is even, then none or both of \( \pm z \) satisfy the above requirements, according to the choice of the sign of \( \gamma \). Moreover, one can check that \( z \) and \( -z \) are not in the same orbit of \( G \), which is consequence of the fact that \( \lambda \) is odd. So, if \( (q + 1)/m \) is even, we find 2 or 0 points in \( Q' \in P^1/G \), outside \( P^1(F_q)/G \), over which \( \pi' \) is ramified, with ramification orders equal to 2. In particular there are exactly \( m/2 \) points \( Q \in Y/G'' \) over each such \( Q' \).

On the other hand, if \( (q + 1)/m \) is odd, for any possible choice of \( \gamma \), just one among \( \pm z \) gives an extra ramification. In conclusion we have:

Lemma 4.2. For \( m \) even the ramification divisor \( R \) of \( \pi' \) has degree:

\[
\deg(R) = (m - 1)(q - 1)/2\lambda + (m - 1) + \delta \cdot m/2
\]

with \( \delta = 0 \) or \( \delta = 2 \) if \( (q + 1)/m \) is even, and \( \delta = 1 \) if \( (q + 1)/m \) is odd.
Proof. From the discussion above it follows:
\[ \deg(R) = (m - 1)|P^1(\mathbb{F}_q)/\overline{G}| + \delta \cdot m/2. \]
But, in our case, no non-trivial element in \( \overline{G} \) fixes any point in \( \mathbb{F}_q^* = P^1 \setminus \{0, \infty\} \). So we have:
\[ |P^1(\mathbb{F}_q)/\overline{G}| = 1 + \frac{q - 1}{2\lambda}, \]
and the result follows immediately.

A straightforward application of the Riemann-Hurwitz formula to the covering \( \pi' : Y/G'' \rightarrow P^1/\overline{G} \) gives us the following result.

**Theorem 4.5.** If \( m \) is even, the genus of \( Y/G'' \) is:
\[ g(Y/G'') = \frac{1}{2} \left( \frac{(m - 1)(q + 1)}{2\lambda} + 1 \right) - f, \]
with \( f = m/2 \) or \( f = 0 \) if \( (q + 1)/m \) is even, and \( f = m/4 \) if \( (q + 1)/m \) is odd.

### 4.4 Groups of type III

We consider now subgroups \( G \subseteq (\mu_{q+1})^2 \rtimes S_3 \). Therefore \( G \) sits in an exact sequence
\[ (1) \rightarrow G' \rightarrow G \rightarrow \overline{G} \rightarrow (1), \]
with \( G' = G \cap (\mu_{q+1})^2 \) and \( \overline{G} \) the image of \( G \) in \( S_3 \). We will consider the Fermat curve \( F \)
with equation 6, and compute the genera of the quotients \( F/G \). To do this, we will adopt
the following strategy: we will compute first the possible genera of the curves \( F/G' \), with \( G' \) any possible subgroup of \( (\mu_{q+1})^2 \), and after this we will find out which curves of the
type \( X \cong F/G' \) admit some automorphism group isomorphic to a subgroup \( \overline{G} \) of \( S_3 \).
Next, we study the extra quotients \( X/\overline{G} \) and add their genera to the set of genera already
obtained.

In proposition 3.5 of Ch. 3 we saw that a curve \( X \) is a Galois covering \( P^1 \) ramified
over three points with abelian Galois group of exponent \( m \) if and only if it is a quotient
of the Fermat curve
\[ F_m : X^m + Y^m + Z^m = 0, \]
by a subgroup of \( (\mu_m)^2 \). If \( m|q+1 \) then \( X \) is also a quotient of the Fermat curve of degree
\( q + 1 \) given by (6). In order to find the possible genera of the quotients of (6) by a group
\( G' \subseteq (\mu_{q+1})^2 \), we can therefore restrict to the abelian coverings of \( P^1 \) ramified over three
points, with Galois group of exponent \( m|q + 1 \).
4.5 Abelian coverings of $\mathbb{P}^1$ ramified over three points

In this section we give a formula for the genera of the abelian coverings of $\mathbb{P}^1$ ramified over three points. Although we will be interested mainly in the case when the exponent of the Galois group of such coverings divides $q + 1$, in this section we will deal with arbitrary exponent of the Galois group not divisible by the characteristic of the base field.

**Notations**
- $[a, b] = \gcd(a, b)$, the greatest common divisor of the integers $a$ and $b$.
- $(a, b) = \text{lcm}(a, b)$ the least common multiple of $a, b$.
- $k$ an algebraically closed field of char$(k) \not| \#(A)$.
- $\pi : X \to \mathbb{P}^1$ an abelian covering ramified over $0, 1, \infty$, defined over $k$.
- $A$ the Galois group of $\pi$.
- $m$ the exponent of $A$.
- For any $i \in \{0, 1, \infty\} \subset \mathbb{P}^1$ and for $x \in X$ such that $\pi(x) = i$, we set
  \[ A_i = \{ \sigma \in A : \sigma(x) = x \}. \]
  This is a cyclic group and a generator of $A_i$ will be often denoted by $\sigma_i$.
- $e_i = \#(A_i); h = \#(A_0 \cap A_1); h' = \#(A_0 \cap A_1 \cap A_\infty); d = h/h'$.

The main result of the section is the following theorem.
Theorem 4.6. The following facts hold:

1. The genus $g(X)$ of $X$ is given by:

$$g(X) = 1 + \frac{e_0e_1 - e_0 - e_1 - [e_0, e_1]d}{2h}.$$ 

2. An abelian covering $X \rightarrow \mathbb{P}^1$ as above exists if and only if the following conditions are satisfied:

- $(e_0, e_1) = m$;
- $h|\langle e_0, e_1 \rangle$, $d|h$;
- $d$ is prime to $e_0 e_1 / [e_0, e_1]^2$ and it is even if $h$ is even and $e_0 e_1 / [e_0, e_1]^2$ is odd.

To prove this theorem, we will make extensive use of the Riemann Existence Theorem 3.7, which is allowed since the characteristic of $k$ does not divide $\#(A)$. Let $\sigma_i$ be a generator of $A_i$, for $i = 0, 1, \infty$. By theorem 3.7 we can assume that $\sigma_\infty = \sigma_0 + \sigma_1$, in the additive notation for $A$. We set $H = A_0 \cap A_1$, and $\tilde{\sigma}_i$ the image of $\sigma_i$ in $A/H$. Then $A/H$ is the direct sum $(\tilde{\sigma}_0) \oplus (\tilde{\sigma}_1)$, and the image of $A_\infty$ in $A/H$ is generated by $(\tilde{\sigma}_0, \tilde{\sigma}_1)$, so it has order $\langle e_0/h, e_1/h \rangle = \langle e_0, e_1 \rangle / h$. On the other hand this image has order $\#(A_\infty) / \#(A_\infty \cap A_1) = e_\infty / h'$, hence we find the formula

$$e_\infty = (e_0, e_1) h' / h = (e_0, e_1) / d.$$  \hspace{1cm} (23)

We observe that $A$ is isomorphic to the quotient $(A_0 \oplus A_1)/H$, hence

$$\#(A) = (e_0 e_1) / h.$$  \hspace{1cm} (24)

Within this setup we can prove the statement 1. in theorem 4.6.

Proof of statement 1). The fibre over $i \in \{0, 1, \infty\}$ contains $\#(A) / \#(A_i)$ points, each appearing in the ramification divisor with multiplicity $\#(A_i) - 1$, since $\text{char}(k) \not| \#(A)$. Hence the Riemann-Hurwitz formula for the covering $\pi$ gives:

$$2g(X) - 2 = (e_0 e_1 / h)(-2 + e_0 + e_1 + e_\infty - 1/e_0 - 1/e_1 - 1/e_\infty).$$

Statement (1) of the theorem follows easily after substitution of the expression (23) for $e_\infty$ into the equation above. \hfill \square
For the proof of statement (2) we observe that, by theorem 3.7, all the coverings $X$ are determined uniquely up to isomorphisms by the choice of generators $\sigma_0$ and $\sigma_1$ for $A_0$ and $A_1$ respectively. A generator for $A_\infty$ is indeed immediately given by $\sigma_0 + \sigma_1$. If we write $A = (A_0 \oplus A_1)/H$, we will produce all $X$, with $\text{Gal}(X/P^1) = A$ and fixed ramification degrees $e_0$ and $e_1$ over $0,1 \in P^1$, by letting $H$ vary among the subgroups of $A_0 \oplus A_1$ isomorphic to the intersection $A_0 \cap A_1 \subseteq A$. It is easy to see that $H$ can be generated by any element of the form $((e_0/t)\sigma_0, (e_1/t)\sigma_1)$, with $t$ prime to $h$. Moreover $A_\infty$ is the image in $(A_0 \oplus A_1)/H$ of the subgroup generated by $(\sigma_0, \sigma_1)$. Once one has fixed the parameters $e_0, e_1, h$ and $t$, one gets the following.

**Lemma 4.3.** We denote $\alpha = e_0/[e_0, e_1]$ and $\beta = e_1/[e_0, e_1]$. Then the integer $d$ in theorem 4.6 is given by:

$$d = [h, \alpha - t\beta].$$

**Proof.** Looking at the expression $e_\infty = (e_0, e_1)/d$ one observes that $d$ is equal to the order of the intersection in $A_0 \oplus A_1$ of $H$ and the subgroup $\langle (\sigma_0, \sigma_1) \rangle$, generated by $(\sigma_0, \sigma_1)$. Indeed it is the order of the kernel of the surjection $\langle (\sigma_0, \sigma_1) \rangle \to A_\infty$, induced by the projection $A_0 \oplus A_1 \to A$. This means also that $d$ is the order of the kernel of the map $\phi : H \to (A_0 \oplus A_1)/(\langle (\sigma_0, \sigma_1) \rangle)$ defined as the restriction to $H$ of the projection $A_0 \oplus A_1 \to (A_0 \oplus A_1)/(\langle (\sigma_0, \sigma_1) \rangle)$. The group $(A_0 \oplus A_1)/(\langle (\sigma_0, \sigma_1) \rangle)$ is isomorphic to $\mathbb{Z}/[e_0, e_1]\mathbb{Z}$ and the projection onto it can be defined by $\sigma_0 \mapsto 1, \sigma_1 \mapsto -1$. Therefore $\phi(H)$ is the subgroup of $\mathbb{Z}/[e_0, e_1]\mathbb{Z}$ generated by $e_0/h - e_1 t/h$, one has $\#(\phi(H)) = r/[r, s]$. Since $d = h/\#(\phi(H))$, we find $d = h[r, s]/r = [rh, sh]/r = [h, sh/r] = [h, a - tb]$. □

It is useful to observe that the integer $t$ can indeed be taken prime to $e_0$. We can do so because only the congruence class of $t$ mod $h$ matters and one knows that the canonical map $(\mathbb{Z}/e_0\mathbb{Z})^* \to (\mathbb{Z}/h\mathbb{Z})^*$ is surjective. Furthermore, setting as above $\alpha = e_0/[e_0, e_1]$ and $\beta = e_1/[e_0, e_1]$, we observe that the set

$$\{[h, \alpha - t\beta] : t \text{ prime to } e_0\}$$

is equal to the set

$$\{[h, x\alpha + y\beta] : x \text{ prime to } e_1 \text{ and } y \text{ prime to } e_0\}.$$ 

Since $h[e_0, e_1]$, this latter is also equal to the set of numbers of the form $[h, D]$, with $D = [e_0, e_1, x\alpha + y\beta]$, with $x$ prime to $e_1$ and $y$ prime to $e_0$.
Proof of statement (2) in theorem 4.6. We start with the necessity of the given numerical conditions. Under the notations introduced above, the exponent $m$ of the Galois group $A = \text{Gal}(X/P^1)$ is clearly $(e_0, e_1)$, and $h$ is a divisor of $[e_0, e_1]$, since it is the order of $A_0 \cap A_1 \subseteq A$. Moreover by the formula in lemma 4.3, the fact that $t$ can be chosen prime to $e_0$ and the fact that $e_0/[e_0, e_1]$ is prime to $e_1/[e_0, e_1]$, it follows that $d$ is prime to both $e_0/[e_0, e_1]$ and $e_1/[e_0, e_1]$. Finally if $h$ is even then $t$ is odd and if $e_0$ and $e_1$ have the same 2-adic valuation it follows that $e_0/[e_0, e_1] - e_1 t/[e_0, e_1]$ is even. Hence $d$ is even. This proves the necessity of the conditions on the parameters $e_0, e_1, h, d$.

Now the sufficiency. By the discussion before lemma 4.3 we know that a Galois covering $X$ of $P^1$ ramified over $\{0, 1, \infty\}$, with abelian Galois group $A$ of exponent $m$ and prescribed ramification groups $A_0, A_1$ and $A_\infty$ is determined up to isomorphisms by a choice of generators $\sigma_0, \sigma_1$ of $A$ such that $\sigma_i$ generates $A_i$ for $i = 0, 1$. The orders $e_0 = \#(A_0)$ and $e_1 = \#(A_1)$ can be arbitrary positive integers such that $(e_0, e_1) = m$, and $A$ is isomorphic to $\mathbb{Z}/e_0 \mathbb{Z} \oplus \mathbb{Z}/e_1 \mathbb{Z}/H$ with $H$ generated by an element of the form $(e_0/h, t e_1/h)$ with $h|[e_0, e_1]$ with arbitrary $t$ prime to $e_0$. The integer $d = \#(A_0 \cap A_1)/\#(A_0 \cap A_1 \cap A_\infty)$ is determined from $t$ by formula (25). When $t$ varies we have already observed that $d$ can assume any value of the form $[h, D]$ where $D = [e_0, e_1], e_0/[e_0, e_1] + ye_1/[e_0, e_1]$, for $x$ and $y$ varying in the units modulo $e_1$ and $e_0$ respectively. The conclusion is then an immediate consequence of the next lemma. 

\textbf{Lemma 4.4.} Let $a, b$ be positive integers. We set $\alpha = a/[a, b]$ and $\beta = b/[a, b]$. Let $D$ be a divisor of $[a, b]$ such that

1. $D$ is prime to $\alpha$ and $\beta$;
2. if $a$ and $b$ are even and they have the same 2-adic valuation, then $D$ is even.

Then $D = [[a, b], x\beta + y\alpha]$ for some $x, y$ such that $[x, a] = 1, [y, b] = 1$.

\textbf{Proof.} We start choosing $x'$ and $y'$ such that $x'\beta + y'\alpha = 1$. If we pose $x = D x' - v\alpha$ and $y = D y' + v\beta$ for an arbitrary $v$, then

$$D = x\beta + y\alpha = [[a, b], x\beta + y\alpha].$$

Our goal is now to find $v$ such that simultaneously $x$ is prime to $a$ and $y$ is prime to $b$. What we can certainly find is $v_1$ such that

$$x_1 = D x' - v_1 \alpha$$

is prime to $a$, because $D x'$ is invertible in $\mathbb{Z}/a \mathbb{Z}$, and $v_2$ such that

$$y_2 = D y' + v_2 \beta$$

53
is prime to \( b \), for a similar reason. We put

\[ y_1 = Dy' + v_1 \beta \]

and

\[ x_2 = Dx' - v_2 \alpha. \]

Then we look for a couple of integer numbers \((\lambda, \mu)\) such that

- \( x = \lambda x_1 + \mu x_2 \) is prime to \( a \),
- \( y = \lambda y_1 + \mu y_2 \) is prime to \( b \),
- \( \lambda + \mu \) is prime to \([a, b]\).

This last condition ensures that \( D = [[a, b], x \beta + y \alpha] \).

Let \( p \) be a prime dividing \( a \) or \( b \). Let us consider the points \( A_p, B_p, C_p \in \mathbb{P}^1_{F_p} \) whose homogeneous coordinates \((u : v)\) satisfy the equations:

\[
\begin{align*}
A_p : & \quad ux_1 + vx_2 = 0, \\
B_p : & \quad uy_1 + vy_2 = 0, \\
C_p : & \quad u + v = 0,
\end{align*}
\]

respectively. Then the Chinese remainder theorem assures us that there is a couple \((\lambda, \mu)\) satisfying our requests if and only if, for any \( p|ab \), there exists \( R_p \in \mathbb{P}^1_{F_p} \) satisfying the inequalities:

\[
\begin{align*}
R_p & \neq A_p, C_p, & \text{if } p|a \text{ and } p \nmid b, & \quad (26) \\
R_p & \neq A_p, B_p, C_p, & \text{if } p|[a, b], & \quad (27) \\
R_p & \neq B_p, C_p, & \text{if } p|b \text{ and } p \nmid a. & \quad (28)
\end{align*}
\]

There always exists \( R_p \) satisfying (26), (28) and also (27) if \( p \geq 3 \), since \( |\mathbb{P}^1_{F_p}| = p + 1 \). So we are left with condition (27) for \( p = 2 \). If \( 2|[a, b] \) but \( 2 \nmid ab/[a, b]^2 \) then \( D \) is even by hypothesis. Since \([X_1, a] = 1\) then \( X_1 = Dx' - v_1 \alpha/[a, b] \) is odd. It follows that \( v_1 \) is odd too. Then also \( Y_1 = Dy' + v_1 b/[a, b] \) is odd. So in the case under consideration, we can see immediately that the point \( R_2 = (1:0) \) satisfies condition (27).

Another case is \( 2|a/[a, b] \), \( 2|[a, b] \), but \( 2 \nmid b/[a, b] \). Here \( D \) is necessarily odd and \( x' \) is also odd. Therefore \( X_2 = Dx' - v_2 a/[a, b] \) is odd and the same also holds for \( Y_2 \) by construction. Then we can choose \( R_p = (0:1) \) as a point satisfying (27). The case \( 2|b/[a, b] \), \( 2|[a, b] \), but \( 2 \nmid a/[a, b] \) is treated similarly.
4.6 Abelian coverings of $\mathbb{P}^1$ ramified over $0, 1, \infty$ with extra automorphisms.

Let $p : X \to \mathbb{P}^1$ be a Galois covering ramified over $0, 1, \infty$, with abelian Galois group $A$ and ramification groups $A_0, A_1, A_\infty$. We are interested to know under which conditions the curve $X$ has other automorphisms than the ones already in $A$. This will enable us to get more quotients of Fermat curves. We will restrict to the following situation. We will assume that there exists a subgroup $P \subset \text{Aut}(X)$ whose elements map fibres of $p$ into fibres of $p$. This fact implies that the action of $P$ on $X$ descends to an action on $\mathbb{P}^1$ via $p$.

It is easy to prove that such a group $P$ normalizes $A$ in $\text{Aut}(X)$. Let us call $\bar{P}$ the groups of automorphisms of $\mathbb{P}^1$ induced by $P$. It permutes $0, 1, \infty$, and its action on $\mathbb{P}^1$ is of course uniquely determined by this permutation action. We have a commutative diagram of Galois coverings:

$$
\begin{array}{ccc}
X & \longrightarrow & X/P \\
p \downarrow & & \downarrow \phi \\
\mathbb{P}^1 & \longrightarrow & \mathbb{P}^1/\bar{P}.
\end{array}
$$

(29)

We denote by $\pi : X \to \mathbb{P}^1$ the composition $\pi = q \cdot p$. One sees that $\pi$ is a Galois covering with Galois group $G$ isomorphic to a semidirect product $A \rtimes \bar{P}$. For any $\tau \in P$, the conjugation map $g \mapsto \tau g \tau^{-1}$ in $\text{Aut}(X)$ induces isomorphisms among the ramification groups $A_i$, compatibly with the induced permutation $\bar{\tau}$ of $\{0, 1, \infty\}$. Finally, we can assume that $P \cong \bar{P}$, which in turn is isomorphic to a subgroup of $S_3$. We can do so without loss of generality, because it is not difficult to prove that one can always reduce oneself to such case, after substituting $X$ with a suitable quotient $X' = X/B$ with $B = A \cap P$.

We will classify the curves $X$ admitting a group $P$ of extra isomorphisms as discussed above, starting with the characteristic zero case. Since all the curves and the automorphism we will consider will be defined over cyclotomic fields, we will obtain interesting new curves by reducing the quotients $X/P$ modulo a prime. This will be done in section 4.7.

Up to changes of coordinates in $\mathbb{P}^1$, the possibilities for $P$ are the following.

**Case 4.1.** $P$ is generated by an order two automorphism $\tau$ which descends to the involution $\bar{\tau}$ of $\mathbb{P}^1$ which interchanges $0$ and $1$, and fixes $\infty$.

It follows that $A_0$ and $A_1$ are conjugated by $\tau$, so $e_0 = e_1 = m$. For the results and under the notations of the preceding section, $A \cong (\mathbb{Z}/m\mathbb{Z})^2/H$, with $H \cong A_0 \cap A_1$ and $H$ generated by an element of the form $(m/h, mt/h)$. The fixed points of $\bar{\tau}$ in $\mathbb{P}^1$ are $\infty$.
and 1/2. It follows that \( \pi : X \to \mathbb{P}^1 \) is ramified over the three points \( P = q(0) = q(1), Q = q(\infty) \) and \( R = q(1/2) \). Hence the degenerate fibres of \( \pi \) are \( \pi^{-1}(P) = p^{-1}(0) \cup p^{-1}(1), \pi^{-1}(Q) = p^{-1}(\infty), \) and \( \pi^{-1}(R) = p^{-1}(1/2) \). We can find ramification points of the covering \( X \to X/P \) only in the last two fibres.

**Case 4.2.** \( P \) is generated by an order three automorphism \( \tau \) such that \( \bar{\tau} \) acts on \( \{0, 1, \infty\} \) as the 3-cycle \( (0, 1, \infty) \).

We find \( e_0 = e_1 = e_\infty = m \) and \( A \cong (\mathbb{Z}/m\mathbb{Z})^2/H \), similarly as in the previous example. The two fixed points of \( \bar{\tau} \) are the \( -\eta \) and \( -\eta^2 \), with \( \eta \) a primitive third root of 1. The degenerate fibres of \( \pi \) are respectively \( p^{-1}(0) \cup p^{-1}(1) \cup p^{-1}(\infty), \ p^{-1}(-\eta) \) and \( p^{-1}(-\eta^2) \). We can find ramification points for \( X \to X/P \) only in the last two ones.

**Case 4.3.** \( P \) descends to the permutation group \( S_3 \) of \( \{0, 1, \infty\} \subset \mathbb{P}^1 \).

As before \( e_0 = e_1 = e_\infty = m \). There are no points in \( \mathbb{P}^1 \) fixed by every element of \( \bar{P} \), so the ramification points for \( \mathbb{P}^1 \to \mathbb{P}^1/\bar{P} \) are all the points of the form \( \tau(S) \), for any \( \tau \in \bar{P} \) and \( S \in \mathbb{P}^1 \) one of the points fixed by the transposition \((0, 1)\) or the 3-cycle \((0, 1, \infty)\), known from the previous examples.

We will now study separately the necessary and sufficient conditions for the existence of a Galois covering \( p : X \to \mathbb{P}^1 \) with abelian Galois group \( A \cong (\mathbb{Z}/m\mathbb{Z})^2/H \), with \( H \) generated by an element of the form \((m/h, tm/h)\), such that \( X \) admits a group \( P \) of extra automorphisms as in cases 4.1, 4.2 and 4.3. Moreover we will compute the genera of the quotient curves \( X/P \).

**Action of \( P \) cyclic of order 2**

We study the curves \( X \) with \( P \) as in Case 4.1. The following characterization holds.

**Theorem 4.7.** Let us assume that \( \text{char}(k) = 0 \). Then there exists a Galois covering \( p : X \to \mathbb{P}^1 \) with abelian Galois group \( A \cong (\mathbb{Z}/m\mathbb{Z})^2/H \) such that \( X \) admits a group \( P \) of extra automorphisms as in Case 4.1 if and only if \( H = \langle (m/h, tm/h) \rangle \), with \( t^2 \equiv 1 \pmod{h} \).

**Proof.** We start with the necessity of the condition. From the discussion of Case (4.1) it is clear that we can find generators \( \alpha \) for \( A_0 \) and \( \beta \) for \( A_1 \) such that \( \beta = \tau \alpha \tau^{-1} \). The stabilizer \( G_x \) of a point \( x \in \pi^{-1}(P) \) is \( A_0 \) or \( A_1 \). The stabilizer \( G_x \) of a point \( x \in \pi^{-1}(Q) \) is cyclic of order \( 2e_\infty \) and so the subgroup of the squares of elements in \( G_x \) is \( A_\infty \). Finally
the stabilizer of a point \( x \) over \( R \) is generated by an element of order two, which we may assume to be a conjugate of \( \tau \). By theorem 3.7 we know that there are three elements \( \sigma_i \in G, i = 1, 2, 3 \), generating ramification groups over the points \( P, Q, R \) respectively, such that \( \sigma_1\sigma_2\sigma_3 = 1 \). Up to conjugation we may assume that \( \sigma_1 = \alpha, \sigma_2 = \alpha^{-1}\tau, \) and \( \sigma_3 = \tau \). A generator of \( A_{\infty} \) is then the square of \( \sigma_2 = \alpha^{-1}\tau \), that is \( \alpha^{-1}\beta^{-1} \). If we identify \( A \) with the quotient of \((\mathbb{Z}/m\mathbb{Z})^2/H\) given by \((0, 1) \mapsto \alpha, (1, 0) \mapsto \beta \), we see that the element \((1, 1) \in (\mathbb{Z}/m\mathbb{Z})^2 \) goes over a generator of \( A_{\infty} \). The conjugation by \( \tau \) lifts to the automorphism of \((\mathbb{Z}/m\mathbb{Z})^2 \) given by \( f(u, v) = (v, u) \). The kernel \( H = \langle (m/h, mt/h) \rangle \) must be invariant by \( f \) and this immediately implies \( t^2 \equiv 1 \pmod{h} \).

Now we sketch a proof of the sufficiency. We take \( X = F_m/H \), a quotient of the Fermat curve of degree \( m \) given by equation (22), and \( H \subseteq (\mathbb{Z}/m\mathbb{Z})^2 \) as in the statement. \( H \) is invariant by conjugation with respect to a subgroup \( P \subseteq S_3 \) of order 2 in the automorphism group \((\mathbb{Z}/m\mathbb{Z})^2 \rtimes S_3 \) of \( F_m \). Then one immediately sees that \( P \) descends to a group of automorphisms of \( X \) of order 2. \( \Box \)

Our next task is to compute the genus of \( X/P \). We need to know the fixed points for the action of \( P \). We call \( G \) the group of automorphisms of \( X \) given by the semidirect product of \( A \) and \( P \):

\[
G = A \rtimes P.
\]

The order two element \( \tau \) generating \( P \) has the general form \( \tau = \alpha^a\beta^b\tau_0 \), under the notations of the proof of theorem 4.7, with \( \tau_0 \) a fixed order two automorphism inducing the transposition of \( 0, 1 \in \mathbb{P}^1 \), and \( a, b \) determined in order to impose the condition of \( \tau \) having order two. Remembering that the conjugation by \( \tau_0 \) transposes \( \alpha \) and \( \beta \), we find that the condition \( \tau^2 = \text{id} \) is equivalent to \( \alpha^{a+b}\beta^{a+b} = 0 \in A = (\mathbb{Z}/m\mathbb{Z})^2/H \), that is: \( a + b = rm/h \) and \( a + b = rtm/h \). Equivalently:

\[
a + b = sm/[h, t - 1]. \tag{30}
\]

We know that the possible fixed points for \( \tau \) are in the fibres \( p^{-1}(\infty) \) and \( p^{-1}(1/2) \). From the proof of theorem 4.7, we can assume that there is a point in \( p^{-1}(\infty) \) fixed by \( \alpha^{-1}\tau_0 \), and a point in \( p^{-1}(1/2) \) fixed by \( \tau_0 \). Let \( x_0 \in p^{-1}(\infty) \cup p^{-1}(1/2) \) be one of these points. The points \( x \) such that \( p(x) = p(x_0) \) can be written \( x = gx_0 \), with \( g \in A \), and they are in one-to-one correspondence with the classes of \( g \) in \( A/A_{x_0} \). One observes that

\( x \) is fixed by \( \tau \) if and only if \( g^{-1}\tau g \in G_{x_0} \).

57
If \( x_0 \) lies over \( \infty \), we know that \( A_{x_0} = A_\infty = \langle \alpha \beta \rangle \), while if \( x_0 \) lies over 1/2, then \( A_{x_0} = (1) \). In any case \( A_{x_0} \) commutes with every element in \( G \). Writing \( g = \alpha^u \beta^v \), the condition above is equivalent to

\[
\alpha^{v-u+a} \beta^{u-v+b} \tau_0 \in G_{x_0}.
\]

By construction of \( \tau_0 \) and \( x_0 \), we see that \( \overline{G}_{x_0} = \langle \alpha \tau_0 \rangle \subset G/A_{x_0} \cong A/A_0 \cong \langle \tau_0 \rangle \), if \( x_0 \in p^{-1}(\infty) \), or \( \overline{G}_{x_0} = \langle \tau_0 \rangle \), if \( x_0 \in p^{-1}(1/2) \). So the following properties hold.

1) If \( x \in p^{-1}(\infty) \), then it is fixed by \( \tau \) if and only if \( \alpha^{v-u+a-1} \beta^{u-v+b} = 1 \) in \( A/A_\infty \).

2) If \( x \in p^{-1}(1/2) \), then it is fixed by \( \tau \) if and only if \( \alpha^{v-u+a} \beta^{u-v+b} = 1 \).

Moreover, the number of the fixed points \( x \) for \( \tau \), in cases 1) and 2) is given by the number of solutions of the equations above \( \alpha^u \beta^v \in A/A_\infty \) and \( \alpha^u \beta^v \in A \), respectively.

In case 1) we have \( A/A_\infty \cong (\mathbb{Z}/m\mathbb{Z})^2/H' \), with \( H' = H + \langle (1,1) \rangle \). Then one finds with easy calculations that \( (\mathbb{Z}/m\mathbb{Z})^2/H' \cong \mathbb{Z}/l\mathbb{Z} \), with \( l = m[h,t-1]/h \), and the quotient map \( A \to A/A_\infty \cong \mathbb{Z}/l\mathbb{Z} \) is represented by \( \alpha^u \beta^v \mapsto z-w \). So the condition in 1) is equivalent to \( 2(v-u)+a-b-1 \equiv 0 \pmod{l} \).

If \( l \) is odd, the equation above has a unique solution \( v-u \) modulo \( l \). That is, there is only one point \( x \) as in case 1) fixed by \( \tau \). We observe that \( l \) odd is equivalent to \( m \) odd: this follows from the observation that \( v_2(m) \geq v_2(h) \geq v_2([h,t-1]) \), and from the fact that \( [m,t] = 1 \).

If \( l \) is even, or equivalently \( m \) even, then the equation above has two solutions modulo \( l \) if \( a-b-1 \) is even and no solutions if \( a-b-1 \) is odd. We recall that \( a+b = sm/[h,t-1] \), hence if \( m/[h,t-1] \) is even, one has \( a-b-1 \) odd and hence no solutions. Else, if \( m/[h,t-1] \) is odd, one can have either no solutions or two solutions according whether the number \( s \) in (30) is even or not.

In case 2) the equation in \( (u,v) \) to solve is \( (v-u+a, u-v+b) \equiv 0 \pmod{H} \). This is equivalent to \( v-u+a \equiv rm/h \) and \( a+b \equiv r(t+1)m/h \pmod{m} \). We have solutions if and only if the second equation is satisfied for some \( r \).

If \( m \) is odd, then \( h \) is odd and since \( t^2 \equiv 1 \pmod{h} \), it follows that \( h = [h,t-1]/[h,t+1] \). Therefore \( a+b = sm/[h,t-1] = sm/h \equiv rm(t+1)/h \pmod{m} \) for a suitable \( r \). Moreover there are \( [h,t+1] \) classes of such \( r \)'s (mod \( h \)). Hence there are \( m/[h,t+1]/h \) classes of \( (u,v) \) modulo \( H \) satisfying the conditions of case 2. This means that there are \( m/[h,t+1]/h \in p^{-1}(1/2) \) when \( m \) is odd.

If \( m \) is even, we need to study the existence of integers \( r \) such that
$sm/[h, t - 1] \equiv rm(t + 1)/h \pmod{m}$. This is equivalent to

$sh/[h, t - 1] \equiv r(t + 1) \pmod{h}$, which is possible if and only if $[h, t + 1]$ divides $sh/[h, t - 1]$, that is, if $[h, t + 1][h, t - 1]$ divides $sh$. This is always the case if $h = [h, t - 1][h, t + 1]$, otherwise one observes that $[h, t - 1][h, t + 1] = 2h$ and therefore there exists a solution $r$ or not according whether $s$ is even or not. In the case when solutions do exist, the number of fixed points in $p^{-1}(1/2)$ is $m[h, t + 1]/h$, as in the case $m$ odd.

We will resume the results of the discussion above in the following proposition.

**Proposition 4.4.** Let $P = \langle r \rangle$ be as in Case 4.1 and let us denote $f_{m,h,t} = m[h, t + 1]/h$. Then the number $N$ of fixed points for $P$ is given by the following formulas:

- $N = 1 + f_{m,h,t}$ if $m$ is odd;
- $N = f_{m,h,t}$ if $m$ is even and $h = [h, t - 1][h, t + 1]$;
- $N = 0$ or $N = f_{m,h,t}$ if $m$ is even, $h \neq [h, t - 1][h, t + 1]$ and $v_2(m) \neq v_2([h, t - 1])$;
- $N = f_{m,h,t}$ or $N = 2$ if $m$ is even and $v_2(m) = v_2([h, t - 1])$.

**Proof.** The case $m$ odd is clear from the discussion above.

If $m$ is even and $h = [h, t - 1][h, t + 1]$, then $t$ is odd and hence $v_2(h) > v_2([h, t - 1])$, so, a fortiori, $v_2(m) > v_2([h, t - 1])$. From the discussion above it follows that there are no fixed points in $p^{-1}(\infty)$ and $m[h, t + 1]/h$ fixed points in $p^{-1}(1/2)$, whence the formula for $N$ in this case.

If $m$ is even, $h \neq [h, t - 1][h, t + 1]$ and $v_2(m) \neq v_2([h, t - 1])$, then $m/[h, t - 1]$ is even and therefore there are no fixed points in $p^{-1}(\infty)$. On the other hand, there are either $m[h, t + 1]/h$ fixed points in $p^{-1}(1/2)$ or no points, according whether $s$ is even or not.

If $m$ is even and $v_2(m) = v_2([h, t - 1])$, then $m/[h, t - 1]$ is odd. Therefore there are no fixed points in $p^{-1}(\infty)$, or two fixed points, according whether $s$ is even or odd, respectively. Since in the present case it also holds that $h \neq [h, t - 1][h, t + 1]$, we see that in $p^{-1}(1/2)$ there are $m[h, t + 1]/h$ fixed points, or no fixed points, if $s$ is even or odd, respectively. The formula for $N$ follows immediately.

Finally, it is clear that the cases above are the only possible ones.

We can now compute the genus of $X/P$, with $P$ as in Case 4.1.
Theorem 4.8. For \( X \) and \( P = \langle \tau \rangle \) of order two, as in Case 4.1, one has
\[
g(X/P) = g(X)/2 + 
\]
with \( \epsilon_{m,h,t} \) defined as follows. We set \( f_{m,h,t} = m[h,t + 1]/h \), as in theorem 4.4. Then:
\[
\epsilon_{m,h,t} = \begin{cases} 
1/4 - f_{m,h,t}/4 & \text{if } m \text{ is odd}, \\
1/2 - f_{m,h,t}/4 & \text{if } m \text{ is even and } h = [h,t - 1][h,t + 1], \\
1/2 \text{ or } 1/2 - f_{m,h,t}/4 & m \text{ is even, } h \neq [h,t - 1][h,t + 1] \\
0 \text{ or } 1/2 - f_{m,h,t}/4 & \text{if } m \text{ is even} \\
& \text{and } v_2(m) \neq v_2([h,t - 1]). 
\end{cases}
\]

Proof. One applies the Riemann-Hurwitz formula to the canonical projection \( X \to X/P \), getting \( 2g(X) = 2(2g(X)/P) - 2 + N \). It follows \( g(X/P) = g(X)/2 + (2-N)/4 \), then one uses the formulas for \( N \) from proposition 4.4. \( \square \)

Action of \( P \) cyclic of order 3

Now we will characterize the curves \( X \) with \( P \) as in Case 4.2.

Theorem 4.9. Let us assume that \( \text{char}(k) = 0 \). Then there exists a Galois covering \( p : X \to \mathbb{P}^1 \) with abelian Galois group \( A \cong (\mathbb{Z}/m\mathbb{Z})^2/H \) such that \( X \) admits a group \( P \) of extra automorphisms as in Case 4.2 if and only if \( H = \langle (m/h, mt/h) \rangle \), with \( t^2 - t + 1 \equiv 0 \pmod{h} \).

Proof. We prove only the necessity part of the statement. The sufficiency can be proved similarly as in theorem 4.7. From the discussion of Case (4.2) it follows that one can find generators \( \alpha, \beta, \gamma \) of \( A_0, A_1, A_\infty \), respectively, which are permuted cyclically by the conjugation by \( \tau \).

Taking \( \sigma_1, \sigma_2, \sigma_3 \in G \), with product equal to 1, as before, we may assume \( \sigma_1 = \alpha \), \( \sigma_2 = gr^2 \) and \( \sigma_3 = \tau \). So we find \( g = \alpha^{-1} \). Moreover \( \sigma_2 \) must have order three. This implies that \( 1 = \alpha^{-1}r^2\alpha^{-1}r^2\alpha^{-1}r^2 = \alpha^{-1}\gamma^{-1}b^{-1} \). This means that \( A_\infty \) is generated by \( \gamma = \alpha^{-1}b^{-1} \). We see then that \( A \cong (\mathbb{Z}/m\mathbb{Z})^2/H \) with \( H \) invariant by the automorphism of \( (\mathbb{Z}/m\mathbb{Z})^2 \) such that \( (0,1) \mapsto (0,1) \mapsto (-1,-1) \). From this it is easy to see that \( t^2 - t + 1 \equiv 1 \pmod{h} \). \( \square \)

We now proceed to compute the genus of \( X/P \). Again, we have to count the fixed points of the action of \( P \) on the curve \( X \). The group \( P \) is generated by \( \tau = g\tau_0 \), with \( \tau_0 \)
any fixed order three automorphism descending to the cycle \((0, 1, \infty)\), and \(g = \alpha^a \beta^b \in A\), with arbitrary \(a, b \in \mathbb{Z}\). Indeed it is easy to see that for any choice of \(a\) and \(b\), the automorphism \(\tau\) as above has order three.

We know that the fixed points of \(\tau\) can be found only in the fibres \(p^{-1}(\{-\eta\})\) and \(p^{-1}(\{-\eta^2\})\). From the proof of theorem 4.9, we can assume that there is a point \(x_0 \in p^{-1}(\{-\eta\})\) fixed by \(\alpha^{-1} \tau_0^2\), and therefore also by \((\alpha^{-1} \tau_0^2)^2 = \beta \tau_0\). Similarly, there exists a point \(y_0 \in p^{-1}(\{-\eta^2\})\) fixed by \(\tau_0\). We start with the study of the fixed points in \(p^{-1}(\{-\eta^2\})\). By computations similar to the ones done for theorem 4.8, this is the same as counting how many elements \(\theta \in A\) satisfy the relation \(\theta \tau \theta^{-1} = \theta g \tau_0 \theta^{-1} = \tau_0\). We write \(\theta = \alpha^2 \beta^a\). Remembering the effect of the conjugation by \(\tau\) from the proof of theorem 4.9, that is \(\tau \alpha \tau^{-1} = \beta, \tau \beta \tau^{-1} = \alpha^{-1} \beta^{-1}, \tau \alpha^{-1} \beta^{-1} \tau^{-1} = \alpha\), the relation above becomes the system

\[
x + y + a = rm/h \quad \text{and} \quad -x + 2y + b = rmt/h.
\]

Similarly the points in \(p^{-1}(\{-\eta\})\) having \(\tau\) in their ramification group are in bijective correspondence with the set of elements \(\theta \in A\) such that \(\theta g \tau_0 \theta^{-1} = \beta \tau_0\). In this case the system to solve is:

\[
x + y + a = rm/h \quad \text{and} \quad -x + 2y + b - 1 = rmt/h.
\]

Let us consider \(\Phi \in \text{End}((\mathbb{Z}/m\mathbb{Z})^2)\), defined by \(\Phi(x, y) = (x + y, -x + 2y)\), with \(\det \Phi = 3\) and \(\text{Im} \Phi\) generated by \((1, -1)\) and \((0, 3)\). The solutions of the homogeneous system \(x + y \equiv rm/h \mod m\) and \(-x + 2y \equiv rmt/h \mod m\), are given by the \((x, y) \in \Phi^{-1}(H)\). We observe that \(H \subset \text{Im} \Phi\). This can be seen by tensoring with \(\mathbb{Z}/p\mathbb{Z}\) for any prime \(p|m\): it is obvious if \(p \neq 3\) and if \(p = 3\) then \(H \otimes \mathbb{Z}/3\mathbb{Z} = \langle m/h(1, t) \rangle = \langle m/h(1, -1) \rangle \subset \text{Im} \Phi(p)\) since \(-1\) is the only solution of \(t^2 - t + 1 \equiv 0 \mod 3\). Therefore \(\Phi^{-1}(H)\) will have \(h\) elements if \(3 \nmid m\) and \(3h\) elements if \(3|m\). Furthermore it is easy to see that \(H \subset \Phi^{-1}(H)\) and therefore our solutions descend to one element in \(A\), or to three elements according whether \(3 \nmid m\) or \(3|m\), respectively. To establish the existence of solutions for the non homogeneous systems, we need only to look whether \((a, b)\) or \((a, b + 1)\) belong to \(\text{Im} \Phi\) or not. In the case \(3 \nmid m\) we know that \(\Phi\) is surjective and therefore the two systems are both solvable and have a unique solution \(\mod H\). In the case \(3|m\) we observe that since \((0, 1) \notin \text{Im} \Phi\) the only possible cases are the following: \((a, b) \in \text{Im} \Phi\) and \((a, b + 1) \notin \text{Im} \Phi\), or \((a, b) \notin \text{Im} \Phi\) and \((a, b + 1) \in \text{Im} \Phi\), or \((a, b) \notin \text{Im} \Phi\) and \((a, b + 1) \notin \text{Im} \Phi\).

In conclusion, there are two fixed points for \(P\) if \(3 \nmid m\), three fixed points or none, if \(3|m\).

We collect these results in the following.
Theorem 4.10. For $X$ and $P = \langle \tau \rangle$ cyclic of order three, as in Case 4.2, one has

$$g(X/P) = g(X)/3 + \varepsilon_m,$$

with

$$\varepsilon_m = \begin{cases} 
0 & \text{if } 3 \nmid m \\
2/3 \text{ or } -1/3 & \text{if } 3|m
\end{cases}$$

Proof. From the Riemann-Hurwitz formula for the quotient map $X \to X/P$, we get:

$$2g(X) - 2 = 3(2g(X/P) - 2) + 2N,$$

with $N$ the number of fixed points for $P$, computed above. The stated formula for $g(X/P)$ follows easily.

Action of $P$ isomorphic to $S_3$

Finally we deal with the case when $X$ admits a group of automorphisms $P$ as in Case 4.3.

Theorem 4.11. Let us assume that $\text{char}(k) = 0$. Then there exists a Galois covering $\pi : X \to \mathbb{P}^1$ with abelian Galois group $A \cong (\mathbb{Z}/m\mathbb{Z})^2/H$ such that $X$ admits a group $P$ of extra automorphisms as in Case 4.3 if and only if either $X$ is the Fermat curve of degree $m$, or $3|m$ and $H = \langle(m/3,2m/3)\rangle$.

Proof. Again, we give a proof of the necessity part of the characterization above. The sufficiency follows easily as in the proof of theorem 4.7.

In Case (4.3) the curve $X$ has automorphisms of both the types appearing in Cases 4.1 and 4.2. A consequence of the discussion of those cases is that $H$ is invariant with respect to the conjugations induced by the transposition $(0,1)$ and the cycle $(0,1,\infty)$. Therefore the class of $t \mod h$ satisfies both the conditions appearing in theorems 4.7 and 4.9. Hence $t \equiv 2$ and $t^2 \equiv 1 \pmod{h}$. So, either $h = 1$ or $h = 3$. In the first case $X$ is the Fermat curve of degree $m$, in the second one $H$ is the subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$ generated by the couple $(m/3,2m/3)$.

We conclude the study of quotients of the quotients of the Fermat curves in $\text{char}= 0$ with the computation of $g(X/P)$ for the case 4.3, i.e. for $P \cong S_3$.

Theorem 4.12. Suppose $X$ and $P \cong S_3$, as in theorem 4.11.

If $X$ is the Fermat curve (22), then

$$g(X/P) = (m^2 - 6m)/12 + \theta_m,$$
\[
\theta_m = \begin{cases} 
5/12 & \text{if } m \equiv 1,5 \pmod{6}, \\
2/3 & \text{if } m \equiv 2,4 \pmod{6}, \\
3/4 & \text{if } m \equiv 3 \pmod{6}, \\
1 & \text{if } m \equiv 0 \pmod{6}.
\end{cases}
\]

If \(h = 3, t = 2\), then

\[g(X/P) = (m^2 - 12m)/36 + \phi_m,\]

with

\[
\phi_m = \begin{cases} 
1 & \text{if } m \equiv 0 \pmod{2}, \\
3/4 & \text{if } m \equiv 1 \pmod{2}.
\end{cases}
\]

**Proof.** The curve \(X\) is covered by the Fermat curve \(F_m\) of equation (22). The group \(P\) is generated by an element \(\tau\) of order two, and an element \(\sigma\) of order three. From the proof of theorem 4.11, we know that \(\tau\) and \(\sigma\) lift to \(F_m\), hence may assume \(\tau = u\tau_0, \sigma = u\sigma_0\), with \(u, v \in A\) and \(\tau_0, \sigma_0\) induced by the Fermat curve automorphisms \(\tau_0(X : Y : Z) = (Y : X : Z)\) and \(\sigma_0(X : Y : Z) = (Z : X : Y)\). We need to find condition on \(u, v\) such that \(P \cong S_3\). One condition is that \(\tau\) has order 2: writing \(u = \alpha^x\beta^y\), this amounts to \(x + y = sm/[h, t - 1]\), as seen in the discussion before proposition 4.4. From theorem 4.11 we know that \(h = 1\) or \(h = 3\) and \(t = 2\), hence the condition above is simply \(x + y \equiv 0 \pmod{m}\). It follows that \(\tau\) is a conjugate of \(\tau_0\), precisely \(\tau = \alpha^x\tau_0\alpha^{-x}\). This means that up to conjugation we can assume that \(\tau = \tau_0\) and \(\sigma = \alpha^x\beta^d\sigma_0\). We can further conjugate by an element in \(A\) which commutes with \(\tau_0\), for example by \(\alpha^d\beta^d\). We get \(a^{-d}\beta^{-d}\sigma_0\alpha^d\beta^d = \alpha^{-d}\beta^{-d}\alpha^c\beta^d\beta^d\alpha^{-d}\beta^{-d}\sigma_0 = \alpha^c\beta^d\sigma_0\). So we assume \(\tau = \tau_0\) and \(\sigma = \alpha^x\sigma_0\). Another condition is that \(\tau\sigma\) must have order two. We have \(\tau\sigma = \beta^a\tau_0\sigma_0 = \beta^a\tau_1\), where \(\tau_1\) descends from the Fermat curve automorphism \((X : Y : Z) \mapsto (X : Z : Y)\). One finds that \((\tau\sigma)^2 = (\beta^a\tau_1)^2 = \beta^a\alpha^{-a}\beta^{-a} = \alpha^{-a}\), so \(\tau\sigma\) has order two if and only if \(a \equiv 0 \pmod{m}\). Hence \(P\) is a conjugate of \(\langle \tau_0, \sigma_0 \rangle\). So we can reduce ourselves to \(P = \langle \tau_0, \sigma_0 \rangle\). To complete the proof, we will examine separately the two cases coming from theorem 4.11.

The first possibility is that \(X\) is the Fermat curve \(F_m\). The number of fixed points for \(\tau_0\) is \(m + 1\) if \(m\) odd, and \(m\) if \(m\) is even. Precisely, they are the points \(\{(1 : -1 : 0)\} \cup \{(x : x : 1) : 2x^m + 1 = 0\}\), when \(m\) is odd, and \(\{(x : x : 1) : 2x^m + 1 = 0\}\), when \(m\) is even.

The fixed points for \(\sigma_0\) are the two points \((1 : \rho : \rho^2)\), where \(\rho\) is a primitive 3rd root of 1 if \(m\) is not divisible by 3, and there are no fixed points if \(m\) is divisible by 3. We see that there are no points in \(X\) fixed by the whole \(P\). So the points fixed by any two distinct
traspositions in $P$ form two disjoint sets, and the total number of points fixed by order two elements in $P$ is $3(m + 1)$ if $m$ odd, and $3m$ if $m$ even.

By applying the Riemann-Hurwitz formula to $X \to X/P$, and taking into account that $2g(X) - 2 = m^2 - 3m$, we obtain $m^2 - 3m = 6(2g(X/P) - 2) + N + 2M$. Here $N = 3(m + 1)$ if $m$ odd, $N = 3m$ if $m$ even, and $M = 2$ if $3 \nmid m$, $M = 0$ if $3|m$. The stated formula $g(X/P) = (m^2 - 6m)/12 + \theta(m)$ follows easily.

The other possibility given by theorem 4.11 is $h = 3$ and $t = 2$, hence $X = C/H$, with $H = \langle (\eta, \eta^2) \rangle \subset \langle \mu_m \rangle^2$, with $\eta$ a primitive third root of the unity. From proposition 4.4 we know that $\tau_0$ has $m + 1$ fixed points if $m$ is odd, and $m$ fixed point if $m$ is even. A point is $(X : Y : Z)$ is fixed under $\sigma_0$ if and only if there exist $i \in \mathbb{Z}$ and $\lambda \in k^*$ such that $(\eta^iZ : \eta^{2i}X : Y) = \lambda(X : Y : Z)$, that is, taking $Z = 1$, $\eta^i = \lambda X = \lambda^2 \eta^i Y = \lambda^3 \eta^i$. Thus $\lambda^3 = 1$,

$$(X : Y : 1) = (\lambda^2 : \lambda : 1) \not\in C,$$ because $3|m$. So we have no fixed points for $\sigma_0$ in $X$. So the fixed points for the action of $P$ come only from the order two elements, and the total number is $3m$, if $2|m$, and $3(m + 1)$, if $2 \nmid m$. From theorem 4.6, one finds $2g(X) - 2 = m(m - 3)/3$. So the Riemann-Hurwitz formula for $X \to X/P$ gives $m(m - 3)/3 = 6(2g(X/P) - 2) + 3m$ if $2|m$ or $m(m - 3)/3 = 6(2g(X/P) - 2) + 3(m + 1)$ if $2 \nmid m$. The stated formula for $g(X/P)$ follows immediately.

4.7 Reduction to characteristic $p$

Finally, we study the reduction of the curves $X/P$ over a prime $p \neq 2$. The formula for $g(X/P)$ given in theorem 4.8 still hold, because in that case $P$ has order 2, hence it is not divisible by $p$. For the same reason, the formulas in theorems 4.10 and 4.12 still hold if $p \neq 3$. So let us suppose $p = 3$, hence $m \not\equiv 0 \pmod{3}$.

We recall that $X$ is a curve admitting a Galois covering $X \to \mathbf{P}^1$ with Galois abelian group $A$ of exponent $m$ not divisible by $p = \text{char}(k)$. As discussed at the beginning of section 4.4, there exists a covering map $F_m \to X$, with $F_m$ the Fermat curve of degree $m$.

This map is obtained by identifying $X \cong F_m/H$ with $H$ a subgroup of the automorphism group $(\mu_m)^2 = (\mu_m)^3/\mu_m$, which acts on $F_m$ as described in section 4.1. The covering map $F_m \to \mathbf{P}^1$ defined by $(X : Y : Z) \mapsto (X^m : Y^m : Z^m)$ identifies the projective line $X + Y + Z = 0$ with the quotient curve $F_m/(\mu_m)^2$, so this covering map factorizes as the composition of Galois coverings $F_m \to X, X \to \mathbf{P}^1$.

If $P$ is a group of isomorphisms as described in Case 4.2, then a generator $\sigma$ is always of the form $g\sigma_0$ with $g \in A$ in the Galois group of $X$ over $\mathbf{P}^1$, and $\sigma_0$ induced by the
automorphism $(X : Y : Z) \mapsto (Z : X : Y)$. Therefore $\sigma$ induces on $X + Y + Z = 0$ exactly the automorphism 

$$\bar{\sigma} : (X : Y : Z) \mapsto (Z : X : Y).$$

Now let $x \in X$ be a ramification point for $\sigma$. Let $y$ be its image in $\mathbb{P}^1$. We already know that $x$ is not a ramification point for $X \rightarrow \mathbb{P}^1$, hence it is easy to see that the contribution of $x$ to the ramification divisor's degree of the covering $X \rightarrow X/(\sigma)$ is the same as the contribution of $y$ with respect to the covering $\mathbb{P}^1 \rightarrow \mathbb{P}^1/(\sigma)$. So it is sufficient to calculate the latter, and multiply the result by the number of $x$'s lying over $y$, which is independent of the characteristic. We have $y = (1 : 1 : 1)$ and a parametrization of a neighborhood of $y$ is $(X : Y : Z) = (1 - \lambda : 1 + \lambda : 1)$. One sees that the rational function $f = \lambda^3/(1 - \lambda)(1 + \lambda)$ is invariant under the action of $\bar{\sigma}$, which is indeed described by $\lambda \mapsto \lambda/(1 + \lambda)$. Moreover the order of this function at $\lambda = 0$ is exactly three, so to compute the order of the ramification divisor at $y$, we can take the order at $\lambda = 0$ of the differential $df$. With a straightforward calculation one sees this order is 4. So the degree of the ramification divisor in characteristic three is the same as in characteristic 0.

Now let $P$ be as in Case 4.3. By theorem, $X$ is the Fermat curve of degree $m$, since $3 \nmid m$, so the case $h = 3$ cannot appear here. The point $x = (1 : 1 : 1)$ is the only total ramification point for $X \rightarrow \mathbb{P}^1$. As before, the order of the ramification divisor at $x$ is the same as for the point $y = (1 : 1 : 1) \in \mathbb{P}^1$ with respect to the covering $\mathbb{P}^1 \rightarrow \mathbb{P}^1/P$. Choosing the same parametrization as before we see that an invariant function of order 6 at $\lambda = 0$ is $f^2$. Then it is immediate that the order of the ramification divisor at $(1 : 1 : 1)$ is 7. Observe that this value is exactly the contribution of three points fixed by a transposition plus two points fixed by a 3-cycle in the case $m = 1$ and for characteristic 0. So, at the end we find the same formulas for $g(X/P)$ as in theorem 4.12, for the cases when $m \neq 0$ (mod 3). In conclusion, we have the following.

**Theorem 4.13.** The formulas in theorems 4.8, 4.10 and 4.12 still hold if $X$ is defined over a field of characteristic $p \neq 2$, and the subgroup of automorphisms $P$ descends isomorphically to a subgroup of automorphisms of $\mathbb{P}^1$ permuting $0, 1, \infty$.

**Remark 4.1.** The geometrical meaning of the discussion above is the following: the curve $X/P$ over Spec($\mathbb{Z}$) has good reduction over $p = 3$, provided that $3 \nmid m$. This fact might be proven with some direct but lengthy calculations, but it is also an consequence of the invariance of the genus of the normalization of any reduction of $X$, which we have just obtained.