Annali di Matematica pura ed applicata
(IV), Vol. CLXVIII (1995), pp. 1-15

On Prime Galois Coverings of the Riemann Sphere (*)(**).

GABINO GONZÁLEZ-DIEZ

0. – Introduction and statement of results.

1. Let C be a complex curve (compact Riemann surface) of genus $g \geq 2$. We shall be primarily dealing with holomorphic automorphisms τ of prime order p such that the quotient surface $C/\langle\tau\rangle$ is isomorphic to $\boldsymbol{P}^1$.

If $p = 2$ the curve is said to be hyperelliptc and τ, which is then called the hyperelliptic involution, is known to be the unique automorphism of order 2 such that $C/\langle\tau\rangle \equiv \boldsymbol{P}^1$. The situation is quite different when $p > 2$, for then well-known curves such as Klein's and Fermat's provide examples of curves admitting different automorphisms of same prime order with quotient $\boldsymbol{P}^1$ (Examples 1.1, 1.2, 1.3). However, in all these examples we easily see that groups generated by such automorphisms are conjugate. The first part of this article is devoted to prove that this holds always; namely we shall prove.

THEOREM 1. – If the automorphism group of a Riemann surface S Aut(S), contains automorphisms τ_1, τ_2 of same prime order and such that the quotient surfaces $S/\langle\tau_i\rangle$ $(i = 1, 2)$ are isomorphic to $\boldsymbol{P}^1$; then $\langle\tau_1\rangle$ and $\langle\tau_2\rangle$ are conjugate in Aut(S).

This result can be viewed as a generalisation of the uniqueness of the hyperelliptic involution. We shall also provide examples to show that our assumptions on the order and the quotient are necessary (Examples 1.9, 1.10).

2. In the rest of the paper we shall investigate the implications of Theorem 1 in the geometry of moduli (and Teichmüller) space. In order to describe our results we need to introduce some notation.

Let $\boldsymbol{P}^n(\boldsymbol{F}_p)$ denote the projective space over the field with p elements $\boldsymbol{F}_p$, and define the following subset $\boldsymbol{D}_p^r$ of $\boldsymbol{P}^{r-1}(\boldsymbol{F}_p)$,

$$\boldsymbol{D}_p^r = \left\{ m = (m_1, \ldots, m_r) \Big/ \sum_{i=1}^{r} m_i = 0 \ \text{ and } \ \prod_{i=1}^{r} m_i \neq 0 \right\}.$$

(*) Entrata in Redazione il 25 settembre 1992.

Indirizzo dell'A.: Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049 Cantoblanco, Madrid, Spain.

(**) Research supported by a grant of the CICYT, M.E.C., Spain.

The symmetric group Σ_r acts on $\boldsymbol{D}_p^r$ in the obvious way; we write $\boldsymbol{D}_p^{(r)}$ for $\boldsymbol{D}_p^r/\Sigma_r$, $\bar{m}$ for the class of $m \bmod \Sigma_r$ and $\Sigma_r(m)$ for the stabilizer of the point $m \in \boldsymbol{D}_p^r$.

Let now $\tau\colon C \mapsto C$ be an automorphism of prime order p, having r fixed points and such that $C/\langle\tau\rangle \equiv \boldsymbol{P}^1$. We can associate to τ a point $\operatorname{rot}(\tau)$ in $\boldsymbol{D}_p^{(r)}$ by putting $\operatorname{rot}(\tau) = r$-tuple wich consists of the inverse of the local rotation angles of τ at the fixed points.

Let g, p, r be positive integers, with p prime and $g \geqslant 2$, related by the formula $2g = (p-1)(r-2)$, this is Riemann-Hurwitz formula for the projection $C \to C/\langle\tau\rangle$ above; let Mg stand for the moduli space of curves of genus g, M_g^p for the subset of Mg of points representing curves C which admit an automorphism τ of prime order p such that $C/\langle\tau\rangle \equiv \boldsymbol{P}^1$, and for each $\bar{m} \in \boldsymbol{D}_p^{(r)}$ let $M_g^p(\bar{m})$ be the subset of M_g^p defined by impossing the automorphisms τ occuring in M_g^p the extra requirement $\operatorname{rot}(\tau) = \bar{m}$.

Finally, let us denote by Δ the diagonal subset of $\boldsymbol{C}^{r-3}$ defined as follows

$$\Delta = \left\{ x \in \boldsymbol{C}^{r-3} \Big/ \prod_{i \neq j} x_i(x_i - 1)(x_i - x_j) = 0 \right\}.$$

We shall define a natural Möbius action of Σ_r on $\boldsymbol{C}^{r-3} - \Delta$ (see §, 2 (2.4)). Building on previous work of the author ([Gon], see also [Gon-Harv]) Theorem 1 will allow us to prove the following result.

THEOREM 2. – i) M_g^p is the *disjoint* union of the sets $M_g^p(\bar{m})$; where $\bar{m}$ ranges in the whole set of points of $\boldsymbol{D}_p^{(r)}$.

ii) Each set $M_g^p(\bar{m})$ is an irreducible subvariety of M_g isomorphic to $(\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m)$; the isomorphism being given by the rule which associates to each point $(\lambda_1, \dots, \lambda_{r-3})$ in $(\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m)$, the point in $M_g^p(\bar{m})$ representing the curve

$$y^p = x^{m_r - 2}(x-1)^{m_r - 1}(x - \lambda_1)^{m_1} \dots (x - \lambda_{r-3})^{m_r - 3}$$

where $m = (m_1, m_2, \dots, m_r)$.

iii) In particular the subvarieties $M_g^p(\bar{m})$ are all normal, affine and unirational.

When $p = 2$, the hyperelliptic case, this is classical. The result had also been previously settled for $p = 3$, by DUMA and RADTKE [D-R].

3. We shall work within the framework of the analytic Teichmüller theory, for which we refer to [Nag]. In the process of proving Theorem 2 we will have to consider the preimage of the subvarieties $M_g^p(\bar{m})$ via the projection $p\colon T_g \mapsto M_g = T_g/\mathrm{Mod}_g$. As usual we shall denote by $T_{g,r}$ (with $T_{g,0} = T_g$) the Teichmüller space of a compact Riemann surface of genus g with r punctures, and by $\mathrm{Mod}\, g$, r (with $\mathrm{Mod}\, g$, $0 = \mathrm{Mod}\, g$) its modular group.

It is a fundamental result of Bers that Tg, r admits a canonical representation as a bounded domain in $\boldsymbol{C}^{3g-3+r}$ on which $\mathrm{Mod}\, g$, r acts properly discontinuously by biholomorphic transformations; the quotient moduli space $Mg = Tg/\mathrm{Mod}\, g$ therefore carries and induced structure of complex analytic V-manifold, for which the canonical projection p: $Tg \mapsto Mg$ is holomorphic. Let us write $[S, \theta]$ for the point of Tg given by a (quasi-conformal) homeomorphism θ: $S_0 \mapsto S$, and let $H_0^\#$ be any subgroup of Mod g (we shall be interested in the case when $H_0^\#$ is induced by a subgroup H_0 of automorphisms of the reference surface S_0); we can introduce the *relative Teichmüller space* $Tg(H_0^\#)$ and the *relative modular group* Mod $g(H_0^\#)$ as follows.

(0.I) $T_g(H_0^\#)$ is the analytic subspace of T_g representing points left fixed by the action of $H_0^\#$.

It is known that when $H_0^\#$ is induced by $H_0 < \mathrm{Aut}(S_0)$, $T_g(H_0^\#)$ consists of Teichmüller points $[S, \theta]$ such that S possesses a group of automorphisms $H < \mathrm{Aut}(S)$ conjugate to H_0 by means of the homeomorphism θ: $S_0 \mapsto S$ ([Harv]). Moreover, denoting by γ the genus of the quotient surface $R_0 = S_0/H_0$ and by r the number of points over which the projection $S_0 \mapsto R_0$ is ramified, $T_g(H_0^\#)$ is a complex subvariety of T_g isomorphic to the Teichmüller space $T_{\gamma, r}$ ([Harv], [Krav]).

(0.II) Mod $g(H_0^\#)$ is the normaliser of $H_0^\#$ in Mod g. The modular group permutes the Teichmüller spaces $Tg(H_0^\#)$ corresponding to the various subgroups of Mod g conjugate to H_0, by the rule $h(T_g(H_0^\#)) = T_g(h \cdot H_0 \cdot h^{-1})$, where $h \in \mathrm{Mod}\, g$ and Mod $g(H_0^\#)$ is precisely the stabiliser of $T_g(H_0^\#)$. ([Mac-Harv]). In § 3 we shall prove.

THEOREM 3. – Let $\bar{m}$ be a fixed element of $\boldsymbol{D}_p^{(r)}$ and let τ_0 be an arbitrary automorphism of a Riemann surface of genus $g \geqslant 2$ with $\mathrm{rot}(\tau_0) = \bar{m}$. If $g = 2$, assume $p \neq 2$.

Then the inverse image of $M_g^p(\bar{m})$ in T_g is the following union of distinct isomorphic subvarieties

$$p^{-1}(M_g^p(\bar{m})) = \bigcup_h h(T_g(\tau_0^\#)),$$

where h ranges over a set of representatives of the cosets of Mod $g/\mathrm{Mod}_g(\tau_0^\#)$.

Moreover, the following three equivalent statements hold

i) The topological surface of genus g possesses infinitely many mapping classes (topologically) conjugate to τ_0.

ii) In T_g there are infinitely many distinct Mod_g-transforms of $T_g(\tau_0^\#)$.

iii) $\mathrm{Mod}_g(\tau_0^\#)$ has infinite index in Mod g.

We would like to comment on this result. When $p = 2$, this is Theorem 6.5 of the famous paper of Kravetz [Krav], and in fact we have to use his theorem to settle ours since our proof fails to work in this case. As a compensation it does work in any other case, *i.e.* when instead of prime coverings of $\boldsymbol{P}^1$ we consider any Galois covering of any Riemann surface. In particular we obtain.

COROLLARY 3.I. – Except for the hyperelliptic covering in genus 2, there does not exist any Galois covering of any Riemann surface with the property that its relative modular group coincides with the entire modular group.

This result was conjectured, and proved for cyclic coverings of $\boldsymbol{P}^1$, by BIRMAN and HILDEN in [Bir-Hill].

The author is grateful to Drs. W. J. HARVEY and C. MACLACHLAN for generous discussions on the subject of this article.

1. Prime Galois coverings of the Riemann sphere.

The main goal of this section is to prove Theorem 1. We begin by showing some curves admitting automorphisms τ_1, τ_2 of same prime order p, generating distinct groups $\langle\tau_1\rangle, \langle\tau_2\rangle$ and having the same quotient $S/\langle\tau_i\rangle \equiv \boldsymbol{P}^1$ $(i = 1, 2)$. We refer to [F-K], [J-S] or [Nar] for the standard techniques to identify algebraic curves and Riemann surfaces.

EXAMPLE 1.1. – Klein's curve $y^7 = x(x-1)^2$.

The group generated by the automorphism $\tau(x, y) = (x, \xi_7 y)$ with $\xi_p = e^{2\pi i/p}$ is different from some conjugate of itself because the automorphism group of this curve is known to be simple; in fact the simple group of order 168.

EXAMPLE 1.2. – Fermat's curve F_p of equation $x^p + y^p = 1$.

The groups generated by $\tau_1(x, y) = (x, \xi_p y)$ and $\tau_2(x, y) = (\xi_p x, y)$ are clearly different, but as in the previous example τ_1 and τ_2 are conjugate (now by means of the coordinate interchanging involution $\sigma(x, y) = (y, x)$).

There is another automorphism of F_p which has order p and quotient surface $\boldsymbol{P}^1$, namely

$$\tau(x, y) = (\xi_p x, \xi_p y).$$

We note that $\langle\tau\rangle$ too is conjugate to $\langle\tau_1\rangle$ and $\langle\tau_2\rangle$, for we have $\varphi^{-1}\cdot\tau\cdot\varphi = \tau_2^{p-1}$; φ being the automorphism $\varphi(x, y) = (1/x, -y/x)$.

It can be easily seen (by working as in Example 1.4 below) that these three account for all the proper subgroups of $H = \langle\tau_1, \tau_2\rangle$ with quotient surface $\boldsymbol{P}^1$.

EXAMPLE 1.3. – The curves D_p of equation

$$y^p = (x^p - 1)(x^p - \lambda^p)^{p-1}; \qquad \lambda \in \boldsymbol{C},\ \lambda^p \neq 1 \text{ (see [D-R] for } p = 3).$$

Again we take $\tau_1(x, y) = (x, \xi_p y)$ and $\tau_2(x, y) = (\xi_p x, y)$.

Now the involution which conjugates $\langle\tau_1\rangle$ and $\langle\tau_2\rangle$ is

$$\sigma(x, y) = \left(\frac{x^p - \lambda^p}{y}, \frac{x^{p-1}(1-\lambda^p)}{x^p - 1}\right)$$

in fact one easily checks that $\sigma^{-1}\cdot\tau_1\cdot\sigma = \tau_2^{p-1}$.

In the next example we see that the exponent $p-1$ in the equation defining D_p is crucial.

EXAMPLE 1.4. – *a*) Let S be the Riemann surface defined by the equation

$$y^p = (x^p - 1)(x^p - \lambda^p)^k, \qquad \lambda^p \neq 1, \ k < p - 1.$$

Now $\tau_1(x, y) = (x, \xi_p y)$ and $\tau_2(x, y) = (\xi_p x, y)$ cannot be conjugate since τ_1 has $2p$ fixed points, namely $(\xi_p^i, 0)$, $(\xi_p^i\lambda, 0)$, $i = 1, \dots p$, whereas τ_2 has only p, namely $(0, \xi_p^i\lambda)$.

In order to show that the points at infinity are not fixed by τ_2, we make the standard representation of S as the p-sheeted covering $S \mapsto S/\langle\tau_1\rangle \equiv \boldsymbol{P}^1$, which is represented by the x-projection,

$$S \mapsto \boldsymbol{P}^1, \qquad (x, y) \mapsto x.$$

We need to understand this projection at ∞, so we take the usual parameter $x = 1/t$ where t is any parameter near the origin, and then we see that S has p points ∞_i $(i = 1, \dots, p)$ above $\infty \in \boldsymbol{P}^1$, corresponding to the p roots

$$y = \xi_p^i \frac{\sqrt[p]{(1-t)^p(1-\lambda^p t^p)^k}}{t^{1+k}}, \qquad i = 1, \dots, p.$$

The action of the automorphism $\tau_{s,d}(x, y) = (\xi_p^s x, \xi_p^d y)$ at these points is given by $\tau_{s,d}(\infty_i) = \xi_p^{d-s(1+k)}\infty_i$ as we see by replacing the parameter t by $t' = \xi_p^{-s}\cdot t$; thus $\tau_{s,d}$ fixes ∞_i if and only if $d \equiv s(1+k)(\mathrm{mod}\cdot p)$; in other words $\tau_2 = \tau_{1,0}$ does not fix any point at infinity when $k < p - 1$.

In fact this computation shows that $\langle\tau_1\rangle$ is the only proper subgroup of $H = \langle\tau_1, \tau_2\rangle$ which has $2p$ fixed points.

b) ($p = 3$, $k = 1$). With a little more work we can see that when $p = 3$ $\langle\tau_1\rangle$ is in fact the only subgroup in the whole Aut(S), having this property. This will follow from the following observations

1) the divisor of the function x (the x-projection) is

$$(x) = \frac{(0, \lambda)\cdot(0, \xi_3\lambda)\cdot(0, \xi_3^2\lambda)}{\infty_1\cdot\infty_2\cdot\infty_3} = U/D;$$

2) the divisor of the differential $(1/y^2)\cdot dx$ is

$$Z = \left(\frac{\infty_1^2 \cdot \infty_2^2 \cdot \infty_3^2}{\prod_{i=1}^{3} (\xi_3^i, 0)\cdot(\xi_3^i \lambda, 0)} \right)^2 \cdot \frac{\prod_{i=1}^{3} (\xi_3^i, 0)^2 \cdot (\xi_3^i \lambda, 0)^2}{\infty_1^2 \cdot \infty_2^2 \cdot \infty_3^2} = (\infty_1 \cdot \infty_2 \cdot \infty_3)^2 .$$

The fact that the degree of the canonical divisor Z is 6 means that the genus of S is 4, and the fact that $D^2 = Z$ implies ([F-K], p. 109; see also [D-R]) that x is, up to a Möbius transformation, the only function of degree 3 on S. This is equivalent to saying that $\langle \tau_1 \rangle$ is the only subgroup of order 3 in $\mathrm{Aut}(S)$ such that $S/\langle \tau_1 \rangle \equiv \boldsymbol{P}^1$.

REMARK 1.5. – For later use, we record here that the Theorem in [F-K], p. 109, mentioned above, also implies that the curves D_3 of Example 1.3 with $p = 3$, $\langle \tau_1 \rangle$ and $\langle \tau_2 \rangle$ are the only subgroups of order 3 with quotient $\boldsymbol{P}^1$.

We start now looking for general results.

LEMMA 1.6. – Let S be a Riemann surface and let $\sigma, \tau \in \mathrm{Aut}(S)$ have same prime order p. Assume further that σ and τ commute and that $\langle \sigma \rangle \neq \langle \tau \rangle$. Then σ permutes the fixed point set of τ, $\mathrm{Fix}(\tau)$, dividing it into a number of orbits of length p, and the rotation angles of τ at the p points in the same orbit coincide. In particular the number of points fixed by τ is a multiple of p.

PROOF. – Clearly since σ and τ commute, they permute the fixed point set of each other. Moreover, since the stabiliser of any point is a cyclic subgroup of $\mathrm{Aut}(S)$ ([F-K], p. 100), τ and σ cannot have fixed points in common for otherwise we would have $\langle \tau \rangle = \langle \sigma \rangle$. From these facts, the proof of the lemma follows.

LEMMA 1.7. – Let S be a Riemann surface of arbitrary genus possessing commuting automorpohisms τ, σ of same prime order p such that $S/\langle \tau \rangle \equiv \boldsymbol{P}^1$ and $\sigma \notin \langle \tau \rangle$. Then, S is isomorphic to the surface determined by an algebraic equation of the form

$$y^p = (x^p - 1)(x^p - \lambda_2^p)^{m_2} \dots (x^p - \lambda_r^p)^{m_r}$$

where the complex numbers $1, \lambda_2^p, \dots, \lambda_r^p$ are all distinct and the numbers m_i are integers $1 \leqslant m_i < p$ with $\sum m_i \equiv 0 \pmod{p}$.

Moreover, in this model of S $\tau(x, y) = (x, \xi_p y)$ and $\sigma(x, y) = (\xi_p^i x, \xi_p^j y)$ for certain integers $1 \leqslant i \leqslant p - 1$ and $0 \leqslant j \leqslant p \cdot 1$.

PROOF. – The hypothesis clearly imply that S admits an algebraic model of the form

$$y^p = (x - a_1)^{d_1} \dots (x - a_n)^{d_n}; \qquad 1 \leqslant d_i < p$$

in which τ is expressed as $\tau(x, y) = (x, \xi_p y)$, the points $(a_i, 0)$, $i = 1 \dots n$ are the fixed points of τ and d_i is the inverse of the rotation angle of τ at the i-th fixed point (see *e.g.* [Gon],§ 1).

By performing a birational transformation, we may assume that $d_1 = 1$; and by Lemma 1.6 we have $n = rp$ for some integer r.

On the other hand, since $S/\langle\tau\rangle \equiv \boldsymbol{P}^1$-via the map $x - \sigma$ induces an automorphisms $\tilde{\sigma}\colon \boldsymbol{P}^1 \mapsto \boldsymbol{P}^1$ of order p. By normalising x so that 0, ∞ are the fixed points of $\tilde{\sigma}$ and $a_1 = 1$, we can assume that $\tilde{\sigma}$ is the rotation $\tilde{\sigma}(x) = \xi_p^i \cdot x$ for some integer $1 \leq i < p \cdot 1$ (see [J-S]).

Let us suppose now that the fixed points of τ are numbered so that

$$\{(a_{(k-1)p+1}, 0), \ldots, (a_{kp}, 0)\}, \qquad k = 1, \ldots r$$

are the r σ-orbits as discussed in Lemma 1.6. Then we must have $d_{(k-1)p+1} = \ldots = d_{kp}$ and also $a_{(k-1)p+2} = \tilde{\sigma}(a_{(k-1)p+1}) = \xi_p^i \cdot a_{(k-1)p+1}$ etc.

Our algebraic model of S becomes

$$y^p = \prod_{i=1}^{p} (x - \xi_p^i) \prod_{i=1}^{p} (x - \xi_p^i \lambda_2)^{m_2} \ldots \prod_{i=1}^{p} (x - \xi_p^i \lambda_r)^{m_r},$$

which is the one we were looking for.

Finally we observe that σ is necessarily of the form $\sigma(x, y) = (\xi_p^i x, \xi_p^j y)$ for some integer $1 \leq j \leq p$. This concludes the proof of our lemma.

PROPOSITION 1.8. – Let S be a Riemann surface of arbitrary genus and $p > 2$ a prime number; then $\mathrm{Aut}(S)$ possesses a p-group H of order $\geq p^2$ generated by automorphisms τ_1, τ_2 of same prime order p and same quotient surface $S/\langle\tau_i\rangle \equiv \boldsymbol{P}^1$ $(i = 1, 2)$, if and only if S is isomorphic to one of the following Riemann surfaces

$$F_p\colon y^p = x^p - 1,$$

$$D_p\colon y^p = (x^p - 1)(x^p - \lambda^p)^{p-1}, \qquad \text{for some } \lambda \in \boldsymbol{C},\ \lambda^p \neq 1.$$

Moreover in both cases H is the group of order p^2 consisting of the following automorphisms

$$\tau(x, y) = (\xi_p^s x, \xi_p^d y) \quad \text{with } 1 \leq s,\ d \leq p.$$

PROOF. – We observe that since p-groups have non-trivial center there exists $\sigma \in H$, which we can assume of order p, commuting with τ_1 (and τ_2). By the preceding lemma then, we know that S is a surface of the form

$$y^p = (x^p - 1)(x^p - \lambda_2^p)^{m_2} \ldots (x^p - \lambda_r^p)^{m_r},$$

with $\tau_1(x, y) = (x, \xi_p y)$, $\sigma(x, y) = (\xi_p^i x, \xi_p^j y)$.

Our next step is to show that τ_2 cannot have more than $2p$ fixed points. In order to do that, we consider on S the meromorphic function $x \cdot \tau_2$ (composition of τ_2 followed by the x projection); since the function x has degree p, it is not hord to prove (see

[F-K], p. 245) that if τ_2 had more than $2p$ fixed points, then $x \cdot \tau_2 = x$ which means that $\tau_2(x, y) = (x, \xi_p^j y)$ for some integer j; in other words we would have $\tau_2 \in \langle \tau_1 \rangle$ and hence $|H| = p < p^2$ in contradiction with our hypothesis.

We also observe that τ_1 and τ_2 have the same number of fixed points because Riemann-Hurwitz formula is the same for both automorphism; thus by Lemma 1.6. τ_1 has either p or $2p$ fixed points and therefore our surface S is of one of the two following forms

$$F_p \colon y^p = x^p - 1\,,$$

$$D_p^k \colon y^p = (x^p - 1)(x^p - \lambda^p)^k.$$

Next assume $p > 3$, we claim that $H = \langle \tau_1, \sigma \rangle$, that is we claim that $\tau_2 \in \langle \tau_1, \sigma \rangle$. If not, τ_1 and τ_2 would induce on $\bar{S} = S/\langle \sigma \rangle$ automorphisms $\bar{\tau}_1, \bar{\tau}_2$ which again satisfy the hypothesis of our Proposition for same prime number p; since the genus $\bar{g}$ of $\bar{S}$ has to be strictly smaller than the genus g of S, we must necessarily have $\bar{S} = F_p$ and $S = D_p^k$ for some integer k (and some $\lambda \in \boldsymbol{C}$). The desired contradiction is provided by the fact that for $p > 3$ the genera do not match in Riemann-Hurwitz formula for the projection $S \mapsto S/\langle \sigma \rangle = \bar{S}$.

This formula states that

$$2g - 2 = p(2\bar{g} - 2) + (p - 1) \cdot (\# \operatorname{Fix}(\sigma))$$

which is incompatible for $p > 3$ with

$$2g - 2 = p(-2) + (p - 1)2p\,,$$

$$2\bar{g} - 2 = p(-2) + (p - 1)p\,,$$

which are Riemann-Hurwitz formulas for the projections $D_p^k \mapsto D_p^k/\langle \tau_1 \rangle$ and $F_p \to \to F_p/\langle \tau_1 \rangle$ respectively.

Thus we have already proved that when $p > 3$ the group $H = \langle \tau_1, \tau_2 \rangle$ consists of the elements

$$\tau(x, y) = (\xi_p^s x, \xi_p^d y) \quad \text{with } 1 \leqslant s,\ d \leqslant p\,;$$

but by Example 1.4.*a* in order for H to possess two distinct proper subgroups with quotient surface $\boldsymbol{P}^1$, we must have $k = p - 1$ i.e. $D_p^k = D_p$.

As for the remaining case $p = 3$, the result follows from Example 1.4.b and Remark 1.5.

We are now in position to prove Theorem 1.

PROOF OF THEOREM 1. – By the uniqueness of the hyperelliptic involution (see e.g. [F-K], p. 102) we can assume from the begining that $p \geqslant 3$.

Let τ_1, τ_2 be automorphisms of same prime order p, such that $\langle \tau_1 \rangle \neq \langle \tau_2 \rangle$ and $S/\langle \tau_i \rangle \equiv \boldsymbol{P}^1$ $(i = 1, 2)$, then each $\langle \tau_i \rangle$ is contained in some p-Sylow group H_i $(i = 1, 2)$.

But Sylow groups are conjugate, so there is $\varphi \in \mathrm{Aut}(S)$ such that $\tau_1' = \varphi \cdot \tau_1 \cdot \varphi^{-1} \in H_2$.

Now if $\langle \tau_1' \rangle \neq \langle \tau_2 \rangle$ Proposition 1.8 says that S is either F_p or D_p and $H = \langle \tau_1', \tau_2 \rangle$ is the group described there; moreover by Examples 1.2 and 1.3 τ_1' and τ_2 are conjugate, hence τ_1 and τ_2 must also be conjugate. This ends the proof.

We close this section by producing two examples showing that if in Theorem 1 the order of τ_i is not prime, or the quotient surface $S/\langle \tau_i \rangle$ is not $\boldsymbol{P}^1$; then τ_1 and τ_2 need not be conjugate. In fact, it can be seen by using deformation theory of Riemann surfaces, that this is a general phenomenon (see [Gon-Harv]).

EXAMPLE 1.9. – Consider the hyperelliptic curve of genus 5 defined by the equation $y^2 = x^{12} + x^6 + 1$ and the following automorphisms of order 6

$$\tau_1(x, y) = (\xi_6 x, y) \quad \text{and} \quad \tau_2(x, y) = (\xi_3 x, -y).$$

One ckecks by hand that τ_1, τ_1^2 and τ_1^3 have the same fixed point set, namely

$$\{(0, 1), (0, -1), \infty_1, \infty_2\};$$

whereas τ_2 has no fixed points, τ_2^2 has the same fixed point set as τ_1, and τ_2^3, which is the hyperelliptic involution, fixes the following 12 points

$$\{(\xi_{18}^k, 0)/k \text{ prime to } 3\}.$$

Clearly $\langle \tau_1 \rangle$ and $\langle \tau_2 \rangle$ cannot be conjugate. On the other hand Riemann-Hurwitz formula implies that $S/\langle \tau_1 \rangle \equiv S/\langle \tau_2 \rangle \equiv \boldsymbol{P}^1$.

Our next example is a translation of computations on reduction of abelian integrals due to Hermite (but that, in fact, going back to Jacobi and Legendre ([Her] see also [Kraz], p. 477)), into the language of algebraic curves.

EXAMPLE 1.10. – Consider the hyperelliptic curve C of genus 2 with equation

$$w^2 = z(1 - z)(1 + az)(1 + bz)(1 - abz)$$

and the automotphisms $\tau_1(z, w) = (1/abz, w/(ab)^{3/2} z^3)$ and $\tau_2 = J \cdot \tau_1$ where J stands for the hyperelliptic involution. Then, τ_1 and τ_2 have both the same order 2 and the same number 2 of fixed points.

The quotient surfaces $S/\langle \tau_i \rangle$ $(i = 1, 2)$ are the elliptic curves of equations

$$y^2 = x(1 - x)(1 - K^2 x) \quad \text{and} \quad y^2 = x(1 - x)(1 - l^2 x)$$

respectively; where

$$K = \frac{\sqrt{a} + \sqrt{b}}{\sqrt{(1 + a)(1 + b)}} \quad \text{and} \quad l = \frac{\sqrt{a} - \sqrt{b}}{\sqrt{(1 + a)(1 + b)}}.$$

One sees by looking at the j-invariant that these two elliptic curves are in general non-isomorphic; thus τ_1 and τ_2 cannot be conjugate.

2. – Moduli of prime Galois coverings of $\boldsymbol{P}^1$.

In this section we derive Theorem 2 from Theorem 1. First we quote from [Gon] some results we need; we employ the same notation as in the introduction.

If G is a subgroup of the group of automorphisms of a Riemann surface S_0, we denote by $M_g(G)$ the subset of M_g consisting of points representing curves which admit a group of automorphisms topologically conjugate to G. We denote by $\widetilde{M}_g(G)$ the quotient variety $\widetilde{M}_g(G) = T_g(G^{\#})/\mathrm{Mod}_g(G^{\#})$. One has the following results.

(2.1) The natural surjection $\widetilde{M}_g(G) \mapsto M_g(G) \subseteq M_g$ is generically injective, and hence $\widetilde{M}_g(G)$ is the normalisation of the irreducible subvariety $M_g(G)$.

(2.2) $M_g(G) \neq \widetilde{M}_g(G)$, that is to say $M_g(G)$ is not normal, if and only if there exists a Riemann surface S of genus g possessing subgroups G_1, G_2 of $\mathrm{Aut}(S)$, which are topologically conjugate to G, but not analytically conjugate to each other.

These two facts were proved in [Gon] for the relevant case here, namely when $G = \langle \tau_0 \rangle$ has prime order and quotient surface $\boldsymbol{P}^1$, but clearly the proof works for the general case (see [Gon-Harv]). In our article [Gon] we also proved the two following statements.

(2.3) Two automorphisms $\tau_i \colon S_i \mapsto S_i$ $(i = 1, 2)$ with the same prime order p, same number r of fixed points, and same quotient surface $S/\langle \tau_i \rangle \equiv \boldsymbol{P}^1$, are topologically conjugate if and only if they have same rotation angles, that is to say if and only if $\mathrm{rot}(\tau_1) = \mathrm{rot}(\tau_2) \in \boldsymbol{D}_p^{(r)}$.

(2.4) Assume $G = \langle \tau_0 \rangle$ has prime order p, r fixed points, quotient surface $\boldsymbol{P}^1$ and rotation data $\mathrm{rot}(\tau_0) = \bar{m} \in \boldsymbol{D}_p^{(r)}$. Then there exists rational functions on the $1/2p$-theta constants $\lambda_i \colon T_g(\tau_0^{\#}) \mapsto \boldsymbol{C} - \{0, 1\}$ such that the curve represented by a point $t \in T_g(\tau_0^{\#})$ is precisely (isomorphic to) $y^p = x^{m_{r-2}}(x-1)^{m_{r-1}}(x - \lambda_1(t))^{m_1} \ldots (x - \lambda_{r-3}(t))^{m_{r-3}}$, where $m = (m_1, \ldots, m_r)$.

Moreover the functions λ_i behave with respect to $\mathrm{Mod}_g(\tau_0^{\#})$ in such a way that the rule

$$t \mapsto (\lambda_1(t), \ldots, \lambda_r(t))$$

induces an isomorphism $\widetilde{M}_g(\tau_0) \xrightarrow{\sim} ((\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m))$, thus these functions λ_i generalise in a natural way the classical λ-function of elliptic modular theory.

Here the symmetric group Σ_r, and hence the subgroups $\Sigma_r(m)$, acts on $\boldsymbol{C}^{r-3} - \Delta$ as follows.

For given $\sigma \in \Sigma_r$ and $(\lambda_1, \ldots, \lambda_{r-3}) \in \boldsymbol{C}^{r-3} - \Delta$, form first the r-tuple $(0, 1, \infty, \lambda_1, \ldots, \lambda_{r-3})$; then apply σ to obtain $(\sigma(0), \sigma(1), \ldots, \sigma(\lambda_{r-3}))$. Finally, let T:

$C \mapsto C$ be the unique Möbius transformation that sends $\sigma(0)$, $\sigma(1)$, $\sigma(\infty)$ to 0, 1, ∞ respectively. Then

$$\sigma \cdot (\lambda_1, \ldots, \lambda_{r-3}) = (T(\sigma(\lambda_1)), \ldots, T(\sigma(\lambda_{r-3}))).$$

We observe that if $m, m' \in \boldsymbol{D}_p^r$ differ by a permutation, then the corresponding subgroups $\Sigma_r(m)$, $\Sigma_r(m')$ are conjugate, thereby inducing natural isomorphisms $((\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m)) \xrightarrow{\sim} ((\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m'))$; thus in Theorem 2 part ii), it is irrelevant which representative m of $\bar{m} \in \boldsymbol{D}_p^{(r)}$ we choose.

PROOF OF THEOREM 2. – *Part* i) By (2.3) $M_g^p(\bar{m}) = M_g(\tau_0)$ for $\bar{m} = \mathrm{rot}(\tau_0)$ and by Theorem 1 all these varieties are disjoint.

Part ii) Theorem 1 along with (2.1) and (2.2) implies that $M_g^p(m) = \widetilde{M}_g^p(\tau_0) = T_g(\tau_0^{\#})/\mathrm{Mod}_g(\tau_0^{\#})$ which by (2.4) is isomorphic to $((\boldsymbol{C}^{r-3} - \Delta)/\Sigma_r(m))$.

Finally Part iii) is a consequence of Parts i) and ii).

REMARKS. – 1) In those terms the meaning of Example 1.9 is that if we do not require the order p to be prime, two subvarieties $M_g(\langle\tau_1\rangle)$, $M_g(\langle\tau_2\rangle)$ may intersect without coinciding. In fact it can be seen using 0.I and 2.1 that in this case $M_g(\langle\tau_1\rangle) = M_g(\langle\tau_1, \tau_2\rangle)$ has dimension 1, $M_g(\langle\tau_2\rangle)$ has dimension 3 and $M_g(\langle\tau_1\rangle) \subsetneq M_g(\langle\tau_2\rangle)$.

2) On the other hand Example 1.10 provides according to (2.2) an instance in which $M_g(\tau) \neq \widetilde{M}_g(\tau)$ because although τ_1 and τ_2 are not analytically conjugate, they are by (a generalisation of) (2.3)-see [Gue]-topologically conjugate. In fact (see [Gon-Harv]) this is a general phenomenon.

3) The number of irreducible (or even connected) components of $M_g^p = \cup M_g^p(\bar{m})$, that is to say the integer $a_r = \# \boldsymbol{D}_p^{(r)}$, can be read of from Lloyd's ([Llo]) generating function

$$\sum a_r x^r = \frac{1}{p-1}\left\{\frac{1}{p}\left[\frac{1}{(1-x)^{p-1}} + (p-1)\frac{1-x}{(1-xp)}\right] + \sum_{\substack{ll' = p-1 \\ l \neq 1}} \frac{\varphi(l)}{(1-x^l)^{l'}}\right\},$$

where φ is the Euler function. For instance for $p = 2$, we obtain

$$a_r = \begin{cases} 0, & \text{for } r \text{ odd} \\ 1, & \text{for } r \text{ even} \end{cases}$$

as it should be.

4) While the language adopted throughout this paper is that of complex analytic geometry, it may be noted that since M_g is known to be a quasi-projective variety, our results remain valid within the framework of complex algebraic geometry. Namely, each $M_g^p(\bar{m})$ is also an irreducible algebraic subvariety of M_g by Chow's Theorem ([Gra-Rem], p. 184).

3. – The relationship between $\mathrm{Mod}_g(G)$ and Mod_g.

The aim of this final section is to prove Theorem 3. Clearly the subgroups of Mod_g conjugate to $\langle \tau_0^\# \rangle$ are in one-to-one correspondence with the cosets of Mod_g module $\mathrm{Mod}_g(\tau_0^\#)$, hence the three statements in Theorem 3. are equivalent and it is enough to prove that the family $\{f\cdot\tau_0^\#\cdot f^{-1}/f\in \mathrm{Mod}_g\}$ contains infinitely many elements.

NOTATION. – Let τ be an automorphism of a Riemann surface S of genus $g \geqslant 2$; we denote by τ^* and τ_* the induced automorphisms of the complex vector spaces $H^0(S, \Omega)$ and $H_1(S, \boldsymbol{C})$ respectively. We denote by $E_\mu(\tau_*)$ the eigenspace of some $\mu \in \boldsymbol{C}$ previously fixed.

LEMMA 3.1. – Let τ, τ' be automorphisms of Riemann surfaces S, S' conjugate by means of a homeomorphism $f\colon S\mapsto S'$. Then for any $\mu\in\boldsymbol{C}$, $f_*\colon H_1(S,\boldsymbol{C})\mapsto H_1(S,\boldsymbol{C})$ maps $E_\mu(\tau_*)$ onto $E_\mu(\tau'_*)$.

PROOF. – The result is a consequence of the identity $f_*\cdot\tau_*\cdot f_*^{-1} = \tau'_*$.

LEMMA 3.2. – If τ has prime order and τ^* has only one eigenvalue $\mu\in\boldsymbol{C}$; then either $\mu = 1$ and τ is the identity, or $\mu = -1$ and τ is the hyperelliptic involution.

PROOF. – Let $\tau \neq$ identity have order p, then it is known (see *e.g.* [F-K]. V) that τ^* can be diagonalized and that its eigenvalues are p-th roots of unity. Now if τ^* has only one eigenvalue μ, that is to say if the complex dimension of the vector space $E_\mu(\tau^*)$ is g, then Lefschetz Fixed Point Theorem reads (see [F-K]. V)

$$g(\mu+\bar{\mu}) = 2 - N\,,$$

where $\bar{\mu}$ is the complex conjugate of μ and N is the number of fixed points of τ, hence an integer; we see that this equation is only possible if the p-th root of unity μ is 1, -1, or a cubic root of unity.

Now, it is known that the dimension of $E_1(\tau^*)$ is precisely the genus $\bar{g}$ of the quotient surface $\bar{S} = S/\langle\tau\rangle$ ([F-K], V, p. 254).

Since for $g \geqslant 2$ we must have $\bar{g} < g$, we conclude that the case $\mu = 1$ is impossible (this conclusion can be also derived directly from Lefschetz's Formula above).

On the other hand if $\mu = -1$, then $p = 2$, $N = 2g+2$, and hence τ is the hyperelliptic involution ([F-K], p. 245).

Finally we consider the case in which $p = 3$ and μ a cubic root of unity. Clearly, we must have $\bar{g} = 0$, for otherwise 1 would also be an eigenvalue. Thus, writing matters in algebraic terms as we did in § 1, we find that, S has algebraic equation

$$y^3 = (x-c_1)\ldots(x-c_l)(x-c_{l+1})^2\ldots(x-c_{l+s})^2\,,$$

where we can assume that $l+2s$ is prime to 3 so that the curve has precisely one point at infinity; and that the automorphism τ has the expression $\tau(x, y) = (x, \xi_3 y)$.

Moreover, it is not hard to check that the divisors of the differentials dx/y and $(x - c_{l+1}) \dots$
$\dots (x - c_{l+s}) dx/y^2$, are $(c_1, 0) \dots (c_l, 0) \infty^{l+2s-4}$ and $(c_{l+1}, 0) \dots (c_{l+s}, 0) \infty^{2l+s-4}$ respectively. Since we are assuming that $g = l + s - 1 \geq 2$ and $l + s \neq 3$, we must have $l + s \geq 4$ which implies that both 1-forms are holomorphic. Not only that; we also observe that these 1-forms are eigenvectors of τ^* with distinct eigenvalues ξ_3^2 and ξ_3 respectively. This completes the proof of the lemma.

PROOF OF THEOREM 3. – By Lemma 3.1 it is enough to construct a sequence of homeomorphisms $f_n\colon S_0 \mapsto S_0$, $n \in \boldsymbol{Z}$; such that for some $\mu \in \boldsymbol{C}$, $f_{m_*}^{-1} \cdot f_{n_*}(E_\mu(\tau_{0_*})) \neq E_\mu(\tau_0)$ wherever $n \neq m$.

We can assume that our automorphism $\tau_0\colon S_0 \mapsto S_0$ is not the hyperelliptic involution because in this case the result is known ([Krav]).

Let $\{a_i, b_i\}$ $i = 1, \dots g$; be a symplectic basis of $H_1(S, \boldsymbol{Z})$ and let $\sigma = \sum z_i a_i + w_i b_i$ be an eigenvector of τ_{0_*} with eigenvalue $\mu \in \boldsymbol{C}$. Here z_i, w_i are complex numbers with, say, $w_1 \neq 0$.

We note that for at least one of the a-loops we have $a_k \notin E_\mu(\tau_{0_*})$ for otherwise all the elements of the dual basis for the holomorphic 1-forms $v_1, \dots, v_g$, would satisfy $\tau^*(v_i) = \mu v_i$ in contradiction ith Lemma 3.2. We assume that k is the first index for which this occurs.

For each $n \in \boldsymbol{Z}$, let f_n be a homeomorphism of S_0 such that f_{n_*} acts on the cycles $a_i, b_i; i = 1, \dots g$; as follows $f_{n_*}(b_1) = na_k + b_1$, $f_{n_*}(b_k) = na_1 + b_k$, and f_{n_*} is the identity for the other cycles of the canonical basis. Such a homeomorphism exists because f_{n_*} is symplectic and it is wellknown that the natural map from Mod g into the symplectic group $S_p(g, \boldsymbol{Z})$ is surjective (see *e.g.* [Bir-Hil 2]). We observe that the following relations are satisfied $f_{m_*} \cdot f_{n_*} = f_{n+m_*}$ and $f_{n_*}^{-1} = f_{-n_*}$.

Therefore we have $f_{m_*}^{-1} f_{n_*}(\sigma) = \sigma + w_1(n-m)a_k + w_k(n-m)a_1$, and $\tau_{0_*}(f_{m_*}^{-1} f_{n_*}(\sigma)) = \mu\sigma + \tau_{0_*}((n-m)w_1 a_k + (n-m)w_k a_1)$.

We would like to show that $f_{m_*}^{-1} \cdot f_{n_*}(\sigma)$ does not lie in $E_\mu(\tau_{0_*})$, or equivalently that $\alpha = (w_1 a_k + w_k a_1) \notin E_\mu(\tau_{0_*})$.

Now if $k = 1$, $a_1 \notin E_\mu(\tau_{0_*})$ and therefore $\alpha = 2w_1 a_1 \notin E_\mu(\tau_{0_*})$, and if $k > 1$ then $a_1 \in E_\mu(\tau_{0_*})$ but $a_k \notin E_\mu(\tau_{0_*})$ and the same argument works. This completes the proof of Theorem 3.

REMARKS. – 1) We have shown that the index of Mod $g(\tau_0^\#)$ in Mod g is infinite for τ_0 of prime order, without any restriction on the quotient surface $S/\langle\tau_0\rangle$; since any non-trivial finite group G contains elements of prime order, we have proved that the same statement holds for all $\mathrm{Mod}_g(G)$ except for the case, of course, when S has genus 2, and G is the group generated by the hyperelliptic involution J (for in this case, it is wellknown that $\mathrm{Mod}_2(J^\#) = \mathrm{Mod}_2$), and also when $g = 2$ and G is such that J is the only element of prime order in G.

Now one sees (see *e.g.* [Rau]) that the only occurrence of the last phenomenon is when S is one of the two curves $w^2 = z^6 - 1$ or $w^2 = z^5 - z$ for which the 1-forms dz/w, dz/w^2 afford a basis for $H^0(S, \Omega)$, and it can be checked by hand that in both cases all possible automorphisms τ such that τ^2 is the hyperelliptic involution have again distinct eigenvalues. Thus the statement of Corollary 3.I. holds.

2) When $p = 2$, the uniqueness of the hyperelliptic involution implies that two copies $h_i(T_g(\tau_0^\#))$, $h_i \in \mathrm{Mod}\,g$ $(i = 1, 2)$ are either disjoint or coincide and in fact Kravetz ([Krav]) uses this observation to prove that in this case there are infinitely many of them. This does not happen again; the fact that for $p > 2$ a Riemann surface may admit two distinct subgroups $\langle\tau_0\rangle$, $\langle\tau_0'\rangle$ analytically conjugate by means of φ, means that the subvarieties $T_g(\tau_0^\#)$ and $\varphi^\#(T_g(\tau_0^\#))$ do intersect.

REFERENCES

[Bir-Hil 1] J. S. BIRMAN - H. M. HILDEN, *On isotopies of homeomorphisms of Riemann surfaces,* Ann. Math., 97 (1973), pp. 424-39.

[Bir-Hil 2] J. S. BIRMAN - H. M. HILDEN, *On the mapping class group of closed surfaces as covering spaces,* Ann. Math. Studies., No. **66**, Princeton (1971), pp. 53-79.

[D-R] A. DUMA - W. RADTKE, *Automorphismen und Modulraum galoisscher dreiblätriger Überlagerungen,* Manuscripta Math., **50** (1985), pp. 215-228.

[F-K] H. M. FARKAS - I. KRA, *Riemann surfaces,* Graduate Texts in Mathematics, **71**, Springer, Berlin (1980).

[Gon] G. GONZÁLEZ-DIEZ, *Loci of curves which are prime Galois coverings of* $\boldsymbol{P}^1$, Proc. London Math. Soc., (3), **62** (1991), pp. 469-489.

[Gon-Harv] G. GONZÁLEZ-DIEZ - W. J. HARVEY, *Moduli of Riemann surfaces with Symmetry, Discrete Groups and Geometry,* London Math. Soc., L.N. Series, **173** (1992), pp. 75-94.

[Gra-Rem] H. GRAUERT - R. REMMERT, *Coherent analytic Sheaves,* Grundlehren der Math. Wissensch., **265**, Springer, Berlin (1980).

[Gue] I. GUERRERO, *Holomorphic families of compact Riemann surfaces with automorphisms,* Illinois J. Maths., **26** (1982), pp. 212-25.

[Harv] W. J. HARVEY, *On branch loci in Teichmüller space,* Trans. Amer. Math. Soc., **153** (1971), pp. 387-99.

[Her] C. HERMITE, *Sur un example de réduction d'intégrales abéliennes, aux fonction elliptiques,* Ann. Soc. Sci. Bruxelles, 1re. année (1876), pp. 1-16.

[J.-S] G. A. JONES - D. SINGERMAN, *Complex Functions,* Cambridge University Press (1987).

[Krav] S. KRAVETZ, *On the geometry of Teichmüller spaces and the structure of their modular groups,* Ann. Acd. Sci. Fenn. (1959), pp. 1-35.

[Kraz] A. KRAZER, *Lehrbuch der Thetafunktionen,* Chelsea, New York, (1970).

[Llo] E. K. LLOYD, *Riemann Surface transformation groups,* J. Combin. Theory A, **13** (1972), pp. 17-27.

[Mac-Harv] C. MACLACHLAN - W. J. HARVEY, *On mapping-class groups and Teichmüller spaces,* Proc. London Math. Soc. (3), **30** (1975), pp. 496-512.

[Nag] S. NAG, *The Complex Analytic Theory of Teichmüller Spaces,* Wiley-Interscience, New York (1988).

[Nar] M. S. NARASIMHAN *et al*, *Riemann Surfaces*, Tata Institute, Bombay (1963).

[Rau] H. E. RAUCH, *Theta Constants on a Riemann Surface with Many Automorphisms*, Symposia Mathematica. Vol. III, Instituto Nazionale di Alta Matematica, Academic Press, New York (1970).