Riemann-Roch space representations from bad hyperelliptic curves: questions and computations[1]

5-27-2005, D. Joyner[2]

Much of this is joint work with Amy Ksir, the rest is "in progress".

1 Motivation

Let $F = \mathbb{C}$ temporarily and let X be a non-singular projective curve of genus > 1 with automorphism group G. This group acts on the vector space of differentials on X and, more generally, on the Riemann-Roch space of a G-equivariant divisor D.

Question: What are these representations? Can we compute their character? Their multiplicities?

For the group action on the differentials, the trace of an individual element can be computed using the Eichler trace formula. For more general character computations, we use the Borne character formula.

1.1 Borne's formula

For any point $P \in X(k)$, let G_P be the decomposition group at P (i.e. the subgroup of G fixing P). Since char k is zero, the quotient $\pi : X \to Y = X/G$ is tamely ramified, and this group G_P is cyclic. G_P acts on the cotangent space of $X(k)$ at P by a k-character. This character is the **ramification character** of X at P.

The **ramification module** is defined by

$$\Gamma_G = \sum_{P \in X(k)_{ram}} Ind_{G_P}^G (\sum_{\ell=1}^{e_P - 1} \ell \psi_P^\ell),$$

[1]Notes for *Idaho Conference on Computational Algebraic Geometry* talk given at Univ. Idaho, 5-27-2005

[2]wdj@usna.edu, Math Dept, USNA

where e_P is the size of the inertia group, and ψ_P is the ramification character at P. By a result of Nakajima, there is a unique G-module $\tilde{\Gamma}_G$ such that

$$\Gamma_G = |G|\tilde{\Gamma}_G.$$

We abuse terminology and also call $\tilde{\Gamma}_G$ the **ramification module**.

Now consider a G-equivariant divisor D on $X(k)$. If $D = \frac{1}{e_P}\sum_{g\in G} g(P)$ then we call D a **reduced orbit**. The reduced orbits generate the group of G-equivariant divisors $Div(X)^G$.

Definition 1 *The* ***equivariant degree*** *is a map from $Div(X)^G$ to the Grothendieck group $R_k(G) = \mathbb{Z}[G_k^*]$ of virtual k-characters of G,*

$$deg_{eq} : Div(X)^G \to R(G),$$

defined by the following conditions:

1. *deg_{eq} is additive on G-equivariant divisors of disjoint support,*
2. *If $D = r\frac{1}{e_P}\sum_{g\in G} g(P)$ is an orbit then*

$$deg_{eq}(D) = \begin{cases} Ind_{G_P}^G(\sum_{\ell=1}^{r}\psi^{-\ell}), & \text{if } r > 0, \\ -Ind_{G_P}^G(\sum_{\ell=0}^{-(r+1)}\psi^{\ell}), & \text{if } r < 0, \\ 0, & r = 0, \end{cases}$$

where $\psi = \psi_P$ is the ramification character of X at P.

Note: In general, this is not additive (except on those divisors which are pull-backs via π).

If $D = \pi^*(D_0)$ is the pull-back of a divisor $D_0 \in Div(Y)$ then $deg_{eq}(D)$ has a very simple form. In this case, r is a multiple of e_P, so the equivariant degree on each orbit is r/e_P times $Ind_{G_P}^G$ of the regular representation of G_P. In this case, we have

$$deg_{eq}(D) = deg(D_0)[k[G]], \tag{1.1}$$

We recall the following formula of Neils Borne [Bo].

Lemma 2 *(***Borne's formula***) If D is a G-equivariant nonspecial divisor, then the (virtual) character of $L(D)$ is given by*

$$[L(D)] = (1 - g_Y)[k[G]] + [deg_{eq}(D)] - [\tilde{\Gamma}_G], \tag{1.2}$$

where Y is the quotient of X by G, g_Y is its genus, $\deg_{eq}(D)$ *is the equivariant degree of D, and $\tilde{\Gamma}_G$ is the ramification module.*

1.2 A multiplicity formula

For each conjugacy class $\gamma_i \in G_*$, pick a cyclic subgroup H_i generated by a $g \in \gamma_i$.

Let ρ denote an irreducible representation of G, let H be a cyclic subgroup, and denote by $n_{\rho,j} = n_{\rho,j}(H) \geq 0$ the integers defined by

$$Res_H(\rho) = \sum_{j=1}^{|H|} n_{\rho,j}\psi^j, \tag{1.3}$$

where ψ is a primitive character of H. Note that $n_{\rho,j} = n_{\rho,j+|H|}$ and

$$\sum_{j=1}^{|H|} n_{\rho,j} = \dim(\rho). \tag{1.4}$$

Recall that $Div(X)^G$ is generated by orbits $r\sum_{g\in G/G_P} g(P)$. If $\mathrm{supp}(D) = \cup_{i=1}^{s}\{g(P_i) \mid g \in G/G_{P_i}\}$, is a disjoint union then we write $\mathrm{supp}(D)/G = \{P_i \mid 1 \leq i \leq s\}$. In this case, we may write D uniquely as

$$D = \sum_{P\in \mathrm{supp}(D)/G} r_P \sum_{g\in G/G_P} g(P),$$

for some $r_P \in \mathbb{Z}$.

Let $L(D)_\rho$ denote the ρ-isotypical component of $L(D)$

Another consequence of Borne's formula is the following formula.

Theorem 3 *([JK1]) Let $F = \mathbb{C}$, $G \subset Aut(X)$, and let D be a G-equivariant nonspecial divisor. Assume all the irreducible characters of G are rational-valued. The multiplicity of an irreducible representation ρ of G in $L(D)$ is given by*

$$\dim(L(D)_\rho) = \dim(\rho)(1-g(X_G)) + \sum_{P\in \mathrm{supp}(D)/G} T_{P,\rho} - \sum_{\ell}(\dim(\rho) - \dim(\rho^{H_\ell}))\frac{R_\ell}{2}, \tag{1.5}$$

where

$$T_{P,\rho} = \begin{cases} \sum_{\ell=1}^{r_P} n_{\rho,\ell}(G_P) = \sum_{\ell=1}^{r_P} \langle \psi_P^{\ell}, \mathrm{Res}_{H_\ell}^G \rho \rangle, & r_P > 0, \\ -\sum_{\ell=0}^{-(r_P+1)} n_{\rho,-\ell}(G_P) = \sum_{\ell=1}^{-(r_P+1)} \langle \psi_P^{-\ell}, \mathrm{Res}_{H_\ell}^G \rho \rangle, & r_P < 0, \end{cases}$$

ρ^{H_ℓ} denotes the restriction of ρ to H_ℓ, $R_\ell = R(H_\ell)$ is the number of branch points with decomposition group conjugate to H_ℓ, and ρ_1, ..., ρ_k denote a complete set of irreducible $\mathbb{Q}[G]$-modules (=irreducible $\mathbb{C}[G]$-modules).

This theorem is false without the rationality criteria ("... all the irreducible characters of G are rational-valued"). Indeed, the paper [JK2] computes explicitly the G-equivariant Riemann-Roch spaces for the modular curves $X(N)$, as $PSL(2, \mathbb{Z}/N\mathbb{Z})$-modules where $N > 5$ is a prime. Even though none of these groups $PSL(2, \mathbb{Z}/N\mathbb{Z})$ have rational characters, in some cases the above multiplicity formula still holds since the "irrational representations" don't occur in the decomposition. In other cases, the multiplicity formula does not hold!

2 Bad curves over finite fields

In general, if C is a curve defined over a field F with finite automorphism group $G = Aut_F(C)$ then we call G **large** if $|G| > |C(F)|$. Obviously F must be finite or else C has only finitely many F-rational points.

Lemma 4 *If G is large then every point of $C(F)$ is ramified for the covering $C \to C/G$.*

Proof: Suppose $P \in C(F)$ is not ramified, so the stabilizer of P, G_P, is trivial. In this case, $|G \cdot P| = |G|/|G_P| = |G|$. But $G \cdot P \subset C(F)$ so $|G \cdot P| \leq |C(F)|$, a contradiction. $\square$

A curve C satisfying this lemma will be called **bad over** F.

Open problem: Find multiplicity formulas for bad curves.

3 A bad hyperelliptic curve

Let $p \geq 3$ be a prime, $F = GF(p)$, and let X denote the curve defined by

$$y^2 = x^p - x.$$

This has genus $\frac{p-1}{2}$ and $p+1$ F-rational points[3]. The automorphism group $\overline{G} = \mathrm{Aut}_F(X)$ is a central 2-fold cover of $G = PSL(2,p)$, we have a short exact sequence,

$$1 \to Z \to \overline{G} \to G \to 1, \tag{3.1}$$

where Z denotes the center of $\overline{G}$ (Z is generated by the hyperelliptic involution). We have $\overline{G} \cong SL(2,p)$, in general[4]. The following transformations are elements of $\overline{G}$:

$$\begin{aligned} \gamma_1 &= \left\{ \begin{array}{c} x \longmapsto x, \\ y \longmapsto -y, \end{array} \right. , \quad \gamma_2 = \gamma_2(a) = \left\{ \begin{array}{c} x \longmapsto a^2 x, \\ y \longmapsto ay, \end{array} \right. \\ \gamma_3 &= \left\{ \begin{array}{c} x \longmapsto x+1, \\ y \longmapsto y, \end{array} \right. , \quad \gamma_4 = \left\{ \begin{array}{c} x \longmapsto -1/x, \\ y \longmapsto y/x^{\frac{p+1}{2}}, \end{array} \right. \end{aligned} \tag{3.2}$$

where $a \in F^\times$ is a primitive $(p-1)^{st}$ root of unity and $Z = \langle \gamma_1 \rangle$. This group acts transitively on $X(F)$, so it has an orbit of size $|X(F)| = p+1$.

Let $P_1 = (1:0:1)$ and let H be its stabilizer in $\overline{G}$. A counting argument shows that H is a solvable group of order $2p(p-1)$ generated by γ_1, $\gamma_2(a)$ and γ_3.

Example 5 *It is known (Proposition VI.4.1, [St]) that, for each $m \geq 1$, the Riemann-Roch space of $D = mP_1$ has a basis consisting of monomials,*

$$x^i y^j, \qquad 0 \leq i \leq p-1,\ j \geq 0,\ 2i + pj \leq m.$$

Observation *The semisimplification ρ_{ss} of the representation ρ of H acting on $L(D)$ is the direct sum of one-dimensional representations of H.*

[3]In the weighted projective model (X, Y, Z) ($x = X/Z$, $y = Y/Z^{g+1}$) with weights 1, $g+1 = \frac{p+1}{2}$, and 1, in which the point at infinity is nonsingular: $Y^2 = X^p Z - XZ^p$. Indeed, say $P \in X(F)$ is not the point at infinity, so $P = (x, y)$, for some $x, y \in F$. By Fermat's Little Theorem, $x^p - x = 0$, so $y = 0$. There are p such points.

[4]When $p \equiv -1 \pmod 4$ one can check $\gamma_4^2 = \gamma_1$, which implies that $G \ncong G_0 \times Z$. When $p \equiv 1 \pmod 4$ one can check $\gamma_2^{\frac{p-1}{2}} = \gamma_1$, which also implies G is not the direct product.

Indeed, the generator γ_1 acts trivially on the basis of $L(D)$, and the other generators act by

$$\gamma_2(a) : \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ a^2 x \\ \vdots \\ a^{2r+s} x^r y^s \end{pmatrix} = \begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & a^2 & ... & \vdots \\ \vdots & \ddots & & 0 \\ 0 & ... & 0 & a^{2r+s} \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix},$$

and

$$\gamma_3 : \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ x+1 \\ \vdots \\ (x+1)^r y^s \end{pmatrix} = \begin{pmatrix} 1 & 0 & ... & 0 \\ 1 & 1 & ... & \vdots \\ \vdots & \ddots & & 0 \\ 0 & ... & r & 1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^r y^s \end{pmatrix},$$

where the non-zero terms in bottom row of the matrix representation of γ_3 are in the last $r+1$ row entries and consist of the binomial coefficients $\frac{r!}{(r-j)!j!}$, $0 \leq j \leq r$. Therefore, the group generated by these matrices is lower-triangular, hence solvable. $\square$

Note every point in

$$X(F) = \{(1:0:0), (0:0:1), (1:0:1), ..., (p-1:0:1)\}$$

is ramified over the covering $X \to X/\overline{G}$ in the sense that each stabilizer $\overline{G}_P = \mathrm{Stab}_{\overline{G}}(P)$ is non-trivial, $P \in X(F)$.

Background on the function field $K = F(X) = F(x, y)$ of this curve from Stichtenoth [St], §VI.4:

(a) $[K : F(y)] = p$, so as an F-vector space

$$F(x, y) = F(y) \oplus xF(y) \oplus ...x^{p-1}F(y).$$

(b) $K/F(y)$ is Galois and

$$\begin{array}{ccc} Gal(K/F(y)) & = & F \\ \sigma & \mapsto & a \\ \sigma(x) = x + a & & \end{array}$$

(c) The pole P_∞ of y in $F(y)$, a place on the projective line $\mathbb{P}^1$, has a unique extension Q_∞, a place of X, which is totally ramified, $e(Q_\infty/P_\infty) = p$. Q_∞ is a place of X of degree 1.

(d) P_∞ is the only place of $\mathbb{P}^1$ which ramifies with respect to the projection map $X \to \mathbb{P}^1$, $(x, y) \longmapsto y$.

(e) $(dy)_\infty = (p-3)Q_\infty$,

(f) $(x)_\infty = 2Q_\infty$, $(y)_\infty = pQ_\infty$.

(g) $L(rQ_\infty) = Span[\ x^i y^j \mid 2i + pj \leq r, 0 \leq i, 0 \leq j \leq p-1\ ]$.

Let

$$D_F = \sum_{P \in X(F)} P,$$

so $\deg(D_F) = |X(F)| = p + 1 = 2g + 2$ and therefore rD_F is non-special for each $r \geq 1$. In particular,

$$\dim L(rD_F) = \deg(rD_F) - g + 1 = r(p+1) - \frac{p+1}{2} + 1 = (2r-1)g + 2r + 1.$$

Taking $r = 1$ for instance, we have $\dim L(D_F) = \frac{p+5}{2}$. Each successive quotient $L((r+1)D_F)/L(rD_F)$ has dimension $p + 1 = 2g$, $r \geq 1$. The vector space $L(rD_F)$ is a $\overline{G}$-module, hence so is each such quotient. Indeed, the hyperelliptic involution acts trivially on $X(F)$, so this action actually factors through an action of G.

Question: Is $L(D_F)$ an irreducible G-module or $\overline{G}$-module? Is $L((r+1)D_F)/L(rD_F)$ an irreducible G-module or $\overline{G}$-module?

Answer: No! No! No! No!

The irreducible $\overline{G}$-modules are known explicitly [Al]. They only occur in degrees 1, 2, ..., p. We denote the degree n $\overline{G}$-module by V_n,

$$V_n = \{\sum_i a_i X^i Y^{n-i-1}\}.$$

Therefore, no $\overline{G}$-module of dimension $p + 1$ can be irreducible. We shall see below that $L(D_F)$ is a reducible $\overline{G}$-module.

The irreducible G-modules are also known explicitly ([BN], §30). Indeed, if n is odd then the $\overline{G}$-module V_n is also an irreducible G-module. (Guess: There are half as many p-regular conjugacy classes of G as there are of $\overline{G}$, so this must be all of them. Prove this...) Therefore, no G-module of dimension $\frac{p+5}{2}$ or $p+1$ can be irreducible.

Now we turn to trying to compute a basis of $L(rD_F)$. Consider the vector space

$$W = \mathrm{Span}\{ \frac{yx^k}{x^p - x} \mid 0 \leq k \leq \frac{p+1}{2}\}.$$

There are $\frac{p+3}{2}$ elements in this spanning set, all of which are linearly independent, so that $\dim W = \frac{p+3}{2}$. It is clear that W remains invariant under the action of γ_1, $\gamma_2(a)$, and γ_3. Note that

$$\gamma_4 : \frac{yx^k}{x^p - x} \longmapsto -\frac{yx^{\frac{p+1}{2}-k}}{x^p - x},$$

so W is indeed a $\overline{G}$-module.

Lemma: $L(D_F) = W \oplus \mathbf{1}$, as $\overline{G}$-modules.

proof: By the above, W is a $\overline{G}$-module. By definition of the Riemann-Roch space, $W \subset L(D_F)$, and $L(D_F)$ contains the constant functions on X. Since D_F is non-special, the Riemann-Roch theorem tells us that $\dim L(D_F) = 1 + \dim W$, and the claimed result follows. $\square$

One might hope that some vector space like

$$W?? = \mathrm{Span}\{ \frac{yx^k}{(x^p - x)^j} \mid 1 \leq j \leq r,\ 0 \leq k \leq (2r-1)p\}$$

might lead to an explicit description of $L(rD_F)$.

Question: What is the character of the representation ρ of $\overline{G}$ on W? What is the decomposition of this representation?

Answer: The first of these seems to have a simple answer. In the basis of W given above, $\gamma_2(a)$ acts diagonally, γ_3 acts by a unipotent upper-triangular matrix (or a lower-triangular one, depending on how the basis is ordered), and γ_4 acts by a signed permutation matrix. Consequently, it is not hard to compute (with $d = \frac{p+1}{2}$)

$$\mathrm{tr}\,\rho(\gamma_2(a)) = \sum_{k=0}^{d} a^{2k-1} = a^{-1}\frac{a^{2d+2}-1}{a^2-1} = a^{-1}\frac{a^{p+3}-1}{a^2-1} = a^{-1}\frac{a^4-1}{a^2-1} = a + a^{-1},$$

$$\operatorname{tr}\rho(\gamma_3) = \deg\,\rho = \frac{p+3}{2}, \qquad \operatorname{tr}\rho(\gamma_4) = 0.$$

What is the character of the representation V_n of $\overline{G}$ at $t = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$? Since t sends (X, Y) to $(aX, a^{-1}Y)$, it follows that t sends X^iY^{n-i-1} to $a^{2i-n+1}X^iY^{n-i-1}$. Therefore, t acts "diagonally" on V_n and the trace is easy to compute:

$$\operatorname{tr} V_n(t) = \sum_{i=0}^{n-1} a^{2i-n} = a^{1-n}\frac{a^{2n}-1}{a^2-1} = \frac{a^n - a^{-n}}{a - a^{-1}},$$

when $n \geq 1$. When $n = 2$ this agrees with $\operatorname{tr}\rho(\gamma_2(a))$. When $n = \frac{p-1}{2}$ this is 0.

In the modular representation case, two representations can have the same character yet not only be inequivalent but have different decompositions. Therefore, it is still unclear what these character formulas definitively say about the decomposition of the semi-simplification of $L(D_F)$. However, they suggest the following decomposition.

Conjecture: $W = V_2 \oplus V_{\frac{p-1}{2}}$.

Example 6 *Let $F = GF(7)$ and let C denote the curves defined by*

$$y^2 = x^7 - x.$$

This has genus 3. The automorphism group G is a central 2-fold cover of $PSL_2(F)$: we have a short exact sequence,

$$1 \to Z \to G \to PSL_2(7) \to 1,$$

where Z denotes the subgroup of G generated by the hyperelliptic involution (which happens to also be the center of G). (Over the algebraic closure $\overline{F}$, $Aut_{\overline{F}}(C)/center \cong PGL_2(\overline{F})$, by [G], Theorem 1.) The following transformations are elements of $Aut_F(C)$:

$$\gamma_1 = \begin{cases} x \longmapsto x, \\ y \longmapsto -y, \end{cases}, \quad \gamma_2 = \begin{cases} x \longmapsto a^2x, \\ y \longmapsto ay, \end{cases} \quad (\ a \in F^\times),$$
$$\gamma_3 = \begin{cases} x \longmapsto x+1, \\ y \longmapsto y, \end{cases}, \qquad \gamma_4 = \begin{cases} x \longmapsto -1/x, \\ y \longmapsto y/x^4, \end{cases}.$$

There are 8 F-rational points:

$$C(F) = \{P_1 = (1:0:0), P_2 = (0:0:1), P_3 = (1:0:1), ..., P_8 = (6:0:1)\}.$$

The automorphism group acts transitively on $C(F)$. Consider the projection $C \to \mathbb{P}^1$ defined by $\phi(x,y) = x$. The map ϕ is ramified at every point in $C(F)$ and at no others.

Let $H_1 = Stab(P_1, G)$ denote the stabilizer of the point at infinity in $C(F)$. All the stabilizers $Stab(P_i, G)$ are conjugate to each other in G, $1 \leq i \leq 8$. The group H_1 is a non-abelian group of order 42 (In fact, the group $H_1/Z(H_1)$ is the non-abelian group of order 21, where $Z(H)$ denotes the center of H.)

It is known (Proposition VI.4.1, [St]) that, for each $m \geq 1$, the Riemann-Roch space $L(mP_1)$ has a basis consisting of monomials,

$$x^i y^j, \qquad 0 \leq i \leq 6,\ j \geq 0,\ 2i + 7j \leq m.$$

Let $D = 5P_1$, $S = C(F) - \{P_1\}$, and let

$$C(D, S) = \{(f(P_2), ..., f(P_8)) \mid f \in L(D)\}.$$

This is a $(7, 3, 5)$ code over F. In fact, $\dim(L(D)) = 3$, so the evaluation map $f \longmapsto (f(P_2), ..., f(P_8))$, $f \in L(D)$, is injective. Since H_1 fixes D and preserves S, it acts on C via

$$g : (f(P_2), ..., f(P_8)) \longmapsto (f(g^{-1}P_2), ..., f(g^{-1}P_8)),$$

for $g \in H_1$.

Let P denote the permutation group of this code. It a group of order 42. However, it is not isomorphic to H_1. In fact, P has trivial center. The (permutation) action of G on this code implies that there is a homomorphism

$$\psi : H_1 \to P.$$

What is the kernel of this map?

GAP will narrow the choices down to two possibilities: either a subgroup of order 6 or a subgroup of order 21 (this is obtained by matching possible orders of quotients H_1/N with possible orders of subgroups of P). Take the automorphisms γ_1, γ_2 with $a = 2$ and γ_3. If we identify $S = \{P_2, ..., P_8\}$ with $\{1, 2, ..., 7\}$ then

$$\gamma_1 \leftrightarrow (2,7)(3,6)(4,5) = g_1,$$

$$\gamma_2 \leftrightarrow (2,5,3)(4,6,7) = g_2,$$
$$\gamma_3 \leftrightarrow (1,2,...7) = g_3.$$

The group $N = \langle g_2, g_3 \rangle$ *is a non-abelian normal subgroup of* $H_1 = \langle g_1, g_2, g_3 \rangle$ *of order* 21.

The character table (over $\mathbb{C}$*) of* N *is (both in GAP and MAGMA)*

Class	*1*	*2*	*3*	*4*	*5*
Size	*1*	*7*	*7*	*3*	*3*
Order	*1*	*3*	*3*	*7*	*7*
$p = 7$	*1*	*2*	*3*	*1*	*1*
χ_1	*1*	*1*	*1*	*1*	*1*
χ_2	*1*	ω	$-1-\omega$	*1*	*1*
χ_3	*1*	$-1-\omega$	ω	*1*	*1*
χ_4	*3*	*0*	*0*	ζ	ζ^3
χ_5	*3*	*0*	*0*	ζ^3	ζ

where ω *denotes a cube root of unity and* $\zeta \neq 0$ *is a root of unity which will be unimportant for our example. Accoding to GAP, the character table (over* F*) of* N *is*

χ_{1a}	*1*	*1*	*1*	*1*	*1*
χ_{1b}	*1*	ω^2	ω	*1*	*1*
χ_{1c}	*1*	ω	ω^2	*1*	*1*

where the ordering on the conjugacy classes is the same. Note that the last two conjuacy classes are irregular mod 7.

Finally, we compute the matrix representation of H_1 *on* $L(D)$*, where* $D = 5P_1$*. First, note that* γ_1 *acts as the identity,*

$$\gamma_2 : \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ 4x \\ 2x^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix},$$

and

$$\gamma_3 : \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \longmapsto \begin{pmatrix} 1 \\ x+1 \\ (x+1)^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix}.$$

In fact, every element of N may be written $g_2^i g_3^j$, $0 \le i \le 2$, $0 \le j \le 6$. The conjugacy classes of N are represented by $1, a, a^2, b, b^3$. The matrices of the representation ρ of H_1 acting on $L(D)$ are

$$\rho(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \rho(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \rho(a^2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix},$$
$$\rho(b) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \quad \rho(b^3) = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 2 & 6 & 1 \end{pmatrix}.$$

This is not a semisimple representation, but it is solvable. In particular, H_1 is solvable.

The character table of N implies that the the semisimplification ρ_{ss} is the direct sum of the three one-dimensional representations: $\mathrm{tr}\rho_{ss} = \chi_{1a} + \chi_{1b} + \chi_{1c}$.

References

[Al] J. Alperin, **Local representation theory** Cambridge Univ. Press, 1986.

[Bo] N. Borne, "Une formule de Riemann-Roch equivariante pour des courbes," Can. J. Math. **55**(2003)693-710. (See also his PhD thesis, Univ. Bordeaux, 1999. Available on the web at `http://www.dm.unibo.it/~borne/`)

[BN] Brauer and Nesbitt, *On the modular characters of groups*, Ann. of Math. 42(1941)556-590.

[Gap] The GAP Group, **GAP – Groups, Algorithms, and Programming, Version 4.3**; 2002, (`http://www.gap-system.org`).

[G] N. Göb, "Computing the Automorphism Groups of Hyperelliptic Function Fields," available at `http://front.math.ucdavis.edu/math.NT/0305284`.

[JK1] D. Joyner and A. Ksir, "Decomposing representations of finite groups on Riemann-Roch spaces," preprint, 2004 (submitted to PAMS)

[JK2] ——, *Modular representations on some Riemann-Roch spaces of modular curves X(N)*, in **Computational Aspects of Algebraic Curves**, (Editor: T. Shaska) Lecture Notes in Computing, WorldScientific, 2005.

[St] H. Stichtenoth, **Algebraic function fields and codes**, Springer-Verlag, 1993.