TSUKUBA J. MATH.
Vol. 11 No. 2 (1987). 287—301

ON THE ACTION OF AUTOMORPHISMS OF A CURVE ON THE FIRST l-ADIC COHOMOLOGY

by

Izumi KURIBAYASHI and Fumiyuki MOMOSE

Introduction

Let $G=\langle\sigma\rangle$ be a cyclic group with $n=\# G>1$. For each divisor d of n, let χ_d denote the character of G of the irreducible representation over $\boldsymbol{Q}$, the field of rational numbers, whose kernel is equal to $\langle\sigma^d\rangle$. Let k be an algebraically closed ground field and X be a complete non-singular curve over k of genus $g\geqq 2$. The main purpose of the present paper is to prove the following theorems, under the assumption that $G\subseteqq \mathrm{Aut}(X)$, the automorphism group of X; in this situation we denote by $\mathrm{Tr}(G|H^1(X,\boldsymbol{Q}_l))$ the character of the natural representation of G on the first l-adic cohomology $H^1(X,\boldsymbol{Q}_l)$ of X, where l is any prime number different from the characteristic of k (cf. Notation, § 2 and also [4]):

THEOREM I. *Assume that* $Tr(G|H^1(X,\boldsymbol{Q}_l))=\sum_{d|n} a_d\chi_d$, where the symbol $\sum_{d|n}$ stands for the summation over all divisors d of n. *Then*

(a) *For divisors d, e of n with $d|e$, we have*

$$a_e\geqq\begin{cases}a_d & \text{if } d\neq 1,\\ a_d-2 & \text{if } d=1.\end{cases}$$

(b) *If we put*

$$\alpha_e=\begin{cases}-e\sum_{f|n/e} a_{ef}\mu(f) & \text{for } e|n, e\neq 1, n,\\ 2-\sum_{f|n} a_f\mu(f) & \text{for } e=1.\end{cases}$$

then $\alpha_e\geqq 0$, *where* $\mu(\ )$ *denotes the Möbius function.*

THEOREM II. $n\leqq 4g+2$. *Moreover, if* $n\neq 4g+2$ *then* $n\leqq 4g$.

Our proofs of Theorem II and Theorem I (a) are essentially due to the fact that the rational character $Tr(G|H^1(X,\boldsymbol{Q}_l))$ has the property described in Theorem I (b). And so, in the large part of this paper we are devoted to the investigation of the rational characters having such a property. Concerning Theorem I, we note that α_e equals to the cardinality of the set

$$\{P\in X|\sigma^e(P)=P, \sigma^f(P)\neq P \quad for \quad f|e, f\neq e\},$$

Received October 8, 1986.

in the case where $k=\boldsymbol{C}$, the field of complex numbers, (cf. Lemma 2.4). Theorem II has been proved by Wiman [10] (cf. [2]) in the case where $k=\boldsymbol{C}$ (cf. also, [9]). We shall see that the bound $4g+2$ (resp. $4g$) is attained by an automorphism of a curve over k of genus g if and only if $p\nmid 4g+2$ or $p=2$ or $p=2g+1$ (resp. $p\nmid 4g$ or "$p\neq 2$, $g=3$"), where p denotes the characteristic of k (cf. Remark 3.3).

We give a brief survey of this paper. In § 1, we provide the "Riemann-Hurwitz relation" and a lemma asserting that our property is preserved for induced characters. We shall use them as basic tools for our proofs. In § 2, we prove (b) of Theorem I by using the Lefschetz formula, and deduce the inequalities in (a) from the property. In § 3, we prove Theorem II and moreover determine the structure of the character $Tr(G|X^1(X, \boldsymbol{Q}_l))$ in the extremal cases. In § 4, as applicasions we shall obtain some results concerning the action of automorphisms on the space $H^0(X, \Omega_X)$ of 1-canonical forms. Especially we shall prove the following proposition as an interpretation (of the rational–character-case) of the existence theorem in [3].

PROPOSITION III. *Let χ be a rational character of G of degree ≥ 2. Then the following conditions are equivalent.*

(i) *χ is realizable, i.e., $\chi=Tr(G|H^0(X, \Omega_X))$ with $G\subseteqq Aut(X)$ for some compact Riemann surface X.*

(ii) *The α_e's ($e|n$, $e\neq n$) defined (as above) for the character 2χ have the property: $\alpha_e\geq 0$.*

NOTATION In this paper, let $G=\langle\sigma\rangle, n, \chi_d$ $(d|n)$, k and l have the meaning described in Introduction, where for integers m and m', if m divides m', we denote $m|m'$ as usual. The symbols $\mu(\ )$ and $\phi(\ )$ denote the Möbius function and the Euler function, respectively. For a finite set U we denote by $\sharp U$ the cardinality of U.

For $\lambda=\sum_{d|n} a_d\chi_d\in R_{\boldsymbol{Q}}(G)$, the group generated by the characters of the representations of G over $\boldsymbol{Q}$ (cf. [7]), we define:

$$(*)\quad \alpha_e=\alpha_e^{(\lambda)}=2\delta_{e,1}-e\sum_{f|n/e} a_{ef}\mu(f) \qquad for\quad e|n,\ e\neq n,$$

where $\delta_{t,s}$ denotes the Kronecker's delta, *i.e.*, $\delta_{t,s}=1$ (resp. $=0$) *if* $t=s$ (resp. $t\neq s$). We note that the χ_d form an orthogonal basis of $R_{\boldsymbol{Q}}(G)$ (cf. *e.g.*, [7, p. 104]).

§ 1. Preliminary

First of all we explain a characterization of the α_e for the later use.

LEMMA 1.1. *Let* $\lambda=\sum_{d|n} a_d\chi_d\in R_{\boldsymbol{Q}}(G)$. *Then*

$$\lambda(\sigma^e)=2-\sum_{f|e}\alpha_f \qquad \textit{for} \quad e|n,\ e\neq n.$$

PROOF. Since $S_d(\zeta_d^e)=[\boldsymbol{Q}(\zeta_d):\boldsymbol{Q}(\zeta_{d/(e,d)})]\cdot S_{d/(e,d)}(\zeta_{d/(e,d)})$, where ζ_m donotes exe $(2\pi\sqrt{-1}/\mathrm{m})$ and $S_m:\boldsymbol{Q}(\zeta_m)\to\boldsymbol{Q}$ the trace form, we have that

$$(1) \qquad \chi_d(\sigma^e)=S_d(\zeta_d^e)=\mu(d/(e,d))\phi(d)/\phi(d/(e,d)) = \sum_{f|(e,d)} f\mu(d/f)$$

for $d|n$, $e\in\boldsymbol{Z}$. To see the last equality, we may assume that $e|d$. Then we put and let as follows:

$$e=e'\cdot\prod p_i^{r_i} \text{ with } p_i\nmid e' \text{ and } \prod p_i^{r_i}=e_0;$$

$$\hat{e}=d/e=\hat{e}'\prod p_i^{\hat{r}_i} \text{ with } p_i\nmid\hat{e}' \text{ and } \prod p_i^{\hat{r}_i}=\hat{e}_0,$$

where $\{p_i\}$ denotes the set of common prime divisors of e and $\hat{e}$. Since the functions $\mu(\ )$ and $\phi(\ )$ are multiplicative, noting that $\phi(e_0\hat{e}_0)=e_0\hat{e}_0\prod(1-1/p_i)$ $=e_0\phi(\hat{e}_0)$, we have

$$\begin{aligned}\sum_{f|e} f\mu(d/f) &= \sum_{f'|e'}\sum_{f_0|e_0} f'f_0\mu(e'/f')\mu(e_0\hat{e}_0/f_0)\mu(\hat{e}')\\ &= e_0\mu(\hat{e}')\mu(\hat{e}_0)\sum_{f'|e'} f'\mu(e'/f')\\ &= e_0\mu(\hat{e}')\mu(\hat{e}_0)\phi(e')\\ &= \mu(\hat{e})\phi(e')\phi(e_0\hat{e}_0)/\phi(\hat{e}_0)\\ &= \mu(d/e)\phi(d)/\phi(d/e),\end{aligned}$$

as desired.

From (1) it follows that

$$\begin{aligned}\lambda(\sigma^e) &= \sum_{d|n} a_d \sum_{f|(e,d)} f\mu(d/f)\\ &= \sum_{f|e} f\{\sum_{g|n/f} a_{fg}\mu(g)\}\\ &= 2-\{2-\sum_{g|n} a_g\mu(g)-\sum_{\substack{f|e\\ f\neq 1}} f\sum_{g|n/f} a_{fg}\mu(g)\}\\ &= 2-\sum_{f|e}\alpha_f.\end{aligned}$$

Q. E. D.

Next, to state our basic technical lemmas bolow concerning the induced virtual characters, we fix some notations.

Notation. Let $d|n$, $d\neq 1$ and put $\bar{G}^{(d)}=G/\langle\sigma^d\rangle$. For $e|d$, the mapping: $\bar{G}^{(d)}\to\boldsymbol{Q}$ defined by $(\tau \bmod \langle\sigma^d\rangle)\mapsto\chi_e(\tau)$ is the character of the irreducible representation over $\boldsymbol{Q}$ whose kernel is equal to $\langle(\sigma \bmod \langle\sigma^d\rangle)^e\rangle$. We denote this mapping χ_e, too. For $\lambda=\sum_{e|n} a_e\chi_e\in R_{\boldsymbol{Q}}(G)$, let $\bar{\lambda}^{(d)}$ denote its induced virtual character of $\bar{G}^{(d)}$

(via the natural homomorphism: $G\to\bar{G}^{(d)}$) and $\bar{\alpha}_e^{(d)}$ $(e|d,\ e\neq d)$ the α_e for $\bar{\lambda}^{(d)}\in R_{\mathbf{Q}}(\bar{G}^{(d)})$.

We note that

$$(2)\qquad \bar{\lambda}^{(d)}=\sum_{e|d} a_e\chi_e \quad ;\text{ and}$$

$$(3)\qquad \bar{\alpha}_e^{(d)}=2\delta_{e,1}-e\sum_{f|d/e} a_{ef}\mu(f).$$

Now we consider the "Rimann-Hurwitz relation" (cf. [3, § 4]).

LEMMA 1.2. *Let $\lambda\in R_{\mathbf{Q}}(G)$. For a divisor d of n with $d\neq n$, we have:*

$$\lambda(1)-2=d(\bar{\lambda}^{(n/d)}(1)-2)+\sum_{\substack{e|n\\ e\neq n}}\alpha_e((n/e,d)-1).$$

PROOF. From $\bar{\lambda}^{(n/d)}(1)=(1/d)\sum_{u=1}^{d}\lambda(\sigma^{un/d})$ it follows that

$$\begin{aligned}\lambda(1)-2&=d(\bar{\lambda}^{(n/d)}(1)-2)+\sum_{u=1}^{d-1}\{2-\lambda(\sigma^{un/d})\}\\ &=d(\bar{\lambda}^{(n/d)}(1)-2)+\sum_{\substack{f|d\\ f\neq 1}}\phi(f)\sum_{e|n/f}\alpha_e\\ &=d(\bar{\lambda}^{(n/d)}(1)-2)+\sum_{\substack{e|n\\ e\neq n}}\alpha_e\{\sum_{\substack{f|(n/e,d)\\ f\neq 1}}\phi(f)\}\\ &=d(\bar{\lambda}^{(n/d)}(1)-2)+\sum_{\substack{e|n\\ e\neq n}}\alpha_e((n/e,d)-1).\end{aligned}$$

Q. E. D.

Finally we prove the following:

LEMMA 1.3. *Let $\lambda=\sum_{f|n} a_f\chi_f\in R_{\mathbf{Q}}(G)$. If $\alpha_f^{(\lambda)}\geqq 0$ for all $f|n$ with $f\neq n$, then $\alpha_e^{(d)}\geqq 0$ $(e|d, e\neq d)$ for each $d|n$, $d\neq 1$.*

PROOF. First we see by (2) that

if $n'|n$, $d|n'$ with $d\neq 1$, then the induced virtual character of $\bar{\lambda}^{(n')}$ via the natural homomorphism: $G/\langle\sigma^{n'}\rangle\to G/\langle\sigma^d\rangle$ is equal to $\bar{\lambda}^{(d)}$.

Thus, by applying (to $\bar{\lambda}^{(n/p)}$) the induction on the number of divisors of n, we see that it suffices to show the lemma only for $d=n/p$ with a prime number p.

To prove the lemma in this case, assume $n=p^r m$ and $e=p^s m'$ with $p\nmid m$, $p\nmid m'$, and $e|d$, $e\neq d$. Then we have by (*) that

$$\alpha_e=2\delta_{e,1}-e\{\sum_{f|n/pe} a_{ef}\mu(f)+\sum_{f|m/m'} a_{efp^{r-s}}\mu(fp^{r-s})\}.$$

Combining this and (3), we get

$$\bar{\alpha}_e^{(n/p)}\begin{cases}\alpha_e & \text{if } r-s\geqq 2,\\ \alpha_e+\alpha_{pe}/p & \text{if } r-s=1.\end{cases}$$

This completes the proof by our assumption on α_e's.

§ 2. Proof of Theorem I

First we prove (a) of Theorem I, assuming (b). For our purpose it suffices to show the following:

PROPOSITION 2.1. *Let* $\lambda=\sum_{f|n} a_f\chi_f\in R_{\boldsymbol{Q}}(G)$. *If* $\alpha_f\geqq 0$ *for all* $f|n$ *with* $f\neq n$, *then for each divisor* e *of* n *we have that*

$$a_e \geqq a_d-2\cdot\delta_{d,1} \qquad \textit{for} \quad d|e.$$

PROOF. Put $b_f=a_f-2\cdot\delta_{f,1}$ for $f|n$. Then we have

$$\sum_{f|n/e} \mathrm{b}_{ef}\mu(f)=-\alpha_e/e \quad \text{for } e|n,\ e\neq n.$$

Hence, by our assumption on the α_e, it suffices to show the following:

LEMMA 2.2. *Let* n *be an integer* >1 *and let* $b_f\in\boldsymbol{Q}$ *for* $f|n$. *Assume that tne inequality*

$$\sum_{f|n/e} b_{ef}\mu(f)\leqq 0$$

holds for each $e|n$, $e\neq n$. *Then* $b_e\geqq b_d$ *for all divisors* e, d *of* n *with* $d|e$.

PROOF of LEMMA 2.2. By induction on the number of divisors of n, we may assume that

$b_d\leqq b_e$ holds for $e|n$, $d|e$ with $d\neq 1$.

In fact, if $b_f^{(n/d)}$ denotes b_{df} for $f|n/d$, then

$b_1^{(n/d)}=b_d$, $b_{e/d}^{(n/d)}=b_e$; and

$$\sum_{f|n/de'} b_{e'f}^{(n/d)}\mu(f)\leqq 0 \qquad (e'|n/d,\ e'\neq n/d),$$

for $e|n$, $d|e$ with $d\neq 1$. There remains to show that

$b_1\leqq b_p$ for each prime divisor p of n.

To see this, we use the assumption:

$$\begin{aligned} 0 &\geqq \sum_{\substack{e|n\\ p\nmid e}} \sum_{f|n/e} b_{ef}\mu(f)=\sum_{d|n} b_d \sum_{\substack{f|d\\ p\nmid d/f}} \mu(f) \\ &=\sum_{\substack{d|n\\ p\nmid d}} b_d\sum_{f|d}\mu(f)-\sum_{\substack{d|n\\ p\| d}} b_d \sum_{f|d/p}\mu(f) \\ &=b_1-b_p. \end{aligned}$$

This completes the proof of Lemma 2.2 and hence of Proposition 2.1.

Throughout the rest of this section we work under the assumption and notation in Theorem I, except for Corollary 2.5. In particular we assume that $G \subseteqq \mathrm{Aut}(X)$. We put:

$$\lambda = Tr(G|H^1(X, \mathbf{Q}_l)), \quad G_P = \{\tau \in G | \tau(P) = P\} \qquad for \quad P \in X.$$

For any $\tau \in G_P$, $\tau \neq 1$, we define $i_P(\tau)$ to be the order of the zero of $\tau^*(\pi) - \pi$ at P, where π is a local uniformizing parameter at P. From the Lefschetz formula (cf. [4], V § 2; [8] VI § 4) we have the following:

LEMMA 2.3. $\lambda(\tau) = 2 - \sum_{\substack{P \in X \\ \tau \in G_P}} i_P(\tau) \qquad for \quad \tau \neq 1.$

Hence, in particular, the character λ is integer-valued, whence it follows that $\lambda \in R_{\mathbf{Q}}(G)$ (cf. [7, p. 93]).

Next we shall prove (b). Here we fix some notation: let $n = p^r m$ with $(p, m) = 1$, where p denotes the characteristic of k ($n = m$ for $p = 0$); we denote by F_f ($f|n$, $f \neq n$) the set of the fixed points of σ^f.

Before giving a proof to (b), we consider its special case:

LEMMA 2.4. *For a divisor e of n with $m \nmid e$, we have*

$$\alpha_e = \#\{P \in X | \sigma^e(P) = P, \ \sigma^f(P) \neq P \quad \text{for } f|e, \ f \neq e\}.$$

PROOF. From Lemma 1.1 and Lemma 2.3 it follows that

(1) $\sum_{f|d} \alpha_f = \sum_{P \in F_d} i_P(\sigma^d)$ (for each $d|n$, $d \neq n$).

On the other hand, by the assumption on e we have that

$$i_P(\sigma^e) = 1 \qquad \text{for} \quad P \in F_e.$$

Hence, by induction on the number of divisors of e we obtain our lemma.

Thus, to prove (b) we may assume that $p > 0$, $e = p^s m$ with $0 \leqq s < r$. Then we have that

$$\begin{aligned} \alpha_e &= \sum_{d|m} \alpha_{p^s d} - \sum_{\substack{d|m \\ d \neq m}} \alpha_{p^s d} \\ &\geqq \{\sum_{f|e} \alpha_f - \sum_{f|e/p} \alpha_f\} - \#F_e && \text{(by Lemma 2.4)} \\ &= \sum_{P \in F_e} i_P(\sigma^e) - \sum_{P \in F_{e/p}} i_P(\sigma^{e/p}) - \#F_e && \text{(by (1))} \\ &= \sum_{P \in F_{e/p}} \{i_P(\sigma^e) - i_P(\sigma^{e/p}) - 1\} + \sum_{\substack{P \in F_e \\ P \notin F_{e/p}}} \{i_P(\sigma^e) - 1\}. \end{aligned}$$

On the other hand, it is easy to see that

(2) if $P \in F_{e/p}$ then $i_P(\sigma^e) \geqq i_P(\sigma^{e/p}) + 1$; and

(3) if $P \in F_e$ then $i_P(\sigma^e) \geqq 2$ (by our assumption on e).

These complete the proof of (b) and hence of Theorem I.

It is well-known that the character $\mathrm{Tr}(\mathrm{Aut}(X)|H^1(X, \boldsymbol{Q}_l))$ is faithful (cf. *e. g.*, [6] and [5, p. 176]). Theorem I provides another proof of this fact. In fact, by proposition 2. 1 we moreover have the following:

COROLLARY 2. 5. *Assume that* $\lambda=\sum_{d|n} a_d\chi_d \in R_{\boldsymbol{Q}}(G)$ *is a character such that* $\alpha_e \geqq 0$ *for all* $e|n$, $e \neq n$. *If* $\lambda \neq \chi_1$, $2\chi_1$ *(in particular, if the degree* $\lambda(1)>2$*) then* λ *is faithful (i. e.,* $a_n \geqq 1$*) and hence* $\lambda(1) \geqq a_n\phi(n) \geqq \phi(n)$.

§ 3. Proof of Theorem II

Since the demension of the space $H^1(X, \boldsymbol{Q}_l)$ is $2g\,(>2)$, to prove Theorem II it suffices by Corollary 2. 5 and Theorem I to show the following:

PROPOSITION 3. 1. *Assume that* $\lambda=\sum_{d|n} a_d\chi_d \in R_{\boldsymbol{Q}}(\mathrm{G})$ *is a faithful character such that* $\alpha_e \geqq 0$ *for all* $e|n$, $e \neq n$. *Denote by* h $(\geqq 1)$ *the degree of* λ. *Then*

$$n=2h+2 \quad \text{or} \quad n \leqq 2h.$$

If $n=2h+2$ *then*

$$\lambda=\sum_{\substack{d|n/2\\ d\neq 1}} \chi_{2d} \qquad \text{with} \quad 2|h.$$

If $n=2h$ *then*

(i) $\lambda=\sum_{d|m} \chi_{2^r d}$ *with* $n=2^r m$ $(r \geqq 1)$, $(2, m)=1$;

(ii) $\lambda=\chi_1+\sum_{\substack{d|h\\ d\neq 1}} \chi_{2d}$ *with* $(2, h)=1$, $h>1$; *or*

(iii) $\lambda=\chi_6+\chi_{12}$.

PROOF. First we prove the proposition for a special type of λ, which serves also as the first step of our induction (cf. the final part of the proof). In fact, now we assume that

(1) $\lambda=a_1\chi_1+a_n\chi_n$.

Then we have by the definition (*) that

$$\alpha_e=-ea_n\mu(n/e) \qquad \text{for} \quad e|n, \ e\neq 1, \ n.$$

For a prime factor p of n, this implies

$$\mu(n/pf) \leqq 0 \qquad \text{for} \ f|n/p \ \text{with} \ f \neq n/p.$$

Hence $n/p=q^{r-1}$ $(r \geqq 1)$ for some prime number q. We estimate n by $h=a_1+a_n\phi(n)$ in the following two cases. In the case where $q=p$, we have that

$$n=\phi(n)p/(p-1)=(h-a_1)p/(p-1)a_n \leqq 2h.$$

and that $\lambda=\chi_2^r$ whenever $n=2h$. In the case where $q\neq p$, we have $n=pq$ (here we may assume $p<q$). Then

$$n=pq\leqq pq+(p-2)(q-2)=2\phi(n)+2=(2h-2a_1)/a_n+2.$$

Hence we have that $n=2h+2$ or $n\leqq 2h$, and that $\lambda=\chi_{2q}$ (resp. $\lambda=\chi_1+\chi_{2q}$) whenever $n=2h+2$ (resp. $n=2h$).

Let n decompose into a product of coprime integers u and m having the property:

for each prime divisor p of n, $a_{n/p}=0$ if and only if $p|u$.

By the above consideration we may assume (for the rest of the proof) that

λ is not of the form in (1).

Then we note that

(2) $m\neq 1$, $n=um$ is not a prime number and $h\geqq a_n\phi(n)>1$.

In fact, if $m=1$ then $a_d=0$ for any $d|n$ with $d\neq 1, n$ by Proposition 2.1.

Next we prove our proposition under an additional condition:

(3) for any prime divisor p of m, $\sum_{d|n/p}\alpha_d\leqq 3$.

We shall examine the following three cases:

Case (a) $u=1$;

Case (b) $u\neq 1$ and $\alpha_{ud}=0$ for each $d|m$, $d\neq m$;

Case (c) $u\neq 1$ and $\alpha_{uf}\neq 0$ for some $f|m$, $f\neq m$.

Proof in Case (a). Since $d|\alpha_d$, from our condition (3) (with $m=n$) it follows that

(4) if $\alpha_d\neq 0$ (where $d|n$, $d\neq n$) then "$d=1$ with $\alpha_1\leqq 3$", "$d=2$ with $\alpha_2=2$, $\alpha_1\leqq 1$" or "$d=3$ with $\alpha_3=3$, $\alpha_1=0$",

and that

(5) $\alpha_2=2$, $\alpha_3=3$ only when $n=6$.

To estimate n by $h=\lambda(1)$, we use the relation:

(6) $$\phi(n)\cdot a_n=\langle\lambda,\chi_n\rangle=(1/n)\{\sum_{\substack{\tau\in G\\ \tau\neq 1}}\lambda(\tau)\chi_n(\tau^{-1})+\phi(n)\cdot h\}.$$

by (4) and Lemma 1.1, we see that

$$\sum_{\substack{\tau\in G\\ \tau\neq 1}}\lambda(\tau)\chi_n(\tau^{-1})=\sum_{\substack{1\leqq i\leqq 3\\ i|n}}(2\cdot\delta_{i,1}-\alpha_i)\sum_{\substack{\tau\in G\\ \tau\neq 1,\ \#\langle\tau\rangle|n/i}}\chi_n(\tau)$$
$$=\phi(n)\{\alpha_1+\alpha_2+\alpha_3-2\}.$$

Hence we have by (6) that

$$n\leqq a_n\cdot n=h-2+\alpha_1+\alpha_2+\alpha_3.$$

Thus, we obtain by (4) and (5) that

$$n\leqq h+1<2h \quad \text{or} \quad n/2=3\leqq 6a_n-3=h.$$

We now consider the case where $n=2h$. Then we have that $n=6$, $h=3$, $\alpha_1=0$, $\alpha_2=2$ and $\alpha_3=3$ and hence that $\lambda=\chi_1+\chi_6$. But this type of λ is avoided in our case.

To consider Case (b) or Case (c), here we note that

(7) if $u\neq 1$ then $\lambda=a_1\chi_1+\sum_{d|m} a_{ud}\,\chi_{ud}$.

In fact, for a prime divisor p of u we have by Proposition 2.1 that $a_e=0$ whenever $e|n/p$, $e\neq 1$.

Proof in Case (b). From (7) it follows that for any $f|u$, $f\neq u$,

$$0\leqq\alpha_{fm}=-fm\sum_{e|n/fm} a_{fme}\,\mu(e)=-fm\,a_n\,\mu(u/f).$$

Thus $u=p^r$ $(r\geqq 1)$ for some prime number p. On the other hand, using the induction on the number of divisors of m/d, we see by the condition of our case and the definition (*) that $a_{ud}=a_n$ for $d|m$. These imply (note (2)) that

(8) $\alpha_d=(2-a_1)\delta_{d,1}+da_n\cdot\delta_{d,n/p}$ for $d|n$, $d\neq n$.

In fact, by (7) we have

$$\begin{aligned}\alpha_d&=2\cdot\delta_{d,1}-d\sum_{f|n/d} a_{df}\,\mu(f)\\&=(2-a_1)\delta_{d,1}-da_n\cdot\mu(u/(d,u))\sum_{f|m/(d,m)}\mu(f)\\&=(2-a_1)\cdot\delta_{d,1}+da_n\cdot\delta_{d,n/p}.\end{aligned}$$

From (8) and Lemma 1.1 it follows that

$$\lambda(\sigma^d)=2-\sum_{e|d}\alpha_e=a_1-da_n\cdot\delta_{d,n/p}\qquad\text{for}\quad d|n,\ d\neq n,$$

and hence that

$$\sum_{\substack{\tau\in G\\ \tau\neq 1}}\lambda(\tau)\chi_n(\tau^{-1})=a_1\sum_{\substack{\tau\in G\\ \tau\neq 1}}\chi_n(\tau)-a_n\cdot n/p\sum_{\substack{\tau\in G\\ \#\langle\tau\rangle=p}}\chi_n(\tau)=\phi(n)\{-a_1+a_n\cdot n/p\}.$$

By (6) this implies that

$$n\leqq a_n\cdot n=(h-a_1)p/(p-1)\leqq 2h.$$

If $n=2h$, then we have that

$$\lambda=\sum_{d|m}\chi_{2^r d}\qquad\text{with}\quad n=2^r m\quad (r\geqq 1),\ (2,m)=1.$$

Proof in Case (c). As before (cf. (4)), from (3) and the condition of our case it follows that

(9) $\alpha_u=u=2$ or 3 and $\alpha_{ud}=0$ for all $d|m$, $d\neq 1$, m.

Using the induction on the number of divisors of m/d as in Case (b), we see by (9) that $a_{ud}=a_n-1\cdot\delta_{d,1}$ for $d|m$. Hence we have by (7) that

(10) $\lambda=a_1\chi_1-\chi_u+a_n\cdot\sum_{d|m}\chi_{ud}$.

Now we consider the case where $u=2$. Then, by (10) we see that

$h=a_1-\phi(2)+a_n\phi(2)m$ and that

$$n\leqq a_n n=2h+2-2a_1, \quad =2h+2 \quad \text{or} \quad \leqq 2h.$$

If $n=2h+2$ then

$$\lambda=\sum_{\substack{d|n/2\\ d\neq 1}}\chi_{2d} \qquad \text{with} \quad 2|h.$$

If $n=2h$ then

$$\lambda=\chi_1+\sum_{\substack{d|n/2\\ d\neq 1}}\chi_{2d} \qquad \text{with} \quad 2\nmid h,\ h>1.$$

Next we consider the case where $u=3$. Then, by (10) we see

$$m\leqq a_n\cdot m=(h-a_1)/2+1\leqq h/2+1.$$

If $h\geqq 6$, then $n=3m\leqq 2h$, and $\lambda=\chi_6+\chi_{12}$ with $n=12$ whenever $n=2h$. (We note that $m=4$ and $\sum_{d|n/2}\alpha_d=4>3$ for $\lambda=\chi_6+\chi_{12}$). If $h=5$ or 4, then $n=3m=6<2h$, since $3\nmid m$ and $m\neq 1$. If $h=3$ (resp. $=2$), then $n=3m=6$ and $\lambda=\chi_1+\chi_6$ (resp. $=\chi_6$). (We note that $m=1$ for $\lambda=\chi_1+\chi_6$ or χ_6).

It remains to show the proposition under the condition:

(11) there is a prime divisor p of m such that $\sum_{d|n/p}\alpha_d\geqq 4$.

For each prime divisor q of n, put

$$\gamma_q=\sum_{d|n/q}\alpha_d \quad \text{and} \quad h_q=\bar{\lambda}^{(n/q)}(1).$$

Then, Lemma 1.2 yields the relation:

(12) $h-2=q(h_q-2)+\gamma_q(q-1)$.

Applying the induction on the number of divisors of n in Proposition 3.1 (cf. (1) for the first step) to the faithful character (note $a_{n/p}\neq 0$ by the choice of p)

(13) $\bar{\lambda}^{(n/p)}=\sum_{e|n/p}a_e\chi_e$

(cf. also, Lemma 1.3) in lieu of λ, we obtain that $n/p\leqq 2h_p+2$ and hence by (12) and (11) that

$$n\leqq 2h+2+2(3-\gamma_p)(p-1)\leqq 2h.$$

We now consider the case where $n=2h$. Then $p=2$, $\gamma_p=4$, $n/p=2h_p+2$. Hence, applying an induction on the number of divisors of n (cf. (1) for the fist step) to our faithful character (13) (with $p=2$) as above, we obtain that $n/4=(n/p)/2$ is an odd integer >1 and that

(14) $\bar{\lambda}^{(n/2)}=\sum_{\substack{d|n/4\\ d\neq 1}}\chi_{2d}.$

We wish to show that $n/4$ is a prime number, so suppose either (15) or (16) below:

(15) $n/4=q^r$ $(r\geqq 2)$ with $q=3$.

(16) There is a prime factor $q>3$ of $n/4$ with $n\neq 4q$.

Since $\gamma_2=4$, we have

$$\sum_{d|n/2}\alpha_d=\alpha_1,\ \alpha_1+\alpha_2,\ \alpha_1+\alpha_3 \quad \text{or} \quad \alpha_2.$$

Thus, by (15) or (16) we get

(17) $\gamma_q=\sum_{d|n/q}\alpha_d \geqq \sum_{d|n/2q}\alpha_d = \sum_{d|n/2}\alpha_d = 4.$

On the other hand, we note by Proposition 2. 1 and (14) that

$$a_{n/q}\geqq a_{n/2q}=\phi(n/2)^{-1}\langle\bar{\lambda}^{(n/2)},\chi_{2\cdot n/4q}\rangle=1.$$

Applying the above argument to the faithful character $\bar{\lambda}^{(n/q)}$, we get $n/q\leqq 2h_q+2$ and hence by (17) that

$$n\leqq 2h+2+2(3-\gamma_q)(q-1)\leqq 2h-2,$$

which is a contradiction. So we can put $n=4q$ with an odd prime integer q. Then $\bar{\lambda}^{(n/2)}=\chi_{2q}$ by (14). Comparing this and (13), we get $a_1=a_2=a_q=0$, $a_{2q}=1$ i. e., $\lambda=\chi_{2q}+a_4\chi_4+a_{4q}\chi_{4q}$. From this we see that $q=3$, $a_4=0$ and $a_{4q}=1$, since

$$2q=h=\phi(2q)+a_4\phi(4)+a_{4q}\phi(4q)=(q-1)(1+2a_{4q})+2a_4\geqq 3(q-1).$$

Thus we get $\lambda=\chi_6+\chi_{12}$.

This completes the proof of Proposition 3. 1 and hence of Theorem II.

From the latter part of Proposition 3. 1 (and Theorem I) we get the following:

COROLLARY 3. 2. *Assume that* $G\subseteqq Aut(X)$ *for some complete nonsingular cunve* X *of genus* $g\geqq 2$. *Put* $\lambda=Tr(G|H^1(X,\mathbf{Q}_l))$. *Then*

(a) *If* $n=4g+2$ *then* $\lambda_\alpha=\sum_{\substack{d|2g+1\\ d\neq 1}}\chi_{2d}$.

(b) *If* $n=4g$ *then* $\lambda_\gamma=\chi_6+\chi_{12}$ *; or*

$$\lambda_\beta=\sum_{d|m}\chi_{2^r d} \quad \textit{with} \quad n=2^r m\ (r>1),\ (2,m)=1.$$

Remark 3. 3. Let g denote an integer $\geqq 2$, and p the characteristic of k. We denote by ζ_m a primitive m-th root of unity (if exists).

(a) The character $\lambda_\alpha=\sum_{d|2g+1}\chi_{2d}-\chi_2$ is realizable as $\mathrm{Tr}(G|H^1(X,\mathbf{Q}_l))$ by the curve X over k and the automorphism σ of X below:

$$y^2=x^{2g+1}+1,\ (x,y)\mapsto(\zeta_{2g+1}\cdot x,\ -y) \quad \text{if } p\nmid 4g+2;$$

$$y^2+y=x^{2g+1},\ (x,y)\mapsto(\zeta_{2g+1}\cdot x,\ y+1) \quad \text{if } p=2;$$

$$y^2=x^{2g+1}-x,\ (x,y)\mapsto(x+1,\ -y) \quad \text{if } p=2g+1.$$

On the other hand, λ_α is not realizable by any curve over k of genus g and any automorphism if $p|2g+1$ and $p\neq 2g+1$.

(b) Assume that $4g=2^r\cdot m$ $(r\geqq 2)$ with $(2,m)=1$. The character $\lambda_\beta=\sum_{d|m}\chi_{2^r d}$ is realizable by the curve and the automorphism below:

$$y^2=x(x^{2g}+1),\ (x,y)\mapsto(\zeta_{2g}\cdot x,\zeta_{4g}\cdot y) \qquad \text{if } p\nmid 4g.$$

On the other hand, λ_β is not realizable if $p|4g$.

(c) The character $\lambda_\gamma=\chi_6+\chi_{12}$ is realizable by the curve in $\mathrm{Proj}(k[x,y,z])$ and the automorphism below:

$$x^3y-xy^3+z^4=0,\ (x,y,z)\mapsto(x+y,y,\zeta_4\cdot z) \qquad \text{if } p=3;$$
$$x^4+y^3x+z^4=0,\ (x,y,z)\mapsto(x,\zeta_3\cdot y,\zeta_4\cdot z) \qquad \text{if } p\neq 2,3.$$

On the other hand, λ_γ is not realizable if $p=2$.

PROOF. First, we note by [4, p. 187 Corollary 2. 8] that

$$4g_2=2g+\mathrm{Tr}(\sigma^{n/2}|H^1(X,\boldsymbol{Q}_l))$$

if $\sigma\in\mathrm{Aut}(X)$ for some curve X of genus g and $2|n$, where g_2 denotes the genus of $X/\langle\sigma^{n/2}\rangle$. Hence, if λ_α (resp. $\lambda_\beta,\lambda_\gamma$) is realizable, then

(19) $\sigma^{n/2}$ is a hyperelliptic (resp. a hyperelliptic, not a hyperelliptic) involution.

(a) By Corollary 3. 2, to see (a) it suffices to show the latter part. Now assume that λ_α is realizable and $p|2g+1$ with $p\neq 2g+1$. Then, the image of G via the natural homomorphism: $G\to\mathrm{PGL}(2,k)$ must be a cyclic group of order $2g+1$. On the other hand, it follows from our assumption on p and g that $\mathrm{PGL}(2,k)$ does not have such a subgroup by considering the Jordan's canonical forms.

(b) This can be proved in the same way as (a).

(c) By (19), it suffices to show the latter part. Now assume that $\lambda_\gamma=\mathrm{Tr}(G|H^1(X,\boldsymbol{Q}_l))$ for some curve X with $G\subseteqq\mathrm{Aut}(X)$ and $p=2$. If X is hyperlliptic, we have a contradiction as in (a). In the case where X is non-hyperelliptic, since $\mathrm{Tr}(\mathrm{Aut}(X)|H^0(X,\Omega_X))$ is faithful, we have an inclusion: $G\to\mathrm{GL}(3,k)$. On the other hand, $\mathrm{GL}(3,k)$ does not have a cyclic subgroup of order 12. Q. E. D.

§ 4. Application

Throughout this section we assume $k=\boldsymbol{C}$ and by ζ_n a primitive n-th root of unity. Before giving a proof to Proposition III, we make, as an interpretation of Theorem I (a), an evaluation of the eigenvalues of the action of an automorphism of a curve X on the space $H^0(X,\Omega_X)$ of 1-canonical forms.

PROPOSITION 4.1. *Assume that $G \subseteqq Aut(X)$ for a compact Riemann surface X of genus $g \geqq 2$. Put $\chi = Tr(G|H^0(X, \Omega_X))$ and let $m_a = \langle \chi, \psi_a \rangle$ $(a \in \boldsymbol{Z})$, where $\psi_a : G \to \boldsymbol{C} \setminus \{0\}$ denotes the homomorphism defined by $\sigma \mapsto \zeta_n^a$. Then we have the following:*

(a) $m_a + m_{n-a} = m_b + m_{n-b}$ *if* $(a, n) = (b, n)$.

(b) $m_e + m_{n-e} \geqq m_d + m_{n-d} - 2 \cdot \delta_{d,n}$ *for* $d|n$, $e|d$.

PROOF. It suffices to show that

(1) $\chi + \chi^{-1} = \mathrm{Tr}(G|H^1(X, \boldsymbol{Q}_l))$.

On the other hand, this follows from the Lefschetz fixed point formula (cf. [1, p. 265]). Q. E. D.

For the rest of this section we consider Proposition III. Our proof is based on an existence theorem ([3, Proposition 4.5]):

LEMMA 4.2. *Let $\chi : G \to \boldsymbol{C}$ be a character of degree $\geqq 2$. Then χ is realizable (cf. Proposition III for this terminology) if and only if χ satisfies the following condition:*

(†) *for each $e|n$, $e \neq n$ and each integer i $(0 < i < n/e)$ with $(i, n/e) = 1$, there exists a non-negative integer α_{ei} with $e|\alpha_{ei}$ such that for all $d|n$ with $d \neq n$,*

$$\chi(\sigma^d) = 1 + \sum_{e|d} \sum_{\substack{1 \leqq i \leqq n/e \\ (i, n/e) = 1}} \alpha_{ei} \cdot \zeta_n^{di} / (1 - \zeta_n^{di}).$$

PROOF of PROPOSITION III. Put $\lambda = \chi + \chi^{-1} = 2\chi$. First we note that

(2) $\zeta/(1-\zeta) + \zeta^{-1}/(1-\zeta^{-1}) = -1$ if $\zeta \neq 1$.

To show the implication: (i) $\Longrightarrow$ (ii), we assume the existence of α_{ei}'s such as in (†). Then, by (2) we have

$$\lambda(\sigma^d) = 2 - \sum_{e|d} \sum_{i} \alpha_{ei} \qquad \text{for } d|n,\ d \neq n.$$

Hence, from Lemma 1.1 it follows that

$$\alpha_e^{(\lambda)} = \sum_i \alpha_{ei} \geqq 0 \qquad \text{for } e|n,\ e \neq n,$$

as desired. To show the converse, we note that

$$2\alpha_e^{(1+\chi)} = \alpha_e^{(\lambda)} \qquad \text{for } e|n \text{ with } e \neq n.$$

In fact, we have

$$\chi(\sigma^d) = 1 - \sum_{e|d} \alpha_e^{(1+\chi)} \qquad (d|n,\ d \neq n).$$

Hence, by our assumption on λ and the definition (*) we have that $\alpha_e^{(1+\chi)} \geqq 0$ and

$e|\alpha_e^{(1+\chi)}$. Using these, we obtain a set of desired α_{ei}'s:

$$\alpha_{ei}=\begin{cases} 2\alpha_e^{(1+\chi)} & \text{if } e=n/2; \\ \alpha_e^{(1+\chi)} & \text{if } e\neq n/2 \text{ and if } i=1 \text{ or } n/e-1; \\ 0 & \text{otherwise.} \end{cases}$$

Q. E. D.

REMARK. We note by (1) that if a real-valued character of G of degree $\geqq 2$ is realizable (in our sense), then it is a rational character.

REMARK 4.3. In this remark, G denotes a finite group. Denote by $\mathcal{C}$ the set of cyclic subgroups D of G such that $D\neq\{1\}$. Let λ be a rational character of G. For each $D\in\mathcal{C}$ we define an integer α_D by the relation below:

$$\lambda(\sigma_E)=2-\sum_{\substack{D\in\mathcal{C} \\ D\supseteqq E}}\alpha_D \qquad \text{for } E\in\mathcal{C},$$

where σ_E denotes a generator of E (cf. Lemma 1.1).

If $G\subseteqq \mathrm{Aut}(X)$ for some compact Riemann surface X of genes $\geqq 2$ and $\lambda=\mathrm{Tr}(G|H^1(X, \boldsymbol{Q}_l))$, then for $D\in\mathcal{C}$ we have that

$$\alpha_D\geqq 0 \text{ and } [N_G(D):D]|\alpha_D,$$

because $\alpha_D=\#\{P\in X|\tau(P)=P\Longleftrightarrow\tau\in D \text{ for } \tau\in G\}$ as in Lemma 2.4 (note: the isotropy subgroup G_P is cyclic, cf. [1, III. 7. 7]).

In general, even if $\alpha_D\geqq 0$ for each $D\in\mathcal{C}$, the condition that $[N_G(D):D]|\alpha_D$ is not necessarily satisfied. In particular, such χ as in Proposition III (ii) is not necessarily realizable for our (abelian) G. For example, take: $G=(\boldsymbol{Z}/p\cdot\boldsymbol{Z})\times(\boldsymbol{Z}/p\cdot\boldsymbol{Z})$ with p being a prime number and $\chi=\sum_{D\in\mathcal{C}}2\chi_D$, where $\chi_D: G\to\boldsymbol{Q}$ denotes the compositum of the character of the faithful irreducible representation of G/D over $\boldsymbol{Q}$ and the natural homomorphism: $G\to G/D$. Then it is easy to see that $\alpha_D=4$ for $D\in\mathcal{C}$.

Note added in proof (Nov. 1987). Proffessor H. Stichtenoth kindly let us know a direct proof of THEOREM II using the Riemann–Hurwitz foumula.

REFERENCES

[1] Farkas, H. M. and Kra, I., Riemann surfaces, Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[2] Harvey, W. J., Cyclic groups of automorphisms of a compact Riemann surface, Quart. J. Math. Oxford (2), **17** (1966), 86-97.

[3] Kuribayashi, I., On automorphism groups of a curve as linear groups, J. Math. Soc. Japan, **39** (1987), 51-77.

[4] Milne, J. S., Étale cohomology, Princeton University Press, New Jersey, 1980.

[5] Mumford, D., Abelian varieties, Oxford University Press, London, 1970.

[6] Sekiguchi, T., On the fields of rationality for curves and for their Jacobian varieties, Nagoya Math. J., **88** (1982), 197-212.

[7] Serre, J. P., Linear representations of finite groups, Springer-Verlag, New York-Heidelberg-Berlin, 1977.

[8] Serre, J. P., Local fields, Springer-Verlag, New York-Heidelberg-Berlin, 1979.

[9] Steiger, F., Die maximalen Ordnungen periodischer topologischer Abbildungen geschlossener Flächen in sich, Commentarii Math. Helv., **8** (1929), 48-69.

[10] Wiman, A., Über die hyperelliptischen Curven und diejenigen vom Geschlechte p=3 welche eindeutigen Transformationen in sich zulassen, Bihang Till. Kongl. Svenska Vetenskaps-Akademiens Handlinger, **21** (1895-6), 1-23.

Izumi Kuribayashi
Institute of Mathematics
University of Tsukuba
Ibaraki, 305 Japan

Fumiyuki Momose
Department of Mathematics
Faculty of Science and
Engineering
Chuo University
Bunkyo-ku, Tokyo 112 Japan