INDUCED AUTOMORPHISMS ON FRICKE CHARACTERS OF FREE GROUPS

BY

ROBERT D. HOROWITZ(1)

ABSTRACT. The term character in this paper will denote the character of a group element under a general or indeterminate representation of the group in the special linear group of 2×2 matrices with determinant 1; the properties of characters of this type were first studied by R. Fricke in the late nineteenth century. Theorem 1 determines the automorphisms of a free group which leave the characters invariant. In a previous paper it was shown that the character of each element in the free group F_n of finite rank n can be identified with an element of a certain quotient ring of the commutative ring of polynomials with integer coefficients in $2^n - 1$ indeterminates. It follows that any automorphism of F_n induces in a natural way an automorphism on this quotient ring. Corollary 1 shows that for $n \geq 3$ the group of induced automorphisms of F_n is isomorphic to the group of outer automorphism classes of F_n. The possibility is thus raised that the induced automorphisms may be useful in studying the structure of this group. Theorem 2 gives a characterization for the group of induced automorphisms of F_2 in terms of an invariant polynomial.

1. **Introduction.** The algebraic properties of group characters under representation in the two-dimensional special linear group were first studied by R. Fricke [1] in connection with problems in the theory of Riemann surfaces. Although Fricke was primarily concerned with analytic questions, his work has led to results of group theoretic interest. Further results on free groups and related results have recently been given by the author [2] and A. Whittemore [5], [6]. Fricke in [1] observed the existence of naturally induced automorphisms on the ring of polynomial expressions in the characters of the

group elements arising from the automorphisms of the group. The present paper investigates the induced automorphisms on the characters of free groups and their relationship to the automorphisms of the groups.

2. **Preliminaries.** SL_2 will denote the special linear group of 2×2 matrices with determinant 1 over the real or complex numbers. If G is a group, χu will denote the character of the element $u \in G$ under a general or indeterminate representation of G in SL_2. By this we mean that any relation which we write among the characters of elements of G will be understood to hold identically for all possible representations in SL_2. If we let $\mathcal{R}_G$ denote the set of all representations of G in SL_2, and let $\mathcal{F}(\mathcal{R}_G, C)$ denote the ring of functions from $\mathcal{R}_G$ to the complex numbers with the usual addition and multiplication, then the symbol χu can be regarded as formally denoting the function in $\mathcal{F}(\mathcal{R}_G, C)$ which assigns to each representation $\rho \in \mathcal{R}_G$ the character *trace* $\rho(u)$ of u under ρ. The relations [1, p. 338]

$$(1) \qquad\qquad \chi u^{-1} = \chi u,$$

$$(2) \qquad\qquad \chi uv = \chi u \chi v - \chi uv^{-1},$$

hold for all $u, v \in G$, and can be readily verified from the corresponding relations among the traces of arbitrary matrices in SL_2. The statement of the following result is due to Fricke [1]. A proof is given in [2]:

The character of an arbitrary element u in the free group F_n on the n generators $a_1, a_2, \ldots, a_n$ can be written as a polynomial expression

$$(3) \qquad \chi u = P(\chi a_1, \chi a_2, \ldots, \chi a_1 a_2, \ldots, \chi a_1 a_2 \cdots a_n)$$

with integer coefficients in the $2^n - 1$ characters

$$(4) \qquad\qquad \chi a_{i_1} a_{i_2} \cdots a_{i_\nu}$$

where $1 \le i_1 < i_2 < \cdots < i_\nu \le n$, $1 \le \nu \le n$.

The polynomial expression (3) is obtained by repeated application of the formulas (1), (2) to the freely reduced word representing u.

The following two lemmas will be used in the next section.

Lemma 1. *Let F be a free group on two or more generators $a, b, \cdots$. If $u \in F$ is such that $au^{-1}bu$ is conjugate to ab (or ba), then $u = b^l a^m$ for some integers l, m.*

The proof of Lemma 1 is a standard cancellation argument. Let U be the freely reduced word representing u. Let $U = b^l V a^m$ where V is freely

reduced, V not beginning with a power of b nor ending with a power of a. Then $aV^{-1}bV = a^m(aU^{-1}bU)a^{-m}$ is conjugate to ab. But $aV^{-1}bV$ is cyclically reduced as written. Therefore V must be the empty word.

Lemma 2 [2, Theorem 7.1]. *Let u be an element of the free group F. If $\chi u = \chi g^m$ where g^m is a power of a primitive element g, then u is conjugate to g^m or g^{-m}.*

3. **Automorphisms leaving the characters invariant.** We shall say that an automorphism α of the free group F *leaves the characters of F invariant* if $\chi u = \chi\alpha(u)$ for all $u \in F$.

Theorem 1. *Let I denote the group of automorphisms of the free group F which leave the characters of F invariant. If F has infinite rank, or if F has finite rank greater than or equal to three, then I is the group of inner automorphisms of F. If F has rank two, then I is the group generated by the inner automorphisms of F together with the automorphism which maps the two generators of F onto their inverses. If F has rank one, then I consists of the two automorphisms of F.*

Proof. The only automorphisms of F_1 are the identity automorphism and the automorphism $u \to u^{-1}$ which clearly leaves the characters of F_1 invariant by (1). Therefore we may restrict our attention to free groups of rank greater than or equal to two. Let a, b be the two generators of F_2. By (3), (4) it follows that the character of any element in F_2 can be represented as a polynomial expression in the three characters $\chi a, \chi b, \chi ab$. The image of this element under the automorphism $a \to a^{-1}, b \to b^{-1}$ will be the same expression in $\chi a^{-1}, \chi b^{-1}, \chi a^{-1}b^{-1}$. Since $\chi a^{-1} = \chi a, \chi b^{-1} = \chi b, \chi a^{-1}b^{-1} = \chi ba = \chi ab$ by (1), it follows that the automorphism $a \to a^{-1}, b \to b^{-1}$ leaves the characters of F_2 invariant. Clearly any inner automorphism leaves the characters of F invariant. Suppose conversely that α is an automorphism of F which leaves the characters invariant. We shall show that α is an inner automorphism or, in the case of F_2, the composition of an inner automorphism with $a \to a^{-1}, b \to b^{-1}$. Let S be the set of free generators which define the words of F. Let $g \in S$. Since α leaves characters invariant, it follows by Lemma 2 that $\alpha(g)$ must be conjugate to g or g^{-1}. Therefore

(5) $$\alpha(g) = u_g^{-1}g^{\epsilon(g)}u_g$$

for some $u_g \in F$ and $\epsilon(g) = \pm 1$. Let a be a fixed element in S. Set $u_a = v$ and $\epsilon(a) = \epsilon$. Then (5) becomes

(6) $$\alpha(a) = v^{-1}a^\epsilon v$$

when $g = a$. Let $\sigma = \pm 1$, and let $g \in S$ with $g \neq a$. Then since ag^σ is a primitive element of F and α leaves characters invariant, Lemma 2 implies that

$$(7) \qquad\qquad \alpha(ag^\sigma) = w^{-1}(ag^\sigma)^\eta w$$

for some $w \in F$ and $\eta = \pm 1$. Since $\alpha(ag^\sigma) = \alpha(a)[\alpha(g)]^\sigma$, we conclude from (7), (6) and (5) that

$$(8) \qquad\qquad w^{-1}(ag^\sigma)^\eta w = v^{-1}a^\epsilon v u_g^{-1} g^{\sigma\epsilon(g)} u_g.$$

The exponent sums on the left and right sides of (8) must be equal. Hence

$$(9) \qquad\qquad (1 + \sigma)\eta = \epsilon + \sigma\epsilon(g).$$

Alternately setting $\sigma = -1$ and $\sigma = +1$ in (9) we obtain

$$(10) \qquad\qquad \epsilon(g) = \epsilon$$

and $\eta = \epsilon$. If we set $\sigma = +1$ in (8), substitute $\eta = \epsilon(g) = \epsilon$, multiply on the left by v and on the right by v^{-1}, we obtain

$$(11) \qquad\qquad vw^{-1}(ag)^\epsilon wv^{-1} = a^\epsilon v u_g^{-1} g^\epsilon u_g v^{-1}.$$

Since $\epsilon = \pm 1$, a^ϵ and g^ϵ are a pair of primitive elements for F. Therefore Lemma 1 implies that $u_g v^{-1} = g^{\epsilon l(g)} a^{\epsilon m(g)}$ for some integers $l(g)$, $m(g)$ depending on $g \in S$. If we substitute (10) and $u_g = g^{\epsilon l(g)} a^{\epsilon m(g)} v$ in (5), we conclude that

$$(12) \qquad\qquad \alpha(g) = v^{-1} a^{-\epsilon m(g)} g^\epsilon a^{\epsilon m(g)} v$$

for all $g \in S$ with $g \neq a$. Let $g, h \in S$ with $g \neq h$, $g, h \neq a$. Then gh is a primitive element of F, and by (12)

$$\alpha(gh) = \alpha(g)\alpha(h) = v^{-1} a^{-\epsilon m(g)} g^\epsilon a^{\epsilon m(g) - \epsilon m(h)} h^\epsilon a^{\epsilon m(h)} v.$$

If we take characters of both sides using the fact that α leaves characters invariant and conjugate elements have the same character, we obtain

$$(13) \qquad\qquad \chi gh = \chi g^\epsilon a^{\epsilon m(g) - \epsilon m(h)} h^\epsilon a^{\epsilon m(h) - \epsilon m(g)}.$$

Now since gh is a primitive element, it follows by Lemma 2 that the argument of the right side must be conjugate to $(gh)^{\pm 1}$. But this is impossible unless $m(g) = m(h)$, for otherwise, since a, g, h are distinct generators of F, the right side of (13) is cyclically reduced and has four syllables. Therefore $m(g)$ has a common value m for all $g \in S$, $g \neq a$. Thus (12) becomes

(14) $$\alpha(g) = v^{-1}a^{-\epsilon m}g^{\epsilon}a^{\epsilon m}v$$

for all $g \in S$ with $g \neq a$. (14) is also clearly valid for $g = a$, for in this case (14) is equivalent to (6). Thus (14) holds for all $g \in S$. If $\epsilon = +1$ in (14), we see that α acts as a conjugation by $a^m v$ on every generator $g \in S$, and consequently on every element of F. Therefore, if $\epsilon = +1$, α is an inner automorphism. Suppose that $\epsilon = -1$. Then (14) becomes

(15) $$\alpha(g) = v^{-1}a^m g^{-1}a^{-m}v$$

for all $g \in S$. Let g, $h \in S$ with $g \neq h$, g, $h \neq a$. Then

$$\alpha(gah) = \alpha(g)\alpha(a)\alpha(h) = v^{-1}a^m g^{-1}a^{-1}h^{-1}a^{-m}v$$

by (15). If we take characters on both sides using the fact that α leaves characters invariant and conjugate elements have the same character, we obtain $\chi gah = \chi g^{-1}a^{-1}h^{-1}$. However if g, h, a are distinct generators of F, this contradicts Lemma 2, as then gah is a primitive element of F, while $g^{-1}a^{-1}h^{-1}$ is clearly not conjugate to $(gah)^{\pm 1}$. Hence in this case there can be at most two generators in S. Since we are assuming F is not F_1 it follows that S has exactly two generators, and from (15) we see that α is the composition of an inner automorphism with the automorphism which maps each generator onto its inverse.

4. **The induced automorphisms.** Let $\mathcal{P}_n$ denote the commutative ring of polynomials with integer coefficients in the $2^n - 1$ indeterminates $x_{i_1 i_2 \ldots i_\nu}$. Let $\mathcal{I}_n$ denote the ideal consisting of all polynomials in $\mathcal{P}_n$ which vanish identically when the characters (4) are substituted for the corresponding indeterminates. Then the character χu of each element $u \in F_n$ can be identified with a unique element of the quotient ring $\mathcal{P}_n/\mathcal{I}_n$, the coset consisting of all polynomials $P \in \mathcal{P}_n$ which satisfy the right side of (3). Any automorphism α of F_n induces in a natural way a permutation $\chi u \rightarrow \chi \alpha(u)$ of the characters of F_n and, consequently, an automorphism on the ring generated by the characters together with the integer constants. Since the equivalence class $\{x_{i_1 i_2 \ldots i_\nu}\}$ of each indeterminate is identified with a character (4), it follows that the ring generated by the characters of F_n together with the integer constants is identified with the entire quotient ring $\mathcal{P}_n/\mathcal{I}_n$. The induced automorphism of F_n corresponding to α can consequently be regarded as an automorphism on the quotient ring $\mathcal{P}_n/\mathcal{I}_n$ given by

(16) $$\{x_{i_1 i_2 \ldots i_\nu}\} \rightarrow \chi \alpha(a_{i_1} a_{i_2} \cdots a_{i_\nu})$$

where the right side of (16) denotes the polynomial equivalence class in $\mathcal{P}_n/\mathcal{I}_n$

identified with the character. Let A_n denote the group of automorphisms of the free group F_n. Let I_n denote the subgroup of inner automorphisms, and let $J_n = A_n/I_n$ denote the quotient group of outer automorphism classes of F_n. It is readily verified that the induced automorphisms of F_n form a group $\mathcal{Q}_n$, and that the mapping which associates to each automorphism of F_n its corresponding induced automorphism on $\mathcal{P}_n/\mathcal{I}_n$ is a homomorphism from A_n to $\mathcal{Q}_n$. The kernel of this homomorphism is the group of all automorphisms in A_n which induce the identity automorphism. These are precisely the automorphisms of F_n which leave the characters invariant. This gives us the following result.

Corollary 1. *If $n \geq 3$, the groups $\mathcal{Q}_n$ and J_n are isomorphic.*

Corollary 1 raises the possibility that the induced automorphisms could be used to study the structure of the group J_n, $n \geq 3$. Results on the structure of the ideals $\mathcal{I}_n$ for $n = 1, 2, 3, 4$ are given in [2] and [5].

5. **The structure of $\mathcal{Q}_2$.** The ideal $\mathcal{I}_2$ is the zero ideal [2]. Thus the character χu of each $u \in F_2$ is given by a unique polynomial in $\mathcal{P}_2$. Let a, b be the two generators of F_2. We set $x = x_1 = \chi a$, $y = x_2 = \chi b$, $z = x_{12} = \chi ab$. Then $\mathcal{P}_2 = Z[x, y, z]$ the commutative ring of polynomials with integer coefficients in x, y, z. The automorphisms

$$
\begin{array}{ccc}
a \to a^{-1} & a \to b & a \to ab \\
(17) & & \\
b \to b & b \to a & b \to b^{-1}
\end{array}
$$

together with the inner automorphisms generate A_2. (See e.g. [4, §4.5].) Consequently the induced automorphisms of (17) given by the right-hand column of (18) below constitute a generating set for $\mathcal{Q}_2$.

$$
\begin{array}{clll}
& \text{(i)} & a \to a^{-1} & x \to x \\
& & b \to b & y \to y \\
& & (ab \to a^{-1}b) & z \to xy - z \\
& \text{(ii)} & a \to b & x \to y \\
(18) & & b \to a & y \to x \\
& & (ab \to ba) & z \to z \\
& \text{(iii)} & a \to ab & x \to z \\
& & b \to b^{-1} & y \to y \\
& & (ab \to a) & z \to x.
\end{array}
$$

(To see (18)(i) we observe that $\chi a^{-1}b = \chi ba^{-1} = \chi b\chi a - \chi ba = xy - z$ by

(2).) The following theorem essentially characterizes $\mathcal{A}_2$ as a subgroup of the group of automorphisms of $Z[x, y, z]$.

Theorem 2. *Let $\mathcal{A}_2^*$ be the group of automorphisms of the ring $Z[x, y, z]$ which keep invariant the polynomial*

(19) $$C(x, y, z) = x^2 + y^2 + z^2 - xyz.$$

Then the automorphisms of $\mathcal{A}_2$ together with the two automorphisms

(20)
$$\begin{array}{ll} x \longrightarrow -x & x \longrightarrow x \\ y \longrightarrow -y & y \longrightarrow -y \\ z \longrightarrow z & z \longrightarrow -z \end{array}$$

generate the automorphisms of $\mathcal{A}_2^*$.

Remarks. The automorphisms (20) are not induced automorphisms because $-x, -y, -z$ cannot be characters. For under the representation which maps every element of F_2 onto the identity matrix of SL_2 we must have $\chi u = 2$ for all $u \in F_2$. Thus $\chi u \neq -\chi v$ for all $u, v \in F_2$. The polynomial (19) has the following significance. The relation

(21) $$\chi aba^{-1}b^{-1} = x^2 + y^2 + z^2 - xyz - 2$$

[1, p. 337, formula (8)] can be verified directly by matrix considerations or derived by applying formulas (1), (2). Since every automorphism in A_2 maps the commutator $aba^{-1}b^{-1}$ onto a conjugate of itself or its inverse, it follows that every induced automorphism must leave (21) and therefore (19) invariant.

Proof. Let $\mathcal{A}_2^{**}$ be the group of automorphisms of $Z[x, y, z]$ generated by $\mathcal{A}_2$ together with the automorphisms (20). Clearly $\mathcal{A}_2^{**} \subseteq \mathcal{A}_2^*$. To complete the proof we must show $\mathcal{A}_2^* = \mathcal{A}_2^{**}$. Let

(22) $$x \longrightarrow P, \quad y \longrightarrow Q, \quad z \longrightarrow R$$

be an arbitrary automorphism in $\mathcal{A}_2^*$ where P, Q, R are polynomials in $Z[x, y, z]$. We wish to show that (22) lies in $\mathcal{A}_2^{**}$. We can suppose without loss of generality that the degrees of P, Q, R are in ascending order

(23) $$\deg P \leq \deg Q \leq \deg R.$$

For we see by (18)(ii), (iii) that the entire symmetric group on x, y, z is contained in $\mathcal{A}_2$. Therefore we can apply a permutation to (22) to obtain an automorphism with degrees in ascending order. If this automorphism can be shown to be in $\mathcal{A}_2^{**}$, it will then follow that the original automorphism (22) lay in $\mathcal{A}_2^{**}$. Let

$$P = P_p + P_{p-1} + \cdots + P_0, \qquad P_p \neq 0,$$

(24)
$$Q = Q_q + Q_{q-1} + \cdots + Q_0, \qquad Q_q \neq 0,$$

$$R = R_r + R_{r-1} + \cdots + R_0, \qquad R_r \neq 0,$$

where P_k, Q_k, R_k are homogeneous polynomials of degree k (i.e. P_k is the sum of all the terms of degree k in P; similarly for Q_k, R_k). If one of the polynomials P, Q, R consisted merely of a constant term, then (22) could not be composed with any mapping to produce the identity, and hence could not be an automorphism. Thus we must have p, q, $r \geq 1$ in (24). Since (22) keeps invariant the polynomial (19) we have

(25) $$-PQR + P^2 + Q^2 + R^2 = -xyz + x^2 + y^2 + z^2.$$

Suppose first that $p = q = r = 1$ in (24). If we then compare highest terms on the left and right of (25), we obtain $P_1 Q_1 R_1 = xyz$. Since x, y, z are irreducible, unique factorization implies that one of the polynomials P_1, Q_1, R_1 is $\pm x$, one is $\pm y$, and one is $\pm z$. We can suppose without loss of generality by composing (22) with a permutation as before that

(26) $$P_1 = c_1 x, \quad Q_1 = c_2 y, \quad R_1 = c_3 z,$$

where c_1, c_2, $c_3 = \pm 1$ and $c_1 c_2 c_3 = 1$. If we substitute (26) in (24) and expand (25), we see that the term $c_2 c_3 P_1 yz$ appears on the left while there is no term in yz on the right of (25). Therefore $P_0 = 0$. Similarly Q_0, $R_0 = 0$. Now the four possibilities for (22) are

$$
\begin{array}{cccc}
x \to x & x \longrightarrow x & x \to -x & x \to -x \\
(27) \qquad y \to y & y \to -y & y \longrightarrow y & y \to -y \\
z \to z & z \to -z & z \to -z & z \longrightarrow z.
\end{array}
$$

All of these are elements of $\mathfrak{A}_2^{**}$ since they are all generated by the automorphisms (20). Now we proceed by induction on the maximum of the degrees of P, Q and R in (24). We may assume without loss of generality that $p \leq q \leq r$ so that this maximum is r. If we expand terms on the left side of (25) using (24), we obtain

(28) $$-P_p Q_q R_r + \cdots + P_p^2 + \cdots + Q_q^2 + \cdots + R_r^2 + \cdots$$
$$= -xyz + x^2 + y^2 + z^2,$$

where the dots represent terms of lower order. Since the situation $p = q = r =

1 has already been considered we may assume $r > 1$. Then the term $-P_p Q_q R_r$ in (28) is of degree at least 4. Since the right side of (28) has highest degree 3, it follows that all the terms of degree greater that 3 on the left side of (28) must cancel to zero. Thus there is no single term of highest degree on the left side of (28). We claim that $r = p + q$. For $r > p + q$ implies that $2r > 2p$, $2r > 2q$, $2r > p + q + r$, and then R_r^2 of degree $2r$ would be the highest term on the left side of (28) and the only term with this degree. Similarly $r < p + q$ implies that $p + q + r > 2r \geq 2p$, $2q$, and then $P_p Q_q R_r$ of degree $p + q + r$ would be the highest term on the left side of (28) and the only term with this degree, again leading to a contradiction. If $r = p + q$, then the terms of highest degree on the left side of (28) are $-P_p Q_q R_r + R_r^2 = 0$. Therefore

(29)
$$R_r = P_p Q_q.$$

Now consider the mapping

(30)
$$x \to P, \quad y \to Q, \quad z \to PQ - R.$$

This mapping lies in $\mathfrak{a}_2^*$ since it is the composition of (22) with (18)(i). However (30) has highest degree less than r as deg $P = p < r$, deg $Q = q < r$ since $r = p + q$, and deg $PQ - R < r$ since the highest terms $P_p Q_q - R_r$ cancel because of (29). Therefore (30) lies in $\mathfrak{a}_2^{**}$ by the induction hypothesis. Now since (18)(i) is in $\mathfrak{a}_2^{**}$ it follows that the automorphism in (22) belongs to $\mathfrak{a}_2^{**}$ which completes the induction.

6. **Remarks on $\mathfrak{a}_3$ and $\mathfrak{a}_4$. Unsolved problems.** The question of the existence of analogous results to Theorem 2 for any of the groups $\mathfrak{a}_n$ where $n \geq 3$ remains open. We have shown in [2] that the ideal $\mathfrak{I}_3$ is a principal ideal generated by a polynomial of degree 4. One can readily obtain a generating set for the group $\mathfrak{a}_3$ by following the same procedure used for $\mathfrak{a}_2$. The induced automorphisms on $\mathcal{P}_3/\mathfrak{I}_3$ thus obtained which generate $\mathfrak{a}_3$ are in turn seen to correspond to a set of automorphisms of $\mathcal{P}_3$ which leave the polynomial generating $\mathfrak{I}_3$ invariant. In a communication to the author, Wilhelm Magnus has conjectured that an analogous result to Theorem 2 might be obtained for the group $\mathfrak{a}_3$ using the polynomial generator of $\mathfrak{I}_3$ as an invariant. The precise relationship between the automorphisms of $\mathfrak{a}_3$ and the automorphisms of $\mathcal{P}_3$ which leave the ideal $\mathfrak{I}_3$ invariant awaits further investigation. Whittemore in [5] has given partial results on the structure of $\mathfrak{I}_4$, and has given a set of polynomials which collectively remain invariant under the automorphisms of $\mathfrak{a}_4$. These results appear to indicate that the structure of $\mathfrak{a}_n$ increases in complexity as n increases.

REFERENCES

1. R. Fricke and F. Klein, *Vorlesungen über die Theorie der automorphen Functionen.* Vol. 1, Teubner, Leipzig, 1897.

2. R. D. Horowitz, *Characters of free groups represented in the two dimensional special linear group,* Comm. Pure Appl. Math. 25 (1972), 635–649. MR 47 #3542.

3. ———, *Two dimensional special linear characters of free groups,* Ph. D. Thesis, New York University, New York, 1970.

4. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations,* Pure and Appl. Math., Vol. 13, Interscience, New York and London, 1966. MR 34 #7617.

5. A. Whittemore, *On special linear characters of free groups of rank $n \geq 4$,* Proc. Amer. Math. Soc. 40 (1973), 383–388. MR 48 #428.

6. ———, *On representations of the group of Listing's knot by subgroups of* SL(2, C), Proc. Amer. Math. Soc. 40 (1973), 378–382. MR 47 #5132.

DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE (CUNY), FLUSHING, NEW YORK 11367