Journal of Algebra **228,** 659–673 (2000)
doi:10.1006/jabr.2000.8293, available online at http://www.idealibrary.com on IDEAL®

On an Article by W. Magnus on the Fricke Characters of Free Groups[1]

Jacques Peyrière

Laboratoire de Mathématiques, UMR 8628 du CNRS, Université Paris-Sud, Bât. 425,
91405 Orsay Cedex, France
E-mail: Jacques.Peyriere@math.u-psud.fr

Communicated by Laurent Clozel

Received December 21, 1998

Another way of deriving the structure of the ring of Fricke characters of free groups and a classification of unitary and associative algebras over an arbitrary field with elements having a minimal polynomial of degree at most 2 are given.

Key Words: PI algebra; matrix identities; Fricke characters.

I. INTRODUCTION

Identities linking traces are not new. Those of Proposition 1 appear in Fricke and Klein [3] and had already been stated by Vogt, as mentioned in [5]. The fact that the trace of a product, the factors of which belong to a finite set $A_1, A_2, \dots, A_n$ of elements of $SL(2, \mathbb{C})$, can be expressed as a polynomial in the traces of the $2^n - 1$ products $A_{j_1} A_{j_2}, \dots, A_{j_k}$, where $1 \le j_1 < j_2 < \cdots < j_k \le n$, conjectured by Fricke and proved by Horowitz [4], has been rediscovered several times, mainly on the occasion of studies in quasi-crystals (see [6, 7] for a tentative compilation of the corresponding literature). The structure of the ideal of polynomials in $2^n - 1$ variables which vanish on any system of traces $\{\operatorname{tr} A_{j_1} A_{j_2} \cdots A_{j_k}\}$ has been elucidated by Whittemore [11] in the case $n = 4$ and by Magnus [5] in general. This structure also has been rediscovered in the context of quasi-crystals [1, 2, 10].

---

[1] This work benefitted from the computer algebra systems available at the UMS Medicis (UMS 658) of CNRS.

0021-8693/00 $35.00

In this work, a new method of obtaining these results is given. It relies upon explicit calculations made possible by the existence of computer algebra software.

Rather than placing ourselves at once in $M_2(K)$, the algebra of 2×2-matrices on a field K, we prefer to consider first an algebra in which any element has a minimal polynomial of degree at most 2. Indeed, it is well known that polynomial identities between traces of matrices come from the Cayley–Hamilton identity [8, 9]. Despite the fact that establishing identities is somewhat harder in this context, this has the advantage of yielding the structure of these algebras (Theorems 1 and 3) and a new characterization of $M_2(K)$.

Theorem 2 is a slight improvement on Theorem 2.2 of [5]. Also, identity (6) is already in [5].

II. ALGEBRAS WITH ELEMENTS HAVING A MINIMAL POLYNOMIAL OF DEGREE AT MOST 2

Let $\mathscr{A}$ be an associative and unitary algebra on a field K, the elements of which have a minimal polynomial of degree at most 2. We assume that $K \neq \mathbb{Z}/2\mathbb{Z}$.

In this section, the characteristic of K is supposed to be different from 2, except in Lemmas 1 and 2 and in Proposition 1.

LEMMA 1. *There exists a linear form*, $a \mapsto \bar{a}$, *and a quadratic form*, $a \mapsto \tilde{a}$, *on* $\mathscr{A}$, *assuming values* 2 *and* 1, *respectively*, *at the unit*, *and such that*, *for any element a in* $\mathscr{A}$, *one has* $a^2 - (\bar{a})a + \tilde{a} = 0$.

Moreover, *if a and b are in* $\mathscr{A}$, *one has* $\overline{ab} = \overline{ba}$ *and* $\widetilde{ab} = \tilde{a}\tilde{b}$, *as well as the relations*

$$ab + ba = \overline{ab} - \bar{a}\bar{b} + \bar{b}a + \bar{a}b \tag{1}$$

$$aba = \overline{ab}a + \tilde{a}(b - \bar{b}). \tag{2}$$

$\bar{a}$ and $\tilde{a}$ will be called the *trace* and the *determinant* of a.

Proof. If $a \in \mathscr{A}$ and if a is not proportional to the unit, its minimal polynomial is written $a^2 - (\bar{a})a + \tilde{a}$. Obviously, one has $\overline{ta} = t\bar{a}$ and $\widetilde{ta} = t^2\tilde{a}$ for any scalar t.

Let a and b be two elements of $\mathscr{A}$ such that 1, a, and b are linearly independent over K. One has

$$\begin{aligned}(a+b)^2 &= \overline{a+b}(a+b) - \widetilde{a+b} \\ &= \bar{a}a - \tilde{a} + \bar{b}b - \tilde{b} + ab + ba,\end{aligned}$$

from which it follows $ab + ba = (\overline{a+b} - \bar{a})a + (\overline{a+b} - \bar{b})b + \tilde{a} + \tilde{b} - \widetilde{a+b}$, which will be provisionally written $ab + ba = \alpha a + \beta b + \gamma$.

Let t be a scalar. By expanding $(a+tb)^2$ one gets

$$\overline{a+tb}(a+tb) - \widetilde{a+tb} = (a+tb)^2 = (\bar{a} + t\alpha)a + t(t\bar{b} + \beta)b + t\gamma - \tilde{a} - \tilde{b}t^2.$$

It follows that, for all $t \in K$, one has $\overline{a+tb} = \bar{a} + t\alpha$ and $t\overline{a+tb} = t(t\bar{b} + \beta)$; since K has at least two non-zero elements, one gets $\overline{a+b} = \bar{a} + \bar{b}$.

Now, let a be an element of $\mathscr{A}$ and t a scalar. One has $(a+t)^2 = a^2 + 2ta + t^2 = (\bar{a} + 2t)(a+t) - \tilde{a} - t\bar{a} - t^2$, whence $\overline{a+t} = \bar{a} + 2t$. When 1, a, and b are linearly dependent over K, it is easy to check the formula $\overline{a+b} = \bar{a} + \bar{b}$.

One has

$$\begin{aligned} aba &= -a^2b + \bar{b}a^2 + \bar{a}ab + (\tilde{a} + \tilde{b} - \widetilde{a+b})a \\ &= \tilde{a}b + \bar{b}a^2 + (\tilde{a} + \tilde{b} - \widetilde{a+b})a \\ &= \tilde{a}b + (\bar{a}\bar{b} + \tilde{a} + \tilde{b} - \widetilde{a+b})a - \bar{a}\tilde{b}, \end{aligned}$$

whence

$$(ab)^2 = (\bar{a}\bar{b} + \tilde{a} + \tilde{b} - \widetilde{a+b})ab - \tilde{a}\tilde{b}.$$

From this one deduces $\overline{ab} = \overline{ba} = \bar{a}\bar{b} + \tilde{a} + \tilde{b} - \widetilde{a+b}$, $\widetilde{ab} = \tilde{a}\tilde{b}$, and formulas (1) and (2).

Remark. In the case $K = \mathbb{Z}/2\mathbb{Z}$, which we have excluded, the trace does not need to be linear, as shown by the following example. Consider the set $\{1, a, b, c\}$ endowed with the multiplication defined by the table

$$\begin{array}{cccc} 1 & a & b & c \\ a & a & c & c \\ b & c & b & c \\ c & c & c & c \end{array}.$$

The $\mathbb{Z}/2\mathbb{Z}$-algebra generated by $\{1, a, b, c\}$ is unitary, associative, all its elements have a minimal polynomial of degree 2 at most, and the traces of a, b, and $a + b$ are all equal to 1.

Since the trace is linear, the relation $a^2 - \bar{a}a + \tilde{a} = 0$ implies $2\tilde{a} = \bar{a}^2 - \overline{a^2}$. So, when the characteristic of K is different from 2, one has $\tilde{a} = (\bar{a}^2 - \overline{a^2})/2$.

Remark. Let $\mathbb{K}$ be a field containing K. Then, due to formula (1), any element of the algebra $\mathscr{A} \otimes_K \mathbb{K}$ has a minimal polynomial of degree 2 at most.

In the sequel it will be convenient to denote by $\mathscr{A}_0$ the kernel of the trace.

PROPOSITION 1 (Fricke Formulas). *If a, b, and c are elements of $\mathscr{A}$ one has*

$$\overline{abc} + \overline{acb} = \bar{a}\overline{bc} + \bar{b}\overline{ca} + \bar{c}\overline{ab} - \bar{a}\bar{b}\bar{c}$$

and

$$\begin{aligned}\overline{abc}\,\overline{acb} &= \bar{a}^2\tilde{b}\tilde{c} + \bar{b}^2\tilde{c}\tilde{a} + \bar{c}^2\tilde{a}\tilde{b} + \overline{bc}^2\,\tilde{a} + \overline{ca}^2\,\tilde{b} + \overline{ab}^2\,\tilde{c}\\ &\quad - \bar{a}\bar{b}\tilde{c}\overline{ab} - \bar{b}\bar{c}\tilde{a}\overline{bc} - \bar{c}\,\bar{a}\tilde{b}\overline{ca} + \overline{bc}\,\overline{ca}\,\overline{ab} - 4\tilde{a}\tilde{b}\tilde{c}.\end{aligned}$$

Proof. Due to formula (1), one has $a(bc + cb) = a(\overline{bc} - \bar{b}\bar{c} + \bar{c}b + \bar{b}c)$, which gives the first formula.

Let us compute the product $abcacb$ in two ways: write $(abca)cb = ab(cac)b$ and use formula (2) repeatedly. One has

$$\begin{aligned}(abca)cb &= \big(\overline{abc}a + \tilde{a}(bc - \overline{bc})\big)cb\\ &= \overline{abc}acb + \tilde{a}b(\bar{c}c - \tilde{c})b - \tilde{a}\overline{bc}cb\\ &= \overline{abc}acb + \tilde{a}\bar{c}\big(\overline{bc}b + \tilde{b}(c - \bar{c})\big) - \tilde{a}\tilde{c}(\bar{b}b - \tilde{b}) - \tilde{a}\overline{bc}cb,\\ ab(cac)b &= ab\big(\overline{ca}c + \tilde{c}(a - \bar{a})\big)b = \overline{ca}a(bcb) + \tilde{c}(ab)^2 - \tilde{c}\bar{a}ab^2\\ &= \overline{ca}a\big(\overline{bc}b + \tilde{b}(c - \bar{c})\big) + \tilde{c}\big(\overline{ab}ab - \widetilde{ab}\big) - \bar{a}\tilde{c}a(\bar{b}b - \tilde{b}),\end{aligned}$$

and

$$\begin{aligned}\overline{abc}acb = &-\tilde{a}\bar{c}\big(\overline{bc}b + \tilde{b}(c - \bar{c})\big) + \tilde{a}\tilde{c}(\bar{b}b - \tilde{b}) + \tilde{a}\overline{bc}cb\\ &+\overline{ca}a\big(\overline{bc}b + \tilde{b}(c - \bar{c})\big) + \tilde{c}\big(\overline{ab}ab - \widetilde{ab}\big) - \bar{a}\tilde{c}a(\bar{b}b - \tilde{b}).\end{aligned}$$

Then, one gets the second relation by taking the traces of both sides of the last formula.

LEMMA 2. *If a, b, and c are three elements of $\mathscr{A}$ such that $\overline{abc} \neq \overline{acb}$, one has*

$$\begin{aligned}\bar{b}abc = &-\bar{a}\tilde{b}\bar{c} + \tilde{b}\overline{ca} + \bar{b}\overline{abc} - \overline{ab}\,\overline{bc}\\ &+ \tilde{b}\bar{c}a - \overline{abc}b + \bar{a}\tilde{b}c\\ &+\overline{bc}ab + \overline{ab}bc - 2\tilde{b}ca.\end{aligned}$$

Proof. First, a direct computation shows that the conclusion of this lemma holds when $c = a$ and when $c = b$.

One evaluates the product $cabcbc$ in two ways by writing $[c(ab)c]bc = ca(bc)^2$ and using formula (2) as in the preceding calculation. One has

$$\begin{aligned}[c(ab)c]bc &= \left(\overline{abc}c + \tilde{c}\left(ab - \overline{ab}\right)\right)bc \\ &= \overline{abc}\left(\overline{bc}c + \tilde{c}b - \tilde{c}\bar{b}\right) + \tilde{c}\left(\bar{b}abc - \tilde{b}ac\right) - \tilde{c}\overline{ab}bc\end{aligned}$$

and

$$ca(bc)^2 = \overline{bc}cabc - \widetilde{bc}ca = \overline{bc}\left(\overline{abc}c + \tilde{c}ab - \tilde{c}\overline{ab}\right) - \widetilde{bc}ca.$$

By subtracting, one gets the relation

$$\begin{aligned}\tilde{c}\Big(-\bar{b}abc - \bar{a}\tilde{b}\bar{c} + \tilde{b}\overline{ca} + \bar{b}\overline{abc} - \overline{ab}\,\overline{bc} + \tilde{b}\bar{c}a - \overline{abc}b + \bar{a}\tilde{b}c \\ + \overline{bc}ab + \overline{ab}bc - 2\tilde{b}ca\Big) = 0.\end{aligned}$$

If $\tilde{c} \neq 0$, we are done.

If $\tilde{c} = 0$, as the relation to be proven is linear in c, it suffices to prove it when c is replaced by $c + \alpha a + \beta b$. As $(c + \alpha a + \beta b)^{\sim} = \alpha^2\tilde{a} + \beta^2\tilde{b} + \tilde{c} - \alpha(\overline{ca} - \bar{c}\bar{a}) - \beta(\overline{bc} - \bar{b}\bar{c}) - \alpha\beta(\overline{ab} - \bar{a}\bar{b})$, one can choose such a linear combination, the determinant of which does not vanish, unless all the terms are zero, which, due to Proposition 1, would imply $\overline{abc} = \overline{acb} = \bar{a}\bar{b}\bar{c}$.

From now on the characteristic of K is supposed to be different from 2.

Remark. At this stage, we have to assume in Lemma 2 that $\overline{abc} \neq \overline{acb}$. It turns out that this hypothesis is superfluous. Indeed, when $\mathscr{A}$ is the algebra of 2 × 2-matrices on an field K, this results from the proof of Proposition 6 below. When $\mathscr{A}$ is not the algebra of 2 × 2-matrices, Theorems 1 and 3 below give the structure of such an algebra, and it can be checked that, in all cases, there is no need of assuming $\overline{abc} \neq \overline{acb}$.

COROLLARY. *If a, b, and c are three elements of $\mathscr{A}_0$ such that $\overline{abc} \neq 0$, one has*

$$\begin{aligned}bc - \frac{1}{2}\overline{bc} = -\frac{1}{2\overline{abc}}\Big[\left(4\tilde{b}\tilde{c} - \overline{bc}^2\right)a + \left(\overline{bc}\,\overline{ca} + 2\overline{ab}\tilde{c}\right)b \\ + \left(\overline{ab}\,\overline{bc} + 2\overline{ca}\tilde{b}\right)c\Big]. \qquad (3)\end{aligned}$$

Proof. It follows from Proposition 1 that

$$-\overline{abc}^2 = \overline{ab}^2\,\tilde c + \overline{bc}^2\,\tilde a + \overline{ca}^2\,\tilde b + \overline{ab}\,\overline{bc}\,\overline{ca} - 4\tilde a\tilde b\tilde c.$$

Lemma 2 gives

$$\overline{bc}\big(ab - \tfrac{1}{2}\,\overline{ab}\big) + \overline{ab}\big(bc - \tfrac{1}{2}\,\overline{bc}\big) - 2\tilde b\big(ca - \tfrac{1}{2}\,\overline{ca}\big) = \overline{abc}b$$

and two other relations obtained by circular permutation. One obtains such a linear system, with determinant $-2\overline{abc}^2$, in the unknowns $bc - \frac{1}{2}\,\overline{bc}$, $ca - \frac{1}{2}\,\overline{ca}$, and $ab - \frac{1}{2}\,\overline{ab}$. By solving this system, one gets the claimed formula as well as two others obtained by circular permutation.

PROPOSITION 2. *If there exist three elements a, b, and c of $\mathscr{A}_0$ such that $\overline{abc} \neq 0$, then, for all $d \in \mathscr{A}_0$, one has*

$$\begin{aligned}&\Big[\big(-4\tilde b\tilde c + \overline{bc}^2\big)\overline{ad} + \big(-2\tilde c\overline{ab} - \overline{ac}\,\overline{bc}\big)\overline{bd} + \big(-2\tilde b\overline{ac} - \overline{ab}\,\overline{bc}\big)\overline{cd}\Big]a\\ &\quad+\Big[\big(-2\tilde c\overline{ab} - \overline{ac}\,\overline{bc}\big)\overline{ad} + \big(-4\tilde a\tilde c + \overline{ac}^2\big)\overline{bd} + \big(-2\tilde a\overline{bc} - \overline{ab}\,\overline{ac}\big)\overline{cd}\Big]b\\ &\quad+\Big[\big(-2\tilde b\overline{ac} - \overline{ab}\,\overline{bc}\big)\overline{ad} + \big(-2\tilde a\overline{bc} - \overline{ab}\,\overline{ac}\big)\overline{bd} + \big(-4\tilde a\tilde b + \overline{ab}^2\big)\overline{cd}\Big]c\\ &\quad+\Big[-8\tilde c\tilde b\tilde a + 2\tilde c\overline{ab}^2 + 2\tilde b\overline{ac}^2 + 2\tilde a\overline{bc}^2 + 2\overline{bc}\,\overline{ac}\,\overline{ab}\Big]d = 0. \qquad (4)\end{aligned}$$

Proof. By multiplying on the right both sides of (3) by d and taking the traces one gets

$$\overline{bcd} = -\frac{1}{2\overline{abc}}\Big[\big(4\tilde b\tilde c - \overline{bc}^2\big)\overline{ad} + \big(\overline{bc}\,\overline{ca} + 2\overline{ab}\tilde c\big)\overline{bd} + \big(\overline{ab}\,\overline{bc} + 2\overline{ca}\tilde b\big)\overline{cd}\Big]. \qquad (5)$$

Now, let us prove formula (4). Due to Proposition 1, the coefficient of d in (4) equals $-2\overline{abc}^2$.

First, suppose that $\overline{bc}^2 - 4\tilde b\tilde c$ and $\overline{bcd}$ do not vanish. By writing formula (3) with a, b, and c, and with d, b, and c and by taking (5) into account, one gets two expressions of bc. After cancelling the factor $\overline{bc}^2 - 4\tilde b\tilde c$, one gets (4).

If $\overline{bc}^2 - 4\tilde b\tilde c \neq 0$ and $\overline{bcd} = 0$, then $\overline{bc(a+d)} \neq 0$ and one can apply the above computation to a, b, c, and $a + d$. One gets relation (4) again.

It remains to get rid of the extra assumption $\overline{bc}^2 - 4\tilde b\tilde c \neq 0$. If one of the quantities $\overline{ab}^2 - 4\tilde a\tilde b$ or $\overline{ac}^2 - 4\tilde a\tilde c$ is non-zero, it suffices to perform a permutation of variables. Therefore we suppose that

$$\overline{ab}^2 - 4\tilde a\tilde b = \overline{ac}^2 - 4\tilde a\tilde c = \overline{bc}^2 - 4\tilde b\tilde c = 0.$$

One has

$$\overline{b(a+c)}^2 - 4\tilde{b}\widetilde{(a+c)} = \left(\overline{ab} + \overline{bc}\right)^2 - 4\tilde{b}\left(\tilde{a} + \tilde{c} - \overline{ac}\right)$$
$$= 2\left(\overline{ab}\,\overline{bc} + 2\tilde{b}\overline{ac}\right).$$

If this last expression vanished, due to the three preceding relations and to the expression of $\overline{abc}^2$ recalled above, one would have $\overline{abc} = 0$, contrary to the hypothesis. Therefore, one can apply what precedes to a, b, $a + c$, and d. This gives the same formula again.

PROPOSITION 3. *If a, b, c, and d are four elements of $\mathscr{A}_0$ such that $\overline{abc} \neq 0$, one has*

$$\begin{aligned}
&+16\tilde{d}\tilde{c}\tilde{b}\tilde{a}\\
&\quad - 4\left(\tilde{d}\tilde{c}\overline{ab}^2 + \tilde{d}\tilde{b}\overline{ac}^2 + \tilde{d}\tilde{a}\overline{bc}^2 + \tilde{c}\tilde{b}\overline{ad}^2 + \tilde{c}\tilde{a}\overline{bd}^2 + \tilde{b}\tilde{a}\overline{cd}^2\right)\\
&\quad - 4\left(\tilde{d}\overline{bc}\,\overline{ac}\,\overline{ab} + \tilde{c}\overline{bd}\,\overline{ad}\,\overline{ab} + \tilde{b}\overline{cd}\,\overline{ad}\,\overline{ac} + \tilde{a}\overline{cd}\,\overline{bd}\,\overline{bc}\right)\\
&\quad - 2\left(\overline{cd}\,\overline{bd}\,\overline{ac}\,\overline{ab} + \overline{cd}\,\overline{bc}\,\overline{ad}\,\overline{ab} + \overline{bd}\,\overline{bc}\,\overline{ad}\,\overline{ac}\right)\\
&\quad + \left(\overline{cd}^2\overline{ab}^2 + \overline{bd}^2\overline{ac}^2 + \overline{bc}^2\overline{ad}^2\right) = 0. \qquad (6)
\end{aligned}$$

Proof. Proposition 1 gives expressions of the squares of $\overline{abc}$ and $\overline{abd}$ as polynomials in the determinants of a, b, c, and d and in the traces of their products two by two. By taking into account formula (5), one gets a polynomial relation with integer coefficients between the determinants of a, b, c, and d and the traces of their products. This polynomial is the product of $\overline{bc}^2 - 4\tilde{b}\tilde{c}$ and of the left hand side of (6). Therefore, if $\overline{bc}^2 - 4\tilde{b}\tilde{c} \neq 0$, the proposition is proven. One gets rid of this extra assumption in the same way as in the proof of Proposition 2.

PROPOSITION 4. *If one can extract square roots in the field K and if there exists in $\mathscr{A}_0$ three elements a, b, and c such that $\overline{abc} \neq 0$, then the algebra $\mathscr{A}$ is isomorphic to $M_2(K)$, the algebra of 2×2-matrices over K.*

Proof. Given a, b, and c, one can find three 2×2 matrices A, B, and C with zero traces and such that $\det A = \tilde{a}$, $\det B = \tilde{b}$, $\det C = \tilde{c}$, $\operatorname{tr} AB = \overline{ab}$, $\operatorname{tr} BC = \overline{bc}$, $\operatorname{tr} CA = \overline{ca}$, and $\operatorname{tr} ABC = \overline{abc}$ (apply Proposition 7, the proof of which uses Propositions 2 and 3 only, and Proposition 1). The linear map from $\mathscr{A}$ into $M_2(K)$ which sends 1, a, b, and c on Id, A, B, and C is an homomorphism of unitary algebras due to formula (4) and to formula (3) and to the ones obtained by circular permutations. The fact that this is an isomorphism comes from Proposition 6, the proof of which uses Proposition 2 only.

Remarks. It is necessary to assume that it is possible to extract square roots in K. Indeed, let us consider the $\mathbb{R}$-algebra $\mathscr{A}$ generated, as a vector space, by 1, a, b, and c such that $a^2 = b^2 = c^2 = -1$, $ab = -ba = c$, $ca = -ac = b$, and $bc = -cb = a$ (observe that $abc = -1$). This algebra cannot be isomorphic to $M_2(\mathbb{R})$ because there exists no real 2×2-matrices A and B such that $A^2 = B^2 = -\mathrm{Id}$ and $\operatorname{tr} AB = 0$ (Lemma 3).

Even when K is a field where square roots exist, $\mathscr{A}$ is not necessarily isomorphic to $M_2(K)$: take $\mathscr{A} = K \oplus V$ and declare that the product of two elements of V is always 0. The following theorem gives the structure of algebras $\mathscr{A}$ when $\overline{abc} = 0$ for all a, b, and c with zero traces.

THEOREM 1. (1) *If there exist in* $\mathscr{A}_0$ *three elements* a, b, *and* c *such that* $\overline{abc} \neq 0$, *then the algebra* $\mathscr{A}$ *has dimension* 4 *and any element* d *such that* $\bar{d} = 0$ *decomposes on the base* $\{a, b, c\}$ *according to formula* (4).

(2) *If, for any elements* a, b, *and* c *of* $\mathscr{A}_0$, *one has* $\overline{abc} = 0$, *then the set* $\mathscr{N}$ *consisting of the elements of* $\mathscr{A}$ *which are nilpotent of order* 2 *is a two-sided ideal, any product of three elements of* $\mathscr{N}$ *equals* 0, *and the quotient* $\mathscr{A}/\mathscr{N}$ *has dimension* 1 *or* 2. *When the dimension is* 2, *then any product of two elements of* $\mathscr{N}$ *equals* 0.

Comment. When K is algebraically closed, the condition that the trace of abc is non-zero distinguishes the algebras isomorphic to the full algebra of 2×2-matrices. The proper subalgebras of 2×2-matrices fall under the second alternative of this theorem, but they are not the only ones which can occur.

Proof. The first assertion comes from the preceding proposition by extending K, if necessary.

Let a, b, and c be three elements of $\mathscr{A}_0$. By using repeatedly formula (1) one gets

$$abc = -cab + \overline{abc} = \left(ac - \overline{ac}\right)b + \overline{abc} = a\left(\overline{bc} - bc\right) - \overline{ac}b + \overline{abc},$$

whence

$$2abc = a\overline{bc} - b\overline{ac} + c\overline{ab} \tag{7}$$

(this last identity appears already in [1]).

By hypothesis, if a and b are two elements of $\mathscr{A}_0$, one has $\overline{ab\left(ab - \frac{1}{2}\,\overline{ab}\right)} = 0$, that is, $\overline{ab}^2 = 4\tilde{a}\tilde{b}$.

It follows that, for any $a \in \mathscr{N}$ and for any $b \in \mathscr{A}_0$, one has $\overline{ab} = 0$. In particular, $aba = \overline{ab}a + \tilde{a}(b - \bar{b}) = 0$. Therefore ab and ba are in $\mathscr{N}$.

Let a and b be two elements of $\mathscr{N}$. One has $(a + b)^2 = ab + ba = \overline{ab} = 0$. This means that $\mathscr{N}$ is a two-sided ideal. The fact that any product of three elements of $\mathscr{N}$ is 0 comes from formula (7).

Let a and b be two non-zero elements of $\mathscr{A}_0$. As, for any $t \in K$, one has $(a + tb)^2 = -\tilde{a} + t\overline{ab} - t^2\tilde{b} = -\tilde{b}(t - \overline{ab}/2\tilde{b})^2$, there exists a $t \in K$ such that $a + tb \in \mathscr{N}$. This proves that the dimension of $\mathscr{A}/\mathscr{N}$ is 1 or 2.

When $\dim \mathscr{A}/\mathscr{N} = 2$, there exists $a \in \mathscr{A}_0$ such that $\tilde{a} \neq 0$. Then formula (7) shows that for any b and c in $\mathscr{N}$ one has $abc = 0$. Therefore $-\tilde{a}bc = a^2bc = 0$, which means $bc = 0$.

PROPOSITION 5. *Let a, b, and c be three elements of $\mathscr{A}_0$ such that* $\overline{abc} \neq 0$. *If x, y, z, and t are four elements of K satisfying the relation*

$$\begin{aligned}
&+16t\tilde{c}\tilde{b}\tilde{a} \\
&\quad - 4\left(t\tilde{c}\overline{ab}^2 + t\tilde{b}\overline{ac}^2 + t\tilde{a}\overline{bc}^2 + \tilde{c}\tilde{b}x^2 + \tilde{c}\tilde{a}y^2 + \tilde{b}\tilde{a}z^2\right) \\
&\quad - 4\left(t\overline{bc}\,\overline{ac}\,\overline{ab} + \tilde{c}yx\overline{ab} + \tilde{b}zx\overline{ac} + \tilde{a}zy\overline{bc}\right) \\
&\quad - 2\left(zy\overline{ac}\,\overline{ab} + z\overline{bc}x\overline{ab} + y\overline{bc}x\overline{ac}\right) \\
&\quad + \left(z^2\overline{ab}^2 + y^2\overline{ac}^2 + \overline{bc}^2x^2\right) = 0,
\end{aligned}$$

then there exists a unique $d \in \mathscr{A}$ such that $\bar{d} = 0$, $\overline{ad} = x$, $\overline{bd} = y$, $\overline{cd} = z$, and $\tilde{d} = t$.

Proof. Uniqueness comes from Theorem 1. Set, as formula (4) suggests,

$$\begin{aligned}
d = \frac{1}{2\overline{abc}^2}\Big\{&\Big[\left(-4\tilde{b}\tilde{c} + \overline{bc}^2\right)x + \left(-2\tilde{c}\overline{ab} - \overline{ac}\,\overline{bc}\right)y + \left(-2\tilde{b}\overline{ac} - \overline{ab}\,\overline{bc}\right)z\Big]a \\
&+\Big[\left(-2\tilde{c}\overline{ab} - \overline{ac}\,\overline{bc}\right)x + \left(-4\tilde{a}\tilde{c} + \overline{ac}^2\right)y + \left(-2\tilde{a}\overline{bc} - \overline{ab}\,\overline{ac}\right)z\Big]b \\
&+\Big[\left(-2\tilde{b}\overline{ac} - \overline{ab}\,\overline{bc}\right)x + \left(-2\tilde{a}\overline{bc} - \overline{ab}\,\overline{ac}\right)y + \left(-4\tilde{a}\tilde{b} + \overline{ab}^2\right)z\Big]c\Big\}.
\end{aligned}$$

Then, a direct computation proves the proposition.

This is a generalization of the decomposition of a 2 × 2-matrix on the Pauli matrices.

III. APPLICATION TO 2 × 2-MATRICES

The algebra $\mathscr{A}$ is the algebra $M_2(K)$ of 2 × 2-matrices with entries in K. Let $M_2^0(K)$ stand for the set of matrices with zero traces. In this section, the characteristic of K is supposed to be different from 2.

PROPOSITION 6. *Three matrices a, b, and c in $M_2^0(K)$ are independent if and only if the trace of abc is not zero. If it is so, any matrix d in $M_2^0(K)$ decomposes on the base (a, b, c) according to formula* (4).

Proof. If $K = \mathbb{C}$, by continuity, formula (4) holds for any four matrices with zero traces. As this formula is a polynomial identity with integer coefficients linking the entries of matrices a, b, c, and d, it holds for any field K (even of characteristic 2).

The same argument also shows that relation (6) holds for any four matrices and that, for any three matrices, the conclusion of Lemma 2 holds.

If $\overline{abc} \neq 0$, formula (4) gives an expression of any matrix with zero trace as a linear combination of a, b, and c.

As a matter of fact, as F. Choucroun pointed out to the author, $\overline{abc}$ is the determinant of (a, b, c) with respect to the base $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 1\\ 0 & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & 0\\ 1 & 0\end{smallmatrix}\right)$.

COROLLARY 1. *Given three matrices a, b, and c, the system $(1, a, b, c)$ is a base of $M_2(K)$ if and only if $\Delta_{a,b,c} = (\overline{abc} - \overline{acb})^2 \neq 0$. If it is so, any matrix d can be written as $d = \alpha a + \beta b + \gamma c + \delta$, where coefficients α, β, γ, and δ are linear combinations of $\bar{d}$, $\overline{ad}$, $\overline{bd}$, and $\overline{cd}$, the coefficients of which are rational fractions (with integer coefficients) in the variables $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, $\bar{a}$, $\bar{b}$, $\bar{c}$, $\overline{ab}$, $\overline{ac}$, $\overline{bc}$, and $\overline{abc}$, the denominators of which are powers of $\Delta_{a,b,c}$ times a power of 2.*

Proof. Apply the preceding theorem to matrices $a - \bar{a}/2$, $b - \bar{b}/2$, $c - \bar{c}/2$, and $d - \bar{d}/2$.

Notice that, due to Proposition 1, $\Delta_{a,b,c}$ is a polynomial with integer coefficients in the variables $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, $\bar{a}$, $\bar{b}$, $\bar{c}$, $\overline{ab}$, $\overline{ac}$, $\overline{bc}$.

COROLLARY 2. *Two matrices a and b span $M_2(K)$ as an algebra if and only if $D_{a,b} = \bar{a}^2\tilde{b} + \bar{b}^2\tilde{a} + \overline{ab}^2 - \bar{a}\bar{b}\overline{ab} - 4\tilde{a}\tilde{b} \neq 0$.*

Proof. It suffices to express that $a - \bar{a}/2$, $b - \bar{b}/2$, and $ab - \overline{ab}/2$ are independent.

LEMMA 3. *If a and b are two elements of $M_2^0(K)$, then there exist α and β in K such that $\overline{ab}^2 - 4\tilde{a}\tilde{b} = 4\alpha^2\tilde{a} + \beta^2$.*

Proof. If $\tilde{a} \neq 0$, up to conjugation, one may assume that $a = \left(\begin{smallmatrix}0 & \tilde{a}\\ -1 & 0\end{smallmatrix}\right)$. Then $b = \left(\begin{smallmatrix}\alpha & u\\ v & -\alpha\end{smallmatrix}\right)$, with $\alpha^2 + uv = -\tilde{b}$ and $v\tilde{a} - u = \overline{ab}$. One obtains the relation $v^2\tilde{a} - \overline{ab}v + \alpha^2 + \tilde{b} = 0$, from which one can deduce the result.

LEMMA 4. *If d_a, d_b, and y_{ab} are three elements in K, there exist two matrices a and b in $M_2^0(K)$ such that $\tilde{a} = d_a$, $\tilde{b} = d_b$, and $\overline{ab} = y_{ab}$ if and only if there exist two elements α and β in K such that $y_{ab}^2 - 4d_a d_b = \alpha^2 d_a + \beta^2$.*

Proof. If $d_a \neq 0$, take

$$a = \begin{pmatrix} 0 & d_a \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad b = \frac{1}{2}\begin{pmatrix} \alpha & \beta - y_{ab} \\ (\beta + y_{ab})/d_a & -\alpha \end{pmatrix}.$$

If $d_a = 0$ and $y_{ab} \neq 0$, take $a = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & y_{ab} \\ -d_b/y_{ab} & 0 \end{smallmatrix}\right)$.

If $d_a = y_{ab} = 0$, take $a = 0$ and $b = \left(\begin{smallmatrix} 0 & d_b \\ -1 & 0 \end{smallmatrix}\right)$.

PROPOSITION 7. *If one can extract square roots in K, given seven elements in K, y_{ab}, y_{bc}, y_{ca}, d_a, d_b, d_c, and z such that*

$$z^2 + y_{ab}^2 d_c + y_{bc}^2 d_a + y_{ca}^2 d_b + y_{ab} y_{bc} y_{ca} - 4 d_a d_b d_c = 0, \tag{8}$$

then there exist three matrices a, b, and c in $M_2^0(K)$ such that $\overline{ab} = y_{ab}$, $\overline{bc} = y_{bc}$, $\overline{ca} = y_{ca}$, $\tilde{a} = d_a$, $\tilde{b} = d_b$, $\tilde{c} = d_c$, and $\overline{abc} = z$.

Proof. If $y_{ab}^2 - 4 d_a d_b \neq 0$, one chooses (Lemma 4) two matrices a and b such that $\tilde{a} = d_a$, $\tilde{b} = d_b$, and $\overline{ab} = y_{ab}$. One has $\overline{ab(ab - \overline{ab}/2)} = (\overline{ab}^2 - 4\tilde{a}\tilde{b})/2 \neq 0$. Proposition 5, applied to a, b, and $ab - \overline{ab}/2$, gives a matrix c such that $\bar{c} = 0$, $\overline{ac} = y_{ac}$, $\overline{bc} = y_{bc}$, and $\overline{(ab - \overline{ab}/2)c} = z$. In this case, once matrices a and b are chosen, the matrix c is unique.

If $y_{ab}^2 - 4 d_a d_b = y_{bc}^2 - 4 d_b d_c = y_{ca}^2 - 4 d_c d_a = 0$, there are three alternatives.

If $z \neq 0$, set $y'_{ab} = y_{ab} + y_{bc}$, $y'_{bc} = y_{bc}$, $y'_{ca} = y_{ca} - 2d_c$, $d'_a = d_a + d_c - y_{ca}$, $d'_b = d_b$, $d'_c = d_c$, and $z' = z$. The dashed letters also fulfill relation (8). Moreover, one has $y'^2_{ab} - 4 d'_a d'_b \neq 0$. Then one constructs, as previously, three matrices a', b', and c'. Matrices $a = a' - c'$, $b = b'$, and $c = c'$ answer the question.

If $z = 0$ and $d_a d_b d_c \neq 0$, one can take for a, b, and c matrices of the form $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$.

If $z = 0$ and if, for instance, $d_a = 0$, one can take for a, b, and c the matrices 0, $\left(\begin{smallmatrix} 0 & -d_b \\ 1 & 0 \end{smallmatrix}\right)$, and

$$\begin{pmatrix} \sqrt{-d_c} & y_{bc} \\ 0 & -\sqrt{-d_c} \end{pmatrix}.$$

Consider the polynomial

$$\begin{aligned} &\Lambda(x_1, x_2, x_3, y_{12}, y_{13}, y_{23}, z) \\ &\quad = z^2 - (x_1 y_{23} + x_2 y_{13} + x_3 y_{12} - x_1 x_2 x_3) z + x_1^2 + x_2^2 + x_3^2 + y_{23}^2 \\ &\qquad + y_{13}^2 + y_{12}^2 - x_1 x_2 y_{12} - x_2 x_3 y_{23} - x_3 x_1 y_{13} + y_{23} y_{13} y_{12} - 4 \end{aligned}$$

and its discriminant $\Delta(x_1, x_2, x_3, y_{12}, y_{13}, y_{23})$ with respect to z.

Let $\mathscr{K}$ denote the quotient field of $\mathbb{Z}[x_1, x_2, x_3, y_{12}, y_{13}, y_{23}, z]/\Lambda$.

If $n \geq 3$, a polynomial $P \in \mathscr{K}[x_j,\ 4 \leq j \leq n;\ y_{jk},\ 1 \leq j \leq 3,\ 4 \leq k \leq n]$ will be also denoted by $P(x_j,\ 1 \leq j \leq n;\ y_{jk},\ 1 \leq j \leq 3,\ j < k \leq n;\ z)$.

Given four unimodular 2×2-matrices A_1, A_2, A_3, and B, the left hand side, multiplied by a suitable power of 2, of the identity obtained by replacing in (6) a, b, c, and d respectively by $A_1 - \overline{A_1}/2$, $A_2 - \overline{A_2}/2$, $A_3 - \overline{A_3}/2$, and $B - \overline{B}/2$ is a polynomial ξ with integer coefficients in the variables $x_1 = \overline{A_1}$, $x_2 = \overline{A_2}$, $x_3 = \overline{A_3}$, $u = \overline{B}$, $y_{12} = \overline{A_1 A_2}$, $y_{13} = \overline{A_1 A_3}$, $y_{23} = \overline{A_2 A_3}$, $v_1 = \overline{A_1 B}$, $v_2 = \overline{A_2 B}$, and $v_3 = \overline{A_3 B}$. Let ξ be viewed as an element of $\mathscr{K}[u, v_1, v_2, v_3]$ and let $\mathscr{I}$ denote the ideal of $\mathscr{K}[x_j,\ 4 \leq j \leq n;\ y_{jk},\ 1 \leq j \leq 3,\ 4 \leq k \leq n]$ generated by the $n - 3$ polynomials $\xi(x_j, y_{1j}, y_{2j}, y_{3j})$ $(3 < j \leq n)$.

THEOREM 2. *Given an element w of the free group $\Gamma_{\langle a_1, a_2, \dots, a_n\rangle}$, there exists a polynomial $P_w \in \mathscr{K}[x_j,\ 4 \leq j \leq n;\ y_{jk},\ 1 \leq j \leq 3,\ 4 \leq k \leq n]$, which is unique modulo $\mathscr{I}$ if K is infinite, and such that, for any representation φ of $\Gamma_{\langle a_1, a_2, \dots, a_n\rangle}$ in $SL(2, K)$ such that $\Delta\Big(\overline{\varphi(a_1)}, \overline{\varphi(a_2)}, \overline{\varphi(a_3)}, \overline{\varphi(a_1 a_2)}, \overline{\varphi(a_1 a_3)}, \overline{\varphi(a_2 a_3)}\Big) \neq 0$, one has*

$$\operatorname{tr} \varphi(w) = P_w\Big(\overline{\varphi(a_j)},\ 1 \leq j \leq n;\ \overline{\varphi(a_j a_k)},\ 1 \leq j \leq 3,\ j < k \leq n;\ \overline{\varphi(a_1 a_2 a_3)}\Big).$$

This statement improves on [5, Theorem 2.2]. Indeed, there is no need for the hypothesis $\overline{\varphi(a_1)}^2 + \overline{\varphi(a_2)}^2 + \overline{\varphi(a_1 a_2)}^2 - \overline{\varphi(a_1)}\,\overline{\varphi(a_2)}\,\overline{\varphi(a_1 a_2)} - 4 \neq 0$ which is the reformulation in our setting of the hypothesis $D(\varphi(a_1), \varphi(a_2)) \neq 2$ assumed in [5].

Proof. Let us first prove the existence of P_w. It results from Theorem 1 that, for $j > 3$, the matrix $\varphi(a_j)$ can be written as $\alpha + \beta_1 \varphi(a_1) + \beta_2 \varphi(a_2) + \beta_3 \varphi(a_3)$, where the coefficients α, β_1, β_2, and β_3 are linear combinations of $\overline{\varphi(a_j)}$, $\overline{\varphi(a_1 a_j)}$, $\overline{\varphi(a_2 a_j)}$, and $\overline{\varphi(a_3 a_j)}$, the coefficients of which are rational fractions in the variables $\overline{\varphi(a_1)}$, $\overline{\varphi(a_2)}$, $\overline{\varphi(a_3)}$, $\overline{\varphi(a_1 a_2)}$, $\overline{\varphi(a_1 a_3)}$, $\overline{\varphi(a_2 a_3)}$, and $\overline{\varphi(a_1 a_2 a_3)}$. The same fact holds for $\varphi(a_j^{-1})$, because $\varphi(a_j^{-1}) = \overline{\varphi(a_j)} - \varphi(a_j)$. One ends by using the corollary to Lemma 2.

Uniqueness results from Propositions 1, 3, 7, and 5.

IV. THE CASE OF CHARACTERISTIC 2

Now, the characteristic of K equals 2 and $\mathscr{A}$ is an associative and unitary algebra with elements having a minimal polynomial of degree at most 2. As previously, $\mathscr{A}_0$ stands for the kernel of the trace. This time, the unit belongs to $\mathscr{A}_0$.

LEMMA 5. *For any a, b, and c in $\mathscr{A}$, one has*

$$\overline{bc}a + \overline{ca}b + \overline{ab}c + \bar{a}bc + \bar{b}ca + \bar{c}ab + \overline{abc} = 0. \tag{9}$$

Proof. This follows the proof of formula (7).

THEOREM 3. (1) *If there exists a and b in $\mathscr{A}_0$ such that $\overline{ab} \neq 0$, then $\dim \mathscr{A} = 4$ and $\mathscr{A}$ is generated, as a unitary algebra, by a and b. Moreover, if K is algebraically closed, $\mathscr{A}$ is isomorphic to $M_2(K)$.*

(2) *If, for any a and b in $\mathscr{A}_0$ one has $\overline{ab} = 0$, then $\mathscr{A}_0$ is a commutative algebra. Moreover, if there exists f in $\mathscr{A} \setminus \mathscr{A}_0$, the set $\mathscr{I} = \{a \in \mathscr{A}_0 \mid \overline{af} = 0\}$ is a two-sided ideal of codimension 2, of dimension ≥ 2, and the product of any two elements of $\mathscr{I}$ is zero.*

Proof. Let us prove assertion (1). Due to formula (9), for any $c \in \mathscr{A}_0$, one has $c = (\overline{abc} + \overline{bc}a + \overline{ca}b)/\overline{ab}$, which proves that $\{1, a, b, ab\}$ is a base for $\mathscr{A}$.

If one can find a' and b' in $\mathscr{A}_0$ such that $a'^2 = b'^2 = 0$ and $(a'b')^2 = a'b'$, then the map $a \mapsto \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $b \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ extends as an isomorphism of unitary algebras from $\mathscr{A}$ to $M_2(K)$. If $\tilde{a} \neq 0$ or $\tilde{b} \neq 0$, this is possible if the equation $\tilde{a}t^2 + \overline{ab}tu + \tilde{b}u^2 = 0$ has two distinct projective roots.

Now suppose that $\overline{ab} = 0$ for all a and b in $\mathscr{A}_0$. It results from formula (1) that $ab = ba$ for all a and b in $\mathscr{A}_0$.

If $\mathscr{A} = \mathscr{A}_0$, there is not much to say. So, from now on, we suppose that there exists $f \in \mathscr{A}$ such that $\bar{f} \neq 0$. We may assume that $\bar{f} = 1$.

Let $\mathscr{I}$ stand for the set $\{a \in \mathscr{A}_0 \mid \overline{af} = 0\}$. This is a subspace of codimension 1 in $\mathscr{A}_0$ (indeed, $1 \in \mathscr{A}_0 \setminus \mathscr{I}$).

If $a \in \mathscr{I}$, one has $fa = af + a$, $(af)f = af^2 = af + \tilde{f}a$. This means that af and fa are in $\mathscr{I}$.

If a and b are elements of $\mathscr{I}$, one has $ab = \overline{abf}$ (due to formula (9)), therefore $ab \in \mathscr{A}_0$; moreover, one has $\tilde{a}b = a^2b = a(ab) = \overline{abf}a$, which means that if $\dim \mathscr{I} > 1$, the product of any two elements of $\mathscr{I}$ is 0.

If $\dim \mathscr{I} = 1$ and if a is a non-zero element of $\mathscr{I}$, one has $af = \lambda a$. Then $(af)a = \lambda \tilde{a}$ whereas $a(fa) = a(af + a) = (\lambda + 1)\tilde{a}$. This means that $\tilde{a} = 0$.

For the sake of completeness, we give the analogues of formulas (4) and (6) in characteristic 2.

PROPOSITION 8. *Let a_1, a_2, a_3, and a_4 be four elements in $M_2(K)$. Then*

$$\begin{aligned}
&\left(\overline{a_2}\,\overline{a_3}\,\overline{a_4} + \overline{a_2}\,\overline{a_3a_4} + \overline{a_3}\,\overline{a_2a_4} + \overline{a_4}\,\overline{a_2a_3}\right)a_1 + \textit{three similar terms}\\
&\qquad + \overline{a_1}\,\overline{a_2}\,\overline{a_3a_4} + \textit{five similar terms}\\
&\qquad + \overline{a_1a_2}\,\overline{a_3a_4} + \textit{two similar terms}\\
&\qquad + \overline{a_1}\,\overline{a_2}\,\overline{a_3}\,\overline{a_4} = 0
\end{aligned}$$

and

$$\begin{aligned}
&\left(\overline{a_2}\,\overline{a_3}\,\overline{a_4} + \overline{a_2}\,\overline{a_3a_4} + \overline{a_3}\,\overline{a_2a_4} + \overline{a_4}\,\overline{a_2a_3}\right)^2 \tilde{a}_1 + \textit{three similar terms}\\
&\qquad + \overline{a_1}\,\overline{a_2}\,\overline{a_3}\,\overline{a_4}\left(\overline{a_1}\,\overline{a_2}\,\overline{a_3a_4} + \textit{five similar terms}\right)\\
&\qquad + \overline{a_1}^2\,\overline{a_2}\,\overline{a_3}\,\overline{a_2a_4}\,\overline{a_3a_4} + \textit{eleven similar terms}\\
&\qquad + \overline{a_1}\,\overline{a_2}\,\overline{a_3a_4}\left(\overline{a_1a_2}\,\overline{a_3a_4} + \overline{a_1a_3}\,\overline{a_2a_4} + \overline{a_1a_4}\,\overline{a_2a_3}\right) + \textit{five similar terms}\\
&\qquad + \overline{a_1}^2\,\overline{a_2a_3}\,\overline{a_2a_4}\,\overline{a_3a_4} + \textit{three similar terms}\\
&\qquad + \left(\overline{a_1a_2}\,\overline{a_3a_4} + \overline{a_1a_3}\,\overline{a_2a_4} + \overline{a_1a_4}\,\overline{a_2a_3} + \overline{a_1}\,\overline{a_2}\,\overline{a_3}\,\overline{a_4}\right)^2 = 0.
\end{aligned}$$

Proof. Assume for a moment that $K = \mathbb{C}$, consider four matrices a_1, a_2, a_3, and a_4, replace a by $a_1 - \overline{a_1}$, b by $a_2 - \overline{a_2}$, c by $a_3 - \overline{a_3}$, and d by $a_4 - \overline{a_4}$ in formulas (4) and (6), and multiply each of the obtained identities by a suitable power of 2 so as to have no denominators. Then by taking these identities modulo 2, one gets the above formulas.

Of course, there is an analogue of Theorem 2 for representations of $\Gamma_{\langle a_1, a_2, \dots, a_n\rangle}$ in $SL(2, K)$ when the characteristic of K equals 2.

REFERENCES

1. Y. Avishai, D. Berend, and D. Glaubman, Minimum-dimension trace maps for substitution sequences, *Phys. Rev. Lett.* **72** (1994), 1842–1845.
2. Y. Avishai, D. Berend, and V. Tkachenko, Trace maps, *Internat. J. Modern Phys. B* **11** (1997), 3525–3542.
3. R. Fricke and F. Klein, "Vorlesungen über die Theorie der automorphen Functionen," Teubner, Leipzig, 1897; reprint, Academic Press, New York, 1965.
4. R. D. Horowitz, Characters of free groups represented in the two-dimensional special linear group, *Comm. Pure Appl. Math* **25** (1972), 635–649.

5. W. Magnus, Rings of Fricke characters and automorphism groups of free groups, *Math. Z.* **170** (1980), 91–103.
6. J. Peyrière, Trace maps, *in* "Beyond Quasicrystals" (F. Axel and D. Gratias, Eds.), pp. 465–480, Editions de Physique and Springer-Verlag, New York/Berlin, 1995.
7. J. Peyrière, Z. W. Wen, and Z. Y. Wen, Polynômes associés aux endomorphismes de groupes libres, *Enseign. Math.* **33** (1993), 153–175.
8. C. Procesi, The invariant theory of $n \times n$ matrices, *Adv. Math.* **19** (1976), 306–381.
9. Ju. P. Razmyslov, Trace identities of full matrix algebras over a field of characteristic zero, *Izv. Akad. Nauk SSSR Ser. Mat.* **38**, No. 4 (1974) [In Russian]; English translation, *Math. USSR Izv.* **8** (1974), 727–760.
10. Z. X. Wen, Relations polynomiales entre les traces de produits de matrices, *C. R. Acad. Sci. Paris Sér. I* **318** (1994), 99–104.
11. A. Whittemore, On special linear characters of free groups of rank $n \geq 4$, *Proc. Amer. Math. Soc.* **40** (1973), 383–388.