**Associative Subalgebras of the Griess Algebra**

Werner Meyer and Wolfram Neutsch

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

MPI/90-64

**Non-Archimedean $L$-Functions**

**Associated with Siegel and Hilbert Modular Forms**

by

A.A.Panchishkin

| | | |
|---|---|---|
| Max-Planck-Institut<br>für Mathematik<br>Gottfried-Claren-Straße 26<br>D-5300 Bonn 3 | und | Moskauer Staatsuniversität<br>Mechanisch-Mathematische<br>Fakultät<br>119899 Moskau |

11.7.1990

# Associative Subalgebras of the Griess Algebra


Werner Meyer and Wolfram Neutsch

Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 3
Federal Republic of Germany

**Associative Subalgebras of the Griess Algebra**

by Werner Meyer and Wolfram Neutsch

**Abstract**

The structure of the Griess algebra $\mathfrak{G}$, whose automorphism group is the Fischer-Griess monster $F_1$, is investigated.
We show the existence of 48-dimensional associative subalgebras in $\mathfrak{G}$ and furthermore demonstrate that they are not contained in strictly larger ones.
It is conjectured that the given explicit examples are of maximal possible dimension among all associative subalgebras in $\mathfrak{G}$. This depends on the validity of a certain inequality.

## Known Results

In this section we compile a number of known results concerning properties of the Griess algebra. Proofs can be found in the literature, especially in Griess [1982] and Conway [1984]; see also Conway et al. [1985], henceforth referred to as the "ATLAS".

The largest sporadic group, the Monster $F_1$, of order

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \qquad (1)$$

has a minimal representation in characteristic 0 of degree

$$196883 \;=\; 47\cdot 59\cdot 71 \qquad (2)$$

which can be realised over the field $\mathbb{Q}$ of rational numbers (Griess [1982]). The character table shows that the trivial representation $\underline{1}$ as well as $\underline{196883}$ itself are contained exactly once in the symmetric square $S^2(\underline{196883})$: the precise decomposition is

$$S^2(\underline{196883}) \;=\; \underline{1} \oplus \underline{196883} \oplus \underline{842609326} \oplus \underline{18538750076} \qquad (3)$$

This implies the existence of a nontrivial $F_1$-invariant inner product and an $F_1$-invariant algebra (the **"Griess algebra"** $\mathfrak{G}$) with unit element 1 on an $\mathbb{R}$-vector space V of dimension 196884, on which the Monster acts as

$$\underline{1} \oplus \underline{196883} \qquad (4)$$

Since the above-mentioned characters lie in the symmetric part of the tensor square of $\underline{196883}$, the inner product

$$\langle .,. \rangle : \quad V \times V \longrightarrow \mathbb{R} \qquad (5)$$

is symmetric: For all $a, b \in V$,

$$\langle a,b\rangle = \langle b,a\rangle \tag{6}$$

Conway chooses it to be positive definite:

$$\langle a,a\rangle > 0 \tag{7}$$

if $a \neq 0$.

For the same reason the algebra product, here denoted by a dot oder by concatenation of the factors, is commutative:

$$a\cdot b = b\cdot a \tag{8}$$

and, since $\underline{1}$ also is contained exactly once in $\underline{196883}^3$ (namely in $S^3(\underline{196883})$), the inner product must be associative with respect to the algebra,

$$\langle a\cdot b,c\rangle = \langle a,b\cdot c\rangle \tag{9}$$

The algebra itself, however, is not associative.

Theorem 1 (Norton):

For two arbitrary vectors a, b the **Norton inequality**

$$\langle a^2,b^2\rangle \geq \langle a\cdot b,a\cdot b\rangle \tag{10}$$

holds.

Definition 1 (Conway [1984]):

Two elements a, b in $\mathfrak{S}$ **associate** if for all $x \in V$:

$$a\cdot(x\cdot b) = (a\cdot x)\cdot b \tag{11}$$

This is clearly tantamount to the commutativity of $ad_a$ and $ad_b$.

One says, a **alternates** with b, if the last equation is fulfilled for x = a,

$$a\cdot(a\cdot b) \quad = \quad a^2\cdot b \tag{12}$$

We use the notation of the ATLAS with the single exception that we choose $\langle .,. \rangle$ as twice the Conway product.

Of fundamental importance is the remarkable

<u>Theorem 2 (Norton):</u>

The following three assertions are equivalent:

(a) We have equality in Norton's formula,

$$\langle a^2, b^2 \rangle \quad = \quad \langle ab, ab \rangle \tag{13}$$

(b) a and b associate;

(c) a alternates with b (or vice versa).

<u>Definition 2 (Conway):</u>

An element which associates with its square is called a **Jordan element**. Trivially, the multiples of idempotents are Jordan.

<u>Theorem 3 (Conway):</u>

Let

$$F \quad = \quad \mathrm{Aut}\ \mathfrak{G} \tag{14}$$

be the automorphism group of the Griess algebra. Then the scalar product is invariant under F, because it can be calculated from the algebra product via

$$\mathrm{tr}(\mathrm{ad}_a \mathrm{ad}_b) \quad = \quad 20336\ \langle a,1\rangle\ \langle b,1\rangle + 4620\ \langle a,b\rangle \tag{15}$$

F is finite; more precisely,

$$F \cong F_1 \qquad (16)$$

We associate to each **transposition** (= 2A-element in F) $\alpha$ an idempotent $i_\alpha$ ("**transposition idempotent**" of $\alpha$) which lies in the (2-dimensional) fix space of

$$C_F(\alpha) \cong 2{\wedge}F_2 \qquad (17)$$

in $\mathfrak{G}$ such that the **transposition axis** $t_\alpha$ described in Conway [1984] is a multiple of $i_\alpha$,

$$a = t_\alpha = 64\, i_\alpha \qquad (18)$$

The axis a fulfills the conditions

$$a \cdot a = 64\, a \qquad (19)$$

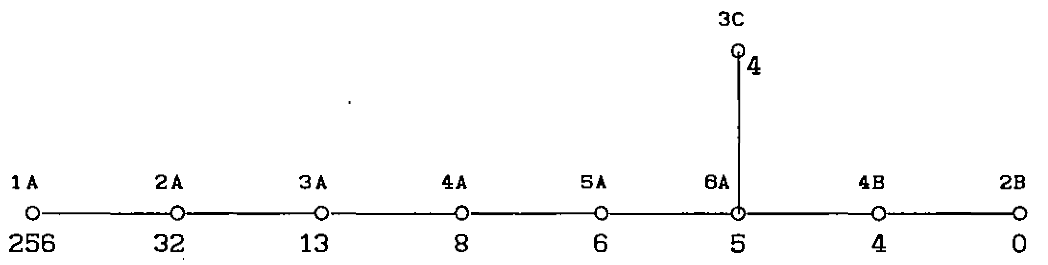
and

$$\langle a, a \rangle = 256 \qquad (20)$$

The fix space of $ad(i_\alpha)$ is one-dimensional.
We can proceed in the same way for 3A-elements $\tau$ instead of transpositions. This gives idempotents $i_\tau$ with norm $\frac{1}{10}$.
We also mention the important fact (Conway [1984]) that F acts by conjugation as a rank-9-permutation group on the transpositions and that the product of two transpositions is contained in one of the $F_1$-classes

$$1A, 2A, 2B, 3A, 3C, 4A, 4B, 5A, 6A \qquad (21)$$

By an observation of McKay, these classes can be associated in a natural way with the nodes of the extended $E_8$ Dynkin diagram:




(22)

The numbers attached to the nodes are the inner products of $t_\alpha$ and $t_\beta$, where $\alpha$ and $\beta$ are transpositions whose product is in the appropriate class of $F_1$.

<u>Theorem 4 (Norton):</u>

The lattice $\Gamma$ which is spanned (as a $\mathbb{Z}$-module) by all vectors of the form 1, t, t·t', (here t and t' denote arbitrary transposition axes), is closed under the algebra product,

$$\Gamma \cdot \Gamma \subseteq \Gamma \qquad (23)$$

and integer with respect to <.,.>,

$$\langle \Gamma, \Gamma \rangle \subseteq \mathbb{Z} \qquad (24)$$

The dual factor $\Gamma^*/\Gamma$ of $\Gamma$ is cyclic, and $|\Gamma^*/\Gamma|$ is a power of 4. Conway [1984] conjectures that $\Gamma$ is unimodular.

**Associative Subalgebras**

The main obstacle for the study of the interior structure of $\mathfrak{G}$ is - besides the large dimension - its non-associativity. It is therefore natural to consider associative subalgebras.
Obviously all vectors in such a subalgebra are power-associative, or, what amounts to the same, Jordan elements.
In order to investigate the structure of associative subalgebras of $\mathfrak{G}$ we need the easy

Lemma 1:
(a) The only nilpotent Jordan element in $\mathfrak{G}$ is 0;
(b) There is no subalgebra in $\mathfrak{G}$ isomorphic to $\mathbb{C}$;
(c) Two idempotent elements a and b annihilate each other if and only if they are perpendicular.
(d) If $i \in \mathfrak{G}$ is idempotent,

$$i^2 = i \qquad (25)$$

the norm $\langle i, i \rangle$ of $i$ lies between 0 and 3 (incl.). The extremal values occur only for $i \in \{0, 1\}$.
(e) For all $a, b \in \mathfrak{G}$,

$$\langle a, b \rangle^2 \leq \langle a, a \rangle \langle b, b \rangle \qquad (26)$$

**(Schwarz' inequality)**.

Proof:
(a) If $x \in \mathfrak{G}^\# = \mathfrak{G} \setminus \{0\}$ is nilpotent and Jordan, there exists a $k > 0$ such that $x^k \neq 0$ and $x^{k+1} = x^{k+2} = \ldots = 0$. This gives

$$\langle x^k, x^k \rangle = \langle x^k, x^k \cdot 1 \rangle = \langle x^{2k}, 1 \rangle = \langle 0, 1 \rangle = 0 \qquad (27)$$

Hence

$$x^k = 0 \tag{28}$$

which contradicts the assumption.

(b) A subalgebra isomorphic to $\mathbb{C}$ would be generated by nonzero vectors e and i, obeying the conditions

$$e \cdot e = e; \qquad e \cdot i = i \cdot e = i; \qquad i \cdot i = -e \tag{29}$$

But then we would have

$$\langle i,i \rangle = \langle i, i \cdot e \rangle = \langle i^2, e \rangle = \langle -e, e \rangle = -\langle e,e \rangle < 0 \tag{30}$$

which is clearly impossible.

(c) From

$$a^2 = a; \qquad b^2 = b \tag{31}$$

and

$$a \cdot b = 0 \tag{32}$$

it follows that

$$\langle a,b \rangle = \langle a \cdot a, b \rangle = \langle a, a \cdot b \rangle = 0 \tag{33}$$

The orthogonality of a and b implies

$$0 = \langle a,b \rangle = \langle a^2, b^2 \rangle \geq \langle ab, ab \rangle \tag{34}$$

by Norton's inequality, whence the proposition.

(d) is trivial if $i \in \{0,1\}$. Otherwise, the subalgebra generated by 1 and i is associative and 2-dimensional. 1-i has the same properties as i. In particular,

$$\langle i, 1-i \rangle = 0 \tag{35}$$

and

$$3 = \langle 1, 1 \rangle = \langle i, i \rangle + \langle 1-i, 1-i \rangle \tag{36}$$

which implies the assertion.

(e) is a well-known general property of positive definite scalar products.

The above lemma immediately provides us with the structure of associative subalgebras:

Theorem 5:

Let $\mathfrak{U}$ be a k-dimensional associative subalgebra of the Griess algebra $\mathfrak{G}$. Then

(a) $\mathfrak{U}$ is isomorphic (as a ring) to the direct sum of k copies of $\mathbb{R}$:

$$\mathfrak{U} \cong \mathbb{R}^k \tag{37}$$

(b) $\mathfrak{U}$ contains a basis of k mutually annihilating idempotent elements which are orthogonal to each other:

$$a_i \cdot a_j = 0 \tag{38}$$

and

$$\langle a_i, a_j \rangle = 0 \tag{39}$$

for all $i, j \in \{1, \ldots, k\}$ with $i \neq j$.

(c) The idempotent elements in $\mathfrak{U}$ are the partial sums of the $a_i$ (and vice versa). In particular, there are exactly $2^k$ idempotents in $\mathfrak{U}$, including the zero element 0.

$$\left\{a_1, \ldots, a_k\right\} \tag{40}$$

is the only orthogonal basis among them. We shall call the $a_i$ the **basic** (or **fundamental**) **idempotents** of $\mathfrak{U}$.

Proof:

As an associative algebra, $\mathfrak{U}$ contains only Jordan elements. By part (a) of Lemma 1, the Jacobson radical of $\mathfrak{U}$ is therefore zero. Hence $\mathfrak{U}$ is semisimple and thus a direct sum of fields of finite dimension over $\mathbb{R}$, i. e. of algebras isomorphic with $\mathbb{R}$ or $\mathbb{C}$. But $\mathbb{C}$ cannot occur by part (b) of Lemma 1. This proves (a), while (b) is just the same, except for the orthogonality of the basic idempotents. The latter proposition, however, is a consequence of

$$\langle a_i, a_j \rangle = \langle a_i \cdot a_i, a_j \rangle = \langle a_i, a_i \cdot a_j \rangle = \langle a_i, 0 \rangle = 0 \qquad (41)$$

for all $i \neq j$. (c) follows trivially from the structure of $\mathbb{R}^k$.

All associative subalgebras of $\mathfrak{G}$ are thus generated by systems of mutually perpendicular idempotent elements. It is therefore of great interest to investigate the properties of idempotents in $\mathfrak{G}$. First we find

Theorem 6:

Let $\alpha$ and $\beta$ be two different transpositions and

$$a = i_\alpha \qquad (42)$$

and

$$b = i_\beta \qquad (43)$$

the associated idempotents. Then the following statements are equivalent:

(a) In the Norton formula for a and b, equality holds,

$$\langle a^2, b^2 \rangle = \langle ab, ab \rangle \qquad (44)$$

(b) a and b associate with each other: for all $x \in \mathfrak{G}$,

$$a\cdot(x\cdot b) \;=\; (a\cdot x)\cdot b \tag{45}$$

(c) a alternates with b,

$$a\cdot(a\cdot b) \;=\; a^2\cdot b \tag{46}$$

(d) b alternates with a,

$$(a\cdot b)\cdot b \;=\; a\cdot b^2 \tag{47}$$

(e) a and b annihilate each other,

$$a\cdot b \;=\; 0 \tag{48}$$

(f) a and b are orthogonal,

$$\langle a, b\rangle \;=\; 0 \tag{49}$$

(g) The product $\alpha\beta$ is a central $F_1$-involution,

$$\alpha\beta \in 2B \tag{50}$$

Proof:

The first four properties are equivalent by Theorem 2, as well as the remaining three by equation (22) and Lemma 1.c.

From (c), we get the eigenvalue relation

$$a\cdot(a\cdot b) \;=\; a^2\cdot b \;=\; a\cdot b \tag{51}$$

and deduce that $a\cdot b$ is a fixed vector af $ad_a$ and thus linearly dependent of a; similarly (with the rôles of a and b interchanged) of b. This is only possible if

$$a\cdot b \;=\; 0 \tag{52}$$

which is (e). The reverse inclusion (e) $\Rightarrow$ (c) is trivial.

A simple consequence is

Corollary 1:
Let $\alpha_1,\ldots,\alpha_k \in 2A$ be pairwise different transpositions and $a_1,\ldots,a_k$ the corresponding idempotents.
The subalgebra $\mathfrak{U}$ of $\mathfrak{G}$ which is generated by $a_1,\ldots,a_k$ is associative if and only if for all $i,j \in \{1,\ldots,k\}$ with $i \neq j$,

$$\alpha_i\alpha_j \in 2B \tag{53}$$

is true. In this case

$$\left\{4\ a_1,\ \ldots\ ,4\ a_k\right\} \tag{54}$$

is an orthonormal basis of $\mathfrak{U}$; in particular

$$\dim \mathfrak{U} \;=\; k \tag{55}$$

Furthermore, $E = \langle\alpha_1,\ldots,\alpha_k\rangle$ is an elementary abelian 2-subgroup of $F_1$.

Proof:
Trivial.

We can now give an upper bound for the dimensions of associative subalgebras of $\mathfrak{G}$ which are generated by transposition axes:

Theorem 7:
(a) For any associative $\mathfrak{G}$-subalgebra $\mathfrak{U}$, which is generated by transposition idempotents,

$$\dim \mathfrak{U} \leq 48 \tag{56}$$

(b) Every system of 49 commuting transpositions in $F_1$ contains at least two whose product is also in the class 2A.

Proof:

Part (b) immediately follows from (a), Corollary 1, and the fact that all $F_1$-involutions lie in either 2A or 2B.

To verify the first statement, we again denote the transposition idempotents by $a_1, \ldots, a_k$, where

$$k = \dim \mathfrak{U} \tag{57}$$

By Theorem 4,

$$\left\{a_1, \ldots, a_k\right\} \tag{58}$$

are the basic idempotents, and all of them have the norm

$$\frac{256}{64^2} = \frac{1}{16} \tag{59}$$

The longest idempotent in $\mathfrak{U}$ is

$$e = \sum_{i=1}^{k} a_i \tag{60}$$

with norm

$$\langle e, e \rangle = \frac{k}{16} \leq 3 \tag{61}$$

(cf Lemma 1.d).

The last formula immediately leads to

$$k \leq 48 \qquad (62)$$

as required.

We notice that the extremal possibility (dimension = 48) can only arise if $1 \in \mathfrak{U}$. The given bound is sharp:

Theorem 8:
There are 48 transpositions in $F_1$ whose pairwise products are in 2B.

Proof:
In the subgroup

$$O_2(C_F(2B)) \cong 2_+^{1+24} \qquad (63)$$

the central factor corresponds to the quotient of the Leech lattice $\Lambda$ by its double $(2\Lambda)$. On it, the group

$$C_F(2B)/O_2(C_F(2B)) \cong Co_1 \qquad (64)$$

acts in a natural way.
The $\Lambda/2\Lambda$-classes may be described by giving the type (Conway [1971]) of the shortest vectors they contain.
Classes of type 2 are associated with 2 transpositions each, those of type 3 with 2 elements of order 4, and those of type 4 with pairs of involutions in 2B. Thus it suffices to choose 24 vectors $v_1, \ldots, v_{24}$ in $\Lambda$ (mod $2\Lambda$) such that the sum of any two of them is of type 4. This is tantamount to the orthogonality (in $\Lambda$) of the $v_i$.
It is easy to find such a set of vectors, for instance

$$(4,4,0^{22}),\ (4,-4,0^{22});\ (0^2,4,4,0^{20}),\ (0^2,4,-4,0^{20});\ \ldots \qquad (65)$$

in the notation of the ATLAS.
The corresponding transposition vectors indeed have 1 as their sum.

The same argument also shows that associative $\mathfrak{G}$-subalgebras of higher dimensions than 48 can only exist if there are nonvanishing idempotents with norm smaller than $\frac{3}{48} = \frac{1}{16}$. It is thus natural to seek the shortest idempotents $\neq 0$ in $\mathfrak{G}$.
This is equivalent to determining the maxima of the function

$$F : \mathfrak{G}^{\#} = \mathfrak{G} \setminus \{0\} \longrightarrow \mathbb{R} \tag{66}$$

defined by

$$F(x) = \frac{\langle x^2, x^2 \rangle}{\langle x, x \rangle^2} \tag{67}$$

This formulation of the problem allows us to apply the methods of calculus. We first have:

Lemma 2:
The points a at which F is stationary are characterized by the condition

$$a^3 \in \mathbb{R} \cdot a \tag{68}$$

Proof:
We have to show that for all $\varepsilon \perp a$ the $\varepsilon$-linear terms in $\langle (a+\varepsilon)^2, (a+\varepsilon)^2 \rangle$ vanish. By polarisation we get

$$0 = \langle 2a\varepsilon, a^2 \rangle + \langle a^2, 2a\varepsilon \rangle = 4 \langle a^2, a\varepsilon \rangle = 4 \langle a^3, \varepsilon \rangle \tag{69}$$

that is $\varepsilon \perp a^3$. This implies the assertion of the theorem.

It is easy to determine the minima of F:

Theorem 9:

The minimal value of F is $\frac{1}{3}$ and is attained at all $a \in \mathfrak{G}$ with

$$a^2 \in \mathbb{R}\cdot 1 \tag{70}$$

and nowhere else.

Proof:
The Schwarz inequality leads with $a = 1$ and $b = x^2$ to

$$\langle 1, x^2\rangle^2 \leq \langle 1,1\rangle \langle x^2, x^2\rangle \tag{71}$$

or

$$\langle x, x\rangle^2 \leq 3 \langle x^2, x^2\rangle \tag{72}$$

hence

$$F(x) \geq \frac{1}{3} \tag{73}$$

Equality holds if and only if $x^2$ is linearly dependent of 1.

The calculation of the global maxima of F is considerably more difficult. The stationarity condition of Lemma 2 for F is fulfilled for every idempotent element a. In that case, F(a) is simply reciprocal to $\langle a,a\rangle$.
Choosing a as a transposition idempotent, we find from (59):

$$F(a) = 16 \tag{74}$$

To determine the character of the function in the vicinity of a, we have to develop $F(a+\varepsilon)-F(a)$ up to second order in $\varepsilon$.
Since $ad_a$ is a symmetric operator, we may find a basis of $a^{\perp}$ which consists of eigenvectors of $ad_a$.
Thus we assume $\varepsilon \perp a$ and

$$a\cdot\varepsilon = ad_a(\varepsilon) = \alpha\,\varepsilon \tag{75}$$

with $\alpha \in \mathbb{R}$. To the required degree of approximation,

$$\langle a+\varepsilon, a+\varepsilon\rangle = \langle a,a\rangle + \langle\varepsilon,\varepsilon\rangle = \frac{1}{16}\left[1 + 16\ \langle\varepsilon,\varepsilon\rangle\right] \tag{76}$$

and therefore

$$\langle a+\varepsilon, a+\varepsilon\rangle^{-2} \approx 16^2\left[1 - 32\ \langle\varepsilon,\varepsilon\rangle\right] \tag{77}$$

Furthermore

$$\langle(a+\varepsilon)^2,(a+\varepsilon)^2\rangle = \langle a^2+2\alpha\varepsilon+\varepsilon^2, a^2+2\alpha\varepsilon+\varepsilon^2\rangle \tag{78}$$

from which we deduce the relation

$$\langle(a+\varepsilon)^2,(a+\varepsilon)^2\rangle \approx \frac{1}{16} + (2\alpha+4\alpha^2)\ \langle\varepsilon,\varepsilon\rangle \tag{79}$$

Multiplying both approximations, we get

$$F(a+\varepsilon) - F(a) \approx -16 + 16^2\left[1 - 32\ \langle\varepsilon.\varepsilon\rangle\right]\left[\frac{1}{16} + \left(2\ \alpha + 4\ \alpha^2\right)\ \langle\varepsilon,\varepsilon\rangle\right] \tag{80}$$

or, simpler,

$$F(a+\varepsilon) - F(a) \approx -\ 512\ \langle\varepsilon,\varepsilon\rangle\left(1 - \alpha - 2\ \alpha^2\right) \tag{81}$$

By Conway [1984], the eigenvalues of $ad_a$ on $a^\perp$ are $\frac{1}{4}$, $\frac{1}{32}$, and 0, thus the quadratic form in $\varepsilon$ given by the last formula is negative definite there. We have proved

Theorem 10:
Let a be a transposition vector in $\mathfrak{G}$, in particular $a^2 = a$, $\langle a,a\rangle = \frac{1}{16}$. Then F has a local maximum at a with $F(a) = 16$.

It is unknown if this is the absolute maximum. If so, no nonzero idempotents of smaller norm than $\frac{1}{16}$ could exist, and the largest possible dimension of any associative subalgebra in $\mathfrak{G}$ were 48.
Theorem 11 is sufficient to show that transposition vectors are indecomposable, i. e., they cannot be written as a sum of two or more mutually associating nontrivial idempotents:

Theorem 11:
Transposition idempotents are indecomposable.

Proof:
It is easily seen that a counterexample x could already be expressed as a sum of only two (shorter) vectors e and f with

$$e^2 = e, \quad f^2 = f, \quad e \cdot f = f \cdot e = 0 \tag{82}$$

and (by Lemma 1.c)

$$\langle e,f \rangle = 0 \tag{83}$$

For the sake of brevity we set

$$\alpha = \langle e,e \rangle \tag{84}$$

and

$$\beta = \langle f,f \rangle \tag{85}$$

The subspace spanned by e and f is clearly a 2-dimensional associative algebra. This simplifies the calculation of F(Ae+Bf) for $A,B \in \mathbb{R}$ with A, B not both equalling 0. We find

$$F(Ae+Bf) = \frac{\alpha A^4 + \beta B^4}{(\alpha A^2 + \beta B^2)^2} \tag{86}$$

The vector

$$v = \beta e - \alpha f \tag{87}$$

is perpendicular to

$$x = e + f \tag{88}$$

We arrive at

$$F(x+\delta v) = F((1+\beta\delta)e+(1-\alpha\delta)f) = \frac{\alpha(1+\beta\delta)^4+\beta(1-\alpha\delta)^4}{\left[\alpha(1+\beta\delta)^2+\beta(1-\alpha\delta)^2\right]^2} \tag{89}$$

or - up to terms of $3^{rd}$ and higher order in $\delta$ -

$$F(x+\delta v) \approx 16 \left[1 + 4\,\alpha\,\beta\,\delta^2\right] \tag{90}$$

Since $\alpha$ and $\beta$ are positive (as norms of e and f), this contradicts the fact that F has a local maximum at x.

An immediate consequence is

Corollary 2:

Those 48-dimensional associative $\mathfrak{G}$-subalgebras, which are generated by transposition axes, are maximal associative.

Proof:

Let $\mathfrak{A}$ be an algebra which is spanned by 48 transposition vectors $a_1,\dots,a_{48}$, and $\mathfrak{B}$ associative with $\mathfrak{A} \subset \mathfrak{B} \subseteq \mathfrak{G}$.

The indecomposability of the $a_i$ implies that all of them must be among the basic idempotents $e_1,\dots,e_k$ ($k = \dim \mathfrak{B}$). This is not in concordance with Theorem 5.c and Lemma 1.d, because

$$e_1 + \dots + e_k \tag{91}$$

then would be idempotent with norm > 3.

## Summary

In this paper, we begin a research into the internal properties of the algebra $\mathfrak{G}$ which has been detected by Robert Griess and which was used by him to construct the monster simple group.

We demonstrate that it is possible to construct certain maximal associative subalgebras in $\mathfrak{G}$ (by elementary means).

In particular, 48-dimensional algebras of this type can be found explicitly. It seems that they are best-possible (with respect to dimension). To prove this, it would suffice to show that for all elements $x \in \mathfrak{G}$, the inequality

$$\langle x^2, x^2 \rangle \leq 16 \langle x, x \rangle^2$$

is fulfilled.

In any case, there are other maximal associative algebras in $\mathfrak{G}$, and it would be of great value to enumerate them completely. This, however, might require more advanced methods.

Approaches similar to those given in this investigation should also be useful for related questions, for instance the determination of Jordan subalgebras in $\mathfrak{G}$.

## References

**Conway, J. H. [1971]:**
Three lectures on exceptional groups
In: Powell, M. B., Higman, G. (eds.): Finite Simple Groups
Academic Press, London, New York

**Conway, J. H. [1984]:**
A simple construction for the Fischer-Griess monster group
Invent. math. **79**, 513-540

**Conway, J. H., Curtis, R. T., Norton, S. P., Parker, R. A., Wilson, R. A. [1985]:**
ATLAS of Finite Groups
Clarendon Press, Oxford

**Griess, R. L. [1982]:**
The Friendly Giant
Invent. math. **69**, 1-102