On a commutative nonassociative algebra associated with a multiply transitive group

By Koichiro HARADA*)

To the memory of Prof. Takuro Shintani

1. Introduction.

This work was motivated by Griess' construction of the "Monster" simple group [1].

THEOREM A[1]. *Let A be a commutative (nonassociative) algebra over some field k satisfying the following conditions:*

(1) *A is a vector space over k with a system of basis $x_1, x_2, \cdots$, and x_n;*
(2) *$x_i^2=(n-1)x_i$ for $1\leqq i\leqq n$; and*
(3) *$x_i x_j=-x_i-x_j$ for $1\leqq i<j\leqq n$.*

Then if the characteristic of k is zero or greater than $n+1$, then the (k-linear) automorphism group of A is isomorphic to the symmetric group Σ_{n+1} of degree $n+1$.

An example of the algebra A in Theorem A is canonically obtained from a triply transitive permutation group G on a set $\Omega=\{x_0, x_1, x_2, \cdots, x_n\}$. Let $k[\Omega]$ be its permutation module over some field whose characteristic is zero or greater than $n+1$. Then $k[\Omega]\cong U\oplus M$ where U is the trivial $k[G]$-module and M is an irreducible $k[G]$-module. We identify M with $k[\Omega]/U$. More precisely, we put

$$M=\langle x_0, x_1, \cdots, x_n\rangle/\langle x_0+x_1+\cdots+x_n\rangle$$

where $\langle\cdots\rangle$ denotes the k-linear subspace generated by $\cdots$. Therefore if $\bar{x}$ denotes the image of $x\in k[\Omega]$ in $k[\Omega]/U$, then

$$M=\langle \bar{x}_1, \bar{x}_2, \cdots, \bar{x}_n\rangle \quad \text{and}$$

$$\bar{x}_0=-\bar{x}_1-\bar{x}_2-\cdots-\bar{x}_n\,.$$

Taking a suitable scalar multiple of x_i's, we shall show:

---

*) Research supported in part by NSF grant 784726.

1) Griess informed the author that he had obtained a similar result with an additional condition on A (existence of an associative form).

THEOREM B. *M possesses a G-invariant commutative (non-associative) algebra structure with the following properties*:

(1) $\bar{x}_i^2=(n-1)\bar{x}_i$ *for* $0\leqq i\leqq n$

(2) $\bar{x}_i\bar{x}_j=-\bar{x}_i-\bar{x}_j$ *for* $0\leqq i<j\leqq n$.

2. Proof of Theorem A.

We first define a new element:

DEFINITION. $x_0=-x_1-x_2-\cdots-x_n$.

LEMMA 1. *The following conditions hold*:

(1) $x_i^2=(n-1)x_i$ *for all* $0\leqq i\leqq n$; *and*

(2) $x_ix_j=-x_i-x_j$ *for all* $0\leqq i<j\leqq n$.

PROOF. It suffices to show $x_0^2=(n-1)x_0$ and $x_0x_i=-x_0-x_i$ for $i\neq 0$. We have

$$
\begin{aligned}
x_0^2&=(x_1+\cdots+x_n)^2\\
&=\sum_{i=1}^n x_i^2+2\sum_{1\leq i<j\leq n}x_ix_j\\
&=(n-1)\sum_{i=1}^n x_i-2(n-1)\sum_{i=1}^n x_i\\
&=-(n-1)\sum_{i=1}^n x_i\\
&=(n-1)x_0;\quad\text{and}\\
x_0x_i&=(-x_1-x_2-\cdots-x_n)x_i\\
&=\sum_{k=1}^n(x_k+x_i)-(x_i+x_i)-x_i^2\\
&=-x_0+nx_i-2x_i-(n-1)x_i\\
&=-x_0-x_i\,.
\end{aligned}
$$

This completes the proof.

LEMMA 2. *Let* $x=a_1x_1+a_2x_2+\cdots+a_nx_n$ *be an element of A with* $a_i\in k$, $1\leqq i\leqq n$. *If* $x^2=\lambda x$ *for some* $\lambda\in k$, *then all nonzero coefficients of x are equal. More precisely, if there are l nonzero* a_i*'s then one of the following possibilities hold*:

(1) $a_i=\dfrac{\lambda}{n+1-2l}$ *for all nonzero* a_i*'s*; *or*

(2) $n+1-2l=\lambda=0$ *in* k *with all nonzero* a_i*'s being equal but arbitrary.*

PROOF. We have

$$x^2=\sum_{i=1}^{n} a_i^2 x_i^2+2\sum_{1\leq i<j\leq n} a_i a_j x_i x_j$$

$$=\sum_{i=1}^{n} b_i x_i\,,$$

where

$$b_i=(n-1)a_i^2-2\sum_{\substack{k=1\\ k\neq i}}^{n} a_i a_k$$

$$=(n+1)a_i^2-2\sum_{k=1}^{n} a_i a_k\,, \qquad \text{for } 1\leqq i\leqq n\,.$$

If $x^2=\lambda x$, we have

$$\lambda a_i=(n+1)a_i^2-2a_i\sum_{k=1}^{n} a_k\,, \qquad \text{for } 1\leqq i\leqq n\,.$$

Suppose $a_i a_j\neq 0$. Then

$$\lambda=(n+1)a_i-2\sum_{k=1}^{n} a_k\,, \quad \text{and}$$

$$\lambda=(n+1)a_j-2\sum_{k=1}^{n} a_k\,.$$

Hence $(n+1)(a_i-a_j)=0$. Since $n+1\neq 0$ in k, we obtain $a_i=a_j$. If there are l nonzero a_i's, then

$$\lambda=(n+1)a_i-2la_i=(n+1-2l)a_i\,.$$

We obtain the latter part of our lemma immediately from this.

COROLLARY 3. *If* x *is a nonzero idempotent of* A, *then*

$$x=\frac{1}{n+1-2l}(x_{i_1}+\cdots+x_{i_l})$$

where $1\leqq i_1<i_2<i_3<\cdots<i_l\leqq n$ *for some* $1\leqq l\leqq n$.

PROOF. Put $\lambda=1$ in Lemma 2.

LEMMA 4. *Let* x, y *be a pair of nonzero elements of* A *satisfying*

$$\begin{cases} x^2=(n-1)x\,, \\ y^2=(n-1)y\,, \quad \textit{and} \\ xy=-x-y\,. \end{cases}$$

Then $\{x, y\} \subseteqq \{x_i ; 0 \leqq i \leqq n\}$.

PROOF. Put

$$x = \sum_{i=1}^{n} a_i x_i \quad \text{and}$$

$$y = \sum_{i=1}^{n} b_i x_i .$$

Then

$$xy = \sum_{i=1}^{n} c_i x_i$$

where

$$\begin{aligned} c_i &= (n-1)a_i b_i - \sum_{\substack{k=1 \\ k\neq i}}^{n} a_i b_k - \sum_{\substack{k=1 \\ k\neq i}}^{n} a_k b_i \\ &= (n+1)a_i b_i - a_i \sum_{k=1}^{n} b_k - b_i \sum_{k=1}^{n} a_k , \qquad \text{for } 1 \leqq i \leqq n . \end{aligned}$$

Since $xy = -x-y$, we have for $1 \leqq i \leqq n$

$$(*) \qquad (n+1)a_i b_i - a_i \sum_{k=1}^{n} b_k - b_i \sum_{k=1}^{n} a_k = -a_i - b_i .$$

By Lemma 2, we have

$$a_i = 0 \quad \text{or} \quad \frac{n-1}{n+1-2l} \qquad \text{for some } l \text{ and}$$

$$b_i = 0 \quad \text{or} \quad \frac{n-1}{n+1-2m} \qquad \text{for some } m .$$

Suppose that $a_i = 0$ if and only if $b_i = 0$. Then $x = y$ and so $xy + x + y = (n+1)x$. Hence $xy = -x-y$ is impossible to hold. Therefore, we may assume, interchanging x and y if necessary, that there exists an index i satisfying $a_i = 0$ but $b_i \neq 0$. By (*) we obtain $\sum a_k = 1$. Hence

$$\frac{n-1}{n+1-2l} l = 1 .$$

This implies $(n+1)(l-1) = 0$. Hence $l = 1$. Without loss of generality, we may assume that $x = x_1$. If $b_1 = 0$, then $m = 1$ by a similar argument as above and so our lemma holds. Therefore we may assume without loss of generality that

$$y = \frac{n-1}{n+1-2m}(x_1 + x_2 + \cdots + x_m) .$$

We compute

$$xy=\frac{n-1}{n+1-2m}(x_1^2+x_1x_2+\cdots+x_1x_m)$$
$$=\frac{n-1}{n+1-2m}\left[(n-m)x_1-\sum_{i=2}^{m}x_i\right].$$

Since $xy=-x-y$ by assumption, we obtain by comparing the coefficients for x_1

$$\frac{n-1}{n+1-2m}(n-m)=-1-\frac{n-1}{n+1-2m}.$$

This implies $(n+1)(n-m)=0$ and so $n=m$. Therefore

$$y=\frac{n-1}{n+1-2n}(x_1+\cdots+x_n)=x_0.$$

Thus the lemma holds in this case also.

The proof of Theorem A now follows immediately from the previous lemma and Lemma 1.

3. Commutative (nonassociative) algebras associated with triply transitive groups.

Let G be a triply transitive permutation group on a set $\Omega=\{x_0, x_1, \cdots, x_n\}$ of $n+1$ symbols with $n\geqq 2$. Let k be a field of characteristic 0 or greater than $n+1$. Then it is well known that the permutation module $k[\Omega]$ splits into the direct sum of the trivial module U and an irreducible module M of dimension n.

We note that G is isomorphic to a subgroup of $\sum_{n+1}$. Since the characteristic of k is zero or greater than $n+1$, the group algebra $k[G]$ is semi-simple. Moreover, every $k[G]$ module is obtained canonically from a $K[G]$-module by reduction for a suitable field K of characteristic zero.

LEMMA 5. *The symmetric product $S^2(M)$ possesses M as an irreducible constituent.*

PROOF. It suffices to show the lemma for the case in which the characteristic of k is zero. Let χ be the rational character of G afforded by M. We shall show

$$\sum_{\sigma\in G}(\chi(\sigma)^2+\chi(\sigma^2))\chi(\sigma)>0$$

which will yield our lemma since

$$\frac{1}{2}(\chi(\sigma)^2+\chi(\sigma^2))$$

is the character of $\sigma\in G$ afforded by $S^2(M)$. We have $\chi(\sigma)^3\geqq\chi(\sigma)$ for all $\sigma\neq 1$ and $\chi(1)^3>\chi(1)$ since $n>1$. Hence

$$\sum_{\sigma\in G}\chi(\sigma)^3>\sum_{\sigma\in G}\chi(\sigma)=0\,.$$

We have

$$\begin{aligned}\sum_{\sigma\in G}\chi(\sigma^2)\chi(\sigma)&=\sum_{\sigma\in G}(1+\chi(\sigma^2))(1+\chi(\sigma))-\Big(\sum_{\sigma\in G}1+\sum_{\sigma\in G}\chi(\sigma)+\sum_{\sigma\in G}\chi(\sigma^2)\Big)\\&\geqq\sum_{\sigma\in G}(1+\chi(\sigma))^2-|G|-|G|\\&=2|G|-|G|-|G|\\&=0\,.\end{aligned}$$

Hence the desired conclusion holds.

The previous result shows that M admits a commutative algebra structure. More precisely we do the following. Since $M\otimes M\cong S^2(M)\oplus A^2(M)$ and $S^2(M)\cong M\oplus M'$, we have a G-invariant mapping f from $M\otimes M$ to M. We define the product ab of $(a, b)\in M\times M$ by $ab=f(a\otimes b)$. Since f factors through $S^2(M)$, $ab=ba$ holds. Thus a commutative algebra structure is given to M.

Since $M\cong k[\Omega]/U$, we identify M with $k[\Omega]/U=k[\Omega]/\langle x_0+x_1+\cdots+x_n\rangle$. For $x\in k[\Omega]$, $\bar{x}$ denotes the image of x in M.

THEOREM B. *The algebra structure of M given above is uniquely determined. More precisely, if we choose a suitable (same) scalar multiple of $\bar{x}_i$, $0\leqq i\leqq n$, then the following relations hold:*

(1) $\bar{x}_i^2=(n-1)\bar{x}_i$ *for* $0\leqq i\leqq n$; *and*
(2) $\bar{x}_i\bar{x}_j=-\bar{x}_i-\bar{x}_j$ *for* $0\leqq i<j\leqq n$.

PROOF. Since $\bar{x}_1, \cdots$, and $\bar{x}_n$ are linearly independent, we write every element of M in terms of $\bar{x}_i$, $1\leqq i\leqq n$.

Let $\bar{x}_1\bar{x}_1=a_1\bar{x}_1+\cdots+a_n\bar{x}_n$. Since G is doubly transitive, there is an element σ in G with cyclic decomposition

$$\sigma=(1)(i0\cdots)\cdots.$$ [2]

So

$$\begin{aligned}\bar{x}_1\bar{x}_1&=a_1\bar{x}_1+\cdots+a_i\bar{x}_0+\cdots\\&=(a_1-a_i)\bar{x}_1+\cdots\,.\end{aligned}$$

Therefore $a_i=0$ for all $i\neq 1$. Hence

$$\bar{x}_i\bar{x}_i=a_1\bar{x}_i\qquad\text{for}\quad 0\leqq i\leqq n\,.$$

2) For simplicity, we write $(1)(i0\cdots)$ for $(x_1)(x_ix_0\cdots)$, etc.

Put $\bar{x}_1\bar{x}_2=b_1\bar{x}_1+\cdots+b_n\bar{x}_n$. Since G is triply transitive, there exists an element α in G with cyclic decomposition

$$(12)(i0\cdots)\cdots,$$

for every i with $3\leqq i\leqq n$. Hence we have

$$\begin{aligned}\bar{x}_1\bar{x}_2&=b_2\bar{x}_1+b_1\bar{x}_2+\cdots+b_i\bar{x}_0+\cdots\\&=(b_2-b_i)\bar{x}_1+(b_1-b_i)\bar{x}_2+\cdots.\end{aligned}$$

Therefore $b_1=b_2-b_i$ and $b_2=b_1-b_i$. Since the characteristic of k is not 2, we conclude $b_1=b_2$ and $b_i=0$ for $3\leqq i\leqq n$. Hence

$$\bar{x}_i\bar{x}_j=b_1(x_i+x_j)$$

for $0\leqq i<j\leqq n$.

We next obtain a relation between a_1 and b_1. Pick an element β of G with cyclic decomposition

$$(1)(20)\cdots.$$

Then from $\bar{x}_1\bar{x}_2=b_1(\bar{x}_1+\bar{x}_2)$, we have

$$\bar{x}_1\bar{x}_0=b_1(\bar{x}_1+\bar{x}_0).$$

Hence

$$\bar{x}_1(-\bar{x}_1-\bar{x}_2-\cdots-\bar{x}_n)=b_1(\bar{x}_1-\bar{x}_1-\bar{x}_2-\cdots-\bar{x}_n).$$

Comparing the coefficients for $\bar{x}_1$ of both sides, we obtain $-a_1-(n-1)b_1=0$. Hence

$$\begin{cases}\bar{x}_i\bar{x}_i=-(n-1)b_1\bar{x}_i & \text{for } 0\leqq i\leqq n,\\ \bar{x}_i\bar{x}_j=b_1(\bar{x}_i+\bar{x}_j) & \text{for } 0\leqq i<j\leqq n.\end{cases}$$

Taking $\bar{x}_i'=-(1/b)\bar{x}_i$ and calling it $\bar{x}_i$ again for simplicity, we obtain a set of normalized generators and the relations between them:

$$\begin{aligned}&\bar{x}_i\bar{x}_i=(n-1)\bar{x}_i && \text{for } 0\leqq i\leqq n,\\ &\bar{x}_i\bar{x}_j=-\bar{x}_i-\bar{x}_j && \text{for } 0\leqq i<j\leqq n.\end{aligned}$$

This completes the proof of Theorem B.

References

[1] Griess, R., A construction of F_1 as automorphisms of 196883 dimensional algebra. unpublished.

(Received March 30, 1981)

Hokkaido University
Sapporo, Japan
and
Ohio State University
Columbus, Ohio
U. S. A.