Hokkaido Mathematical Journal Vol. 16(1987), p. 177～190

Automorphism groups of certain non-associative non-commutative algebras

Masayuki WAJIMA

(Received April 2, 1986, Revised November 25, 1986)

1. Introduction.

In this paper, we investigate the automorphism group of a non-associative algebra V of the following type: the binary product is defined on its basis elements $x_1, \ldots, x_n$ satisfying

(i) $x_ix_i = c\ x_i\ (c \neq 0)$ for all i
(ii) $x_ix_j = -x_jx_i$ for $i \neq j$

and the product is extended linearly to general vectors. Let us call this an almost alternating algebra, a. a. algebra for brevity. For simplicity we assume that the characteristic of the base field of V is zero throughout. We call an a. a. algebra non-trivial if $x_ix_j \neq 0$ for some distinct indices i and j.

There have been several works on the non-associative algebras. Some showed that interesting finite groups appear as the automorphism groups of non-associative algebras. In this paper, we consider the following question: Can any finite group be an automorphism group of a certain non-associative algebra? (See Theorem 3.7 and Theorem 3.12 (D. Tambara).) We also wish to give many such examples.

In section 2, the basic properties of a. a. algebras are discussed. It is shown that the automorphism group of an a. a. algebra can be viewed as a subgroup of a symmetric group of certain degree. In section 3, we construct several examples of a. a. algebras and calculate their automorphism groups. These are associated to finite graphs (Theorem 3.1); sharply 2-transitive groups (Theorem 3.2); sharply 3-transitive groups (Theorem 3.3); orthogonal groups (Theorem 3.6); abstract groups (Theorem 3.7). This work is a part of the author's dissertation [3] under the direction of Prof. Harada at the Ohio State University.

2. Basic Properties.

In general, it is not easy to determine the group structure of Aut(V) for an algebra V. However, for any a. a. algebra V the automorphism group Aut(V) is of finite order. The following theorem is our starting point:

THEOREM 2.1. *Let V be an a. a. algebra with a basis $x_1, \dots, x_n$. The automorphism group* Aut(V) *is isomorphic to a subgroup of the symmetric group S_n of degree n.*

PROOF. Since $x_i x_j = -x_j x_i$ for $i \neq j$, a short computation shows that

$$(\sum r_i x_i)^2 = \sum c(r_i)^2 x_1.$$

For any element a in Aut(V), $(x_i)^a (x_i)^a = c(x_i)^a$. In particular, we have

$$(x_i)^a = \sum x_k$$

where k runs through A_i, a subset of the indices $\{1, \dots, n\}$.

We must show that each A_i consists of one index and all A_i's are distinct. It suffices to show that the intersection of A_i and A_j is empty whenever i is different from j. Suppose that the assertion is false. We have

$$(x_i)^a (x_j)^a = \sum c x_k + \sum x_s x_t + \sum x_s x_k + \sum x_k x_t$$

where k is in $A_i \cap A_j$, s is in $A_i \backslash A_j$ and t is in $A_j \backslash A_i$. By the assumption, the first summation is not zero. Unless $A_i \cap A_j$ is empty, we get

$$(x_i)^a (x_j)^a \neq -(x_j)^a (x_i)^a$$

a contradiction.

Let (G, X) be a permutation group. The next theorem shows that G admits at least one non-trivial a. a. algebra on the associated permutation module.

THEOREM 2.2. *Let G act on X, a finite set. Let V be the permutation module associated with the action of G on X. Let $e_1, \dots, e_n$ be the permutation basis of V. There exists a G-homomorhism f from $V \otimes V$ to V satisfying*

$$f(e_i \otimes e_i) = e_i$$
$$f(e_i \otimes e_j) = -f(e_j \otimes e_i) \text{ if } i \neq j,$$
$$f(e_i \otimes e_j) \neq 0 \text{ for some pair } i \neq j.$$

PROOF. Let $1 + \varphi$ be the character of the permutation module V associated to (G, X). The tensor product $V \otimes V$ decomposes into the symmetric part V_S and the alternating part V_A. As a constituent, V_S contains the diagonal subspace $\{v \otimes v \mid v \in V\}$ isomorphic to V. On the other hand, V_A contains a submodule W which affords the character φ. Let p be the composition of the projection maps one from $V \otimes V$ onto V_S and one from V_S onto V. Let q be the composition of the projection maps one from $V \otimes V$ onto V_A and one from V_A onto W. Note that $p(e_i \otimes e_i) = e_i$ and $q(e_i$

$\otimes e_j) = -q(e_j \otimes e_i)$. By a suitable identification, $f = p + q$ satisfies the assertion.

The mapping f in the previous theorem determines an a. a. algebra structure on a permutation module V; we simply extend f linearly to V and put

$$u\ v = f(u \otimes v)$$

for any elements u, v in V.

From now on, when we consider G acting on X, the action is supposed to be faithful. So by the theorems 2.1 and 2.2, if G acts on X and we construct a G-invariant a. a. algebra V, then G and $\mathrm{Aut}(V)$ are regarded as subgroups of S_n where n is the cardinality of X.

Next we describe the structure constants of a G-invariant a. a. algebra for a 2-transitive group. Let G act on X 2-transitively. Let V be the associated permutation module with a basis $x_1, \dots, x_n$. Let $P(i, j\,; t)$ and $P(i, j\,; t')$ be a paired orbital for distinct indices i and j. We also write

$$\bar{Y} = \sum_{k \in Y} x_k$$

for a subset Y of X.

PROPOSITION 2.3 *Let G and V be as above. Then an a. a. algebra structure defined on V is G-invariant if and only if*

$$x_i x_i = c\ x_i \textit{ for all } i \textit{ and}$$
$$x_i x_j = k(x_i - x_j) + \sum_{t=1}^{s} c_t(\overline{P(i, j\,; t)} - \overline{P(i, j\,; t')}) \textit{ for } i \neq j,$$

where $c \neq 0$, k, $c_1, \dots, c_s$ are constant numbers.

PROOF. We see that the multiplication stated is G-invariant. Conversely, suppose that an a. a. algebra on V is G-invariant. Let a point-wise stabilizer $G_{1,2}$ act on $x_1 x_2$. We see that the coefficients of any two base elements are same if they belong to the same $G_{1,2}$-orbit. Next, let a global stabilizer $G_{\{1,2\}}$ act on $x_1 x_2$. Since $x_i x_j = -x_j x_i$, it is easy to obtain the result.

We see that if G acts 3-transitively on X, then there is a unique G-invariant a. a. algebra structure on the associated permutation module. Let us complete the characterization of an a. a. algebra whose automorphism group is S_n. Note that this result is analogous to [2].

THEOREM 2.4. *Let V be an a. a. algebra with a basis $x_1, \dots, x_n$. Then* $\mathrm{Aut}(V)$ *is isomorphic to S_n if and only if there exist constant numbers*

$c(\neq 0)$ and k such that

$$x_ix_i=cx_i \textit{ for all } i,$$
$$x_ix_j=k(x_i-x_j) \textit{ for any indices } i\neq j.$$

Proof. Suppose that an a. a. algebra V satisfies the conditions on binary product. By theorem 2. 1, we only need to check that any permutation on $x_1, \dots, x_n$ preserves the given binary product. For instance, a permutation p sends x_i to x_s and x_j to x_t. Then we have

$$(x_i)^p(x_j)^p=x_sx_t=k(x_s-x_t) \text{ and}$$
$$(x_ix_j)^p=k(x_i-x_j)^p=k(x_s-x_t),$$

which give $(x_ix_j)^p=(x_i)^p(x_j)^p$.

Suppose that Aut(V) is isomorphic to S_n. By theorem 2. 1, Aut(V) permutes $x_1, \dots, x_n$. When $n=1$ or 2, there is nothing to prove. When n is greater than 2, Aut(V) acts 3-transitively on $x_1, \dots, x_n$. By Proposition 2. 3, the binary product satisfies the conclusion.

3. Examples.

In this section, several examples of a. a. algebras and their automorphism groups are discussed. First we consider a. a. algebras induced from finite graphs. Let Y be a graph with a finite set of vertices $\{1, \dots, n\}$. Let E be the set of the edges of Y. The automorphism group Aut(Y) of Y is defined as:

$$\mathrm{Aut}(Y)=\{p\in S_Y \mid (i^p, j^p)\in E \text{ whenever } (i, j)\in E.\}$$

The corresponding a. a. algebra is defined as follows: Let $1, \dots, n$ be the vertices of Y. Let V be the permutation module of Aut(Y) with a basis $x_1, \dots, x_n$. We define a binary product on V by

$$x_ix_i=x_i \text{ for all } i,$$

$$x_ix_j=\sum_{(i,k)\in E} x_k-\sum_{(j,m)\in E} x_m \text{ for } i\neq j.$$

We obtain the following:

Theorem 3. 1. *Let Y be a finite graph. Then* Aut(Y) *is isomorphic to* Aut(V) *for the corresponding a. a. algebra V defined above.*

Proof. First, we show that Aut(Y) is contained in Aut(V). If an element p in Aut(Y) acts on Y as $i^p=j$, then the action of p on V is defined by $(x_i)^p=x_j$.

For any element p in Aut(Y), we have

$$
\begin{aligned}
(x_i x_j)^p &= \sum_{(i,\, k)\in E} (x_k)^p - \sum_{(j,\, m)\in E} (x_m)^p \\
&= \sum_{(i^p,\, k^p)\in E} (x_k)^p - \sum_{(j^p,\, m^p)\in E} (x_m)^p
\end{aligned}
$$

for $i\neq j$. On the other hand, we have

$$(x_i)^p(x_j)^p = \sum_{(i^p,\, s)\in E} x_s - \sum_{(j^p,\, t)\in E} x_t .$$

Since p permutes the vertices of Y, we see that the first claim holds.

Next we check that $\mathrm{Aut}(V)$ is contained in $\mathrm{Aut}(Y)$. For any element a in $\mathrm{Aut}(V)$, we have

$$(x_i x_j)^a = \sum_{(i,\, k)\in E} (x_k)^a - \sum_{(j,\, m)\in E} (x_m)^a$$

which is equal to

$$(x_i)^a(x_j)^a = \sum_{(i^a,\, s)\in E} x_s - \sum_{(j^a,\, t)\in E} x_t$$

for $i\neq j$. Suppose that (i, j) is an edge. Then in the expression of $(x_i x_j)^a$, the term $(x_j)^a$ appears only in the first summation once. This implies that in the expression of $(x_i)^a(x_j)^a$, the same term $(x_j)^a$ must appear in the first summation. Thus, we see that if (i, j) is an edge then (i^a, j^a) is also an edge. This completes the proof of the theorem.

In section 2, we have characterized the a. a. algebras associated to 3-transitive groups. The next example handles sharply 2-transitive groups.

THEOREM 3. 2. *Suppose that G acts sharply 2-transitively on X, a set of cardinality n. Let V be the associated permutation module with a basis $\{x_1, \dots, x_n\}$. Let t be the unique element in G such that $(x_1)^t = x_2$ and $(x_2)^t = x_1$. Let m be the greatest integer not exceeding $n/2$.*

Rearrange the numbering if necessary, we define an a. a. algebra on V as follows:

$$
\begin{aligned}
&x_i x_i = x_i \text{ for all } i,\\
&x_1 x_2 = \sum r(1,2\,;k)(x_k - (x_k)^t),
\end{aligned}
$$

where k runs from 1 through m,

$$x_i x_j = (x_1 x_2)^p \text{ for } i\neq j$$

where p is a unique element in G such that $(x_1)^p = x_i$ and $(x_2)^p = x_j$.

If all the coefficients $r(1, 2\,; k)$'s are non-zero and have different absolute values, then $\mathrm{Aut}(V)$ *is isomorphic to G.*

PROOF. We first determine the possible G-invariant a. a. algebra structures on V. We need to consider only x_ix_j for $i\neq j$. Put

$$x_ix_j=\sum r(i,j;k)x_k.$$

By comparing the coefficients of $(x_ix_j)^g$ and $(x_i)^g(x_j)^g$ for an element g in G, we get

$$r(i^g,j^g;k^g)=r(i,j;k).$$

Since G acts sharply 2-transitively on X, it suffices to consider $r(1,2;k)$ for $k=1,\dots,n$. Namely, if a pair of indices i, j with $i\neq j$ is given, then there is a unique element g in G such that $1^g=i$ and $2^g=j$. Therefore, the coefficients satisfy

$$r(i,j;k)=r(1,2;k^h)$$

for $k=1,\dots,n$, where $h=g^{-1}$.

Next we investigate the interrelation of the $r(1,2;k)$'s. Consider $H=G_{\{1,2\}}$, the global stabilizer of $\{1,2\}$ in G. The subgroup H is of order two; let t be the generator. Comparing the coefficients of x_1x_2 and x_2x_1, we get

$$r(1,2;k)=-r(2,1;k^t).$$

Rearrange the numbering if necessary, we get

$$x_1x_2=\sum r(1,2;k)(x_k-(x_k)^t),$$

where k runs through a complete set of representatives of H-orbits of length two.

Suppose that all $r(1,2;k)$'s are none-zero and have different absolute values. We show that $\mathrm{Aut}(V)$ is isomorphic to G itself.

For any element a in $\mathrm{Aut}(V)$, which induces a permutation on the basis elements of V, we have $(x_1x_2)^a=x_sx_u$ where $s=1^a$ and $u=2^a$. On the other hand, there exists a unique element g in G such that $1^g=s$ and $2^g=u$. We want to show that $i^g=i^a$ for all i. Compare the coefficients of

$$(x_1x_2)^a=\sum r(1,2;k)((x_k)^a-(x_k^t)^a) \text{ and}$$
$$(x_1x_2)^g=\sum r(1,2;k)((x_k)^g-(x_k^t)^g).$$

By the assumption on the $r(1,2;k)$'s we get

$$(x_i)^a=(x_i)^g \text{ for all } i.$$

This implies the result.

Next, suppose that G acts on X sharply 3-transitively. As we considered them in lemma 2.3, an a.a. algebra V can not be defined on the associated permutation module in order that Aut(V) is relatively small. So we take a non-standard permutation module of G. The group G acts on the ordered pairs of X naturally: for any element g in G and (i, j) in $X \times X$, define

$$(i, j)^g = (i^g, j^g).$$

There are two G-orbits in $X \times X$: the diagonal set $\{(i, i) \mid i \in X\}$ and the off-diagonal set $Y = \{(i, j) \mid i \neq j\}$.

We define a permutation module V associated with the action of G on the off-diagonal set Y. Let $\{e(i, j) \mid (i, j) \in Y\}$ be a permutation basis of V. Notice that

$$\dim(V) = |Y| = |X|(|X|-1).$$

Define a binary product on V as follows:

(1) $e(i, j)e(i, j) = e(i, j)$ for all (i, j) in Y,

(2) $e(1, 2)e(1, 3) = \sum r(1, 2, 1, 3; s, t)(e(s, t) - e(s^g, t^g))$

where g is the unique element in G such that $1^g = 1$, $2^g = 3$, $3^g = 2$ and (s, t) runs through a complete set of representatives of $<g>$-orbits on Y. Since $g^2 = 1$, each $<g>$-orbit consists of at most two elements. We see that (2) is well-defined. Note that if $(s, t) = (s^g, t^g)$ then $r(1, 2, 1, 3; s, t) = 0$. And if this happens, $1 \in \{s, t\}$.

(3) $e(i, j)e(i, k) = (e(1, 2)e(1, 3))^h$ for $j \neq k$, where h is the unique element in G such that $1^h = i$, $2^h = j$ and $3^h = k$.

(4) $e(i, j)e(p, q) = 0$ if $i \neq p$.

Since we have defined the binary product on every G-orbit on $Y \times Y$, it is easy to see that V has a G-invariant algebra structure. We now state the theorem:

THEOREM 3.3. *On the algebra V defined above, if*

(5) $|r(1, 2, 1, 3; s, t)| \neq |r(1, 2, 1, 3; p, q)|$ *whenever* $(s, t) \neq (s^g, t^g)$, $(p, q) \neq (p^g, q^g)$ *and* $(s, t) \neq (p, q)$ *then* Aut(V) *is isomorphic to* G.

PROOF. By theorem 2.1, it suffices to show that G contains Aut(V). Let a be any element in Aut(V), and suppose that $j \neq k$. We have

$$(e(i, j)e(i, k))^a = e(i, j)^a e(i, k)^a \neq 0.$$

By (4) if $(i, j)^a = (u, v)$ and $(i, k)^a = (p, w)$, then we must have $u = p$.

Thus, $(i, j)^a=(u, v)$ and $(i, k)^a=(u, w)$. Since G is sharply 3-transitive on X, there exists a unique element h in G such that $i^h=u$, $j^h=v$ and $k^h=w$. To get the conclusion, we must show

$$(s, t)^a=(s^h, t^h) \text{ for all } (s, t) \text{ in } Y.$$

Compare the coefficients in $(e(1,2)e(1,3))^a$ and $(e(1,2)e(1,3))^h$:

$$(e(1,2)e(1,3))^a=\sum r(1,2,1,3\,;s,t)(e(s,t)^a-e(s^g,t^g)^a)$$

and

$$(e(1,2)e(1,3))^h=\sum r(1,2,1,3\,;s,t)(e(s,t)^h-e(s^g,t^g)^h).$$

We have $(s, t)^a=(s, t)^h=(s^h, t^h)$ if $(s, t)\neq(s^g, t^g)$. As we mentioned, unless $1\in\{s, t\}$, we get $(s, t)\neq(s^g, t^g)$. Thus, we have to show

$$(s, t)^a=(s^h, t^h) \text{ for } s=1 \text{ or } t=1.$$

Let us consider the coefficients in $e(i, 1)e(i, 2)$ for $1\neq i\neq 2$. According to (3), there exists a unique element x in G such that $1^x=i$, $2^x=1$ and $3^x=2$. We have

$$e(i,1)e(i,2)=\sum r(1,2,1,3\,;s,t)(e(s,t)^x-e(s^g,t^g)^x).$$

Now compare the coefficients in $A=(e(i,1)e(i,2))^a$ and $B=(e(i,1)e(i,2))^h$:

$$A=\sum r(1,2,1,3\,;s,t)(e(s^x,t^x)^a-e(s^{gx},t^{gx})^a) \text{ and}$$
$$B=\sum r(1,2,1,3\,;s,t)(e(s^x,t^x)^h-e(s^{gx},t^{gx})^h).$$

We see that $(s^x, t^x)^a=(s^x, t^x)^h$ if the coefficient $r(1,2,1,3\,;s,t)\neq 0$, that is, if $(s, t)\neq(s^g, t^g)$. Since $(2, k)\neq(2^g, k^g)$ for any $k\neq 2$, we have

$$(2^x, t^x)^a=(2^x, t^x)^h$$

for any $t\neq 2$. Therefore, we have $(1, t^x)^a=(1, t^x)^h$. This completes the proof.

Next we consider the orthogonal groups of vector spaces over the finite fields. We construct an a. a. algebra whose automorphism group is isomorphic to a given orthogonal group. Let W be a vector space of finite dimension over a finite field K. We need a pair of lemmas.

LEMMA 3.4. *The set* $A(n)=\{1, 2, 4, \dots, 2^{n-1}\}$ *has the following property* : *if*

$$a-b=c-d\neq 0$$

for any elements a, b, c, d *in* $A(n)$, *then*

$a=c$ *and* $b=d$.

PROOF. Trivial.

LEMMA 3.5. *Let* W *be an* n*-dimensional vector space over a finite field* K. *Let* W *have a non-degenerate inner product. Suppose that* s *is a permutation on the vectors of* W *such that*

$$(a^s, d^s)=(a, d)$$

for any vectors a *and* d *in* W. *Then* s *is a* K*-linear mapping.*

PROOF. First we show that s is an additive mapping. By the assumption, for any vector d in W, a short computation shows that

$$((a+b)^s,\ d^s)=(a^s+b^s,\ d^s).$$

Since the inner product is non-degenerate, we have

$$(a+b)^s=a^s+b^s.$$

Next we show that s is a K-mapping. For any element k in K and any vectors a and d in W, a short computation shows that

$$((ka)^s,\ d^s)=(k\ a^s,\ d^s).$$

We obtain $(ka)^s=ka^s$.

This completes the proof.

In the previous lemma, the mapping s is a permutation (one-to-one and onto) on W. So s belongs to $\mathrm{GL}(W)$. Since it preserves the inner product, we see that s is in the orthogonal group of W with respect to the inner product.

THEOREM 3.6. *Let* W *be an* n*-dimensional vector space over a finite field* K. *Let* W *possess a non-degenerate inner product. We define an a. a. algebra* V *over the complex number field as follows*: V *has a basis* $\{v_a \mid a\in W\}$ *such that*

$$(v_a)(v_a)=v_a \text{ for all } a \text{ in } W,$$

$$(v_a)(v_b)=\sum r_k(\sum_{(a,\,c)=k} v_c-\sum_{(b,\,d)=k} v_d)$$

for $a\neq b$, *where* k *runs through* K *and the* r_k*'s are complex numbers. Then* $\mathrm{Aut}(V)$ *is isomorphic to the orthogonal group of* W *with respect to the inner product.*

PROOF. Note that $(v_b)(v_a)=-(v_a)(v_b)$, so the binary product induces an a. a. algebra structure on V. We also note the following:

$$(v_a)(v_b)=\sum_{k\in K}\sum_{(a,c)=k} r_k v_c-\sum_{k\in K}\sum_{(b,d)=k} r_k v_d$$
$$=\sum_{c\in W}(r_{(a,c)}-r_{(b,c)})v_c.$$

After defining an order on K, choose the coefficients $\{r_k\}$ to be

$$A(|K|)=\{1,2,4,\ldots,2^{|K|-1}\}$$

as in lemma 3.4. By Theorem 2.1, Aut(V) is isomorphic to a subgroup of $S_{|W|}$. For s in Aut(V) and v_a in V, define a^s in W by

$$v_{(a^s)}=(v_a)^s.$$

Similarly, if p is a permutation on the vectors of W, identify p as an element in GL(V) by

$$(v_a)^p=v_{(a^p)}.$$

Let p be an element of the orthogonal group of W ; that is, $(a^p, b^p)=(a, b)$ for any vectors a and b in W. It is easy to see that p preserves the a. a. algebra structure of V.

Let s be an element of Aut(V). For two distinct elements a and b in W, we have

$$(v_a v_b)^s=\sum_{c\in W}(r_{(a,c)}-r_{(b,c)})V_{(c^s)},$$

$$v_{(a^s)}v_{(b^s)}=\sum_{d\in W}(r_{(a^s,d)}-r_{(b^s,d)})v_d.$$

Comparing the coefficients, we have

$$r_{(a,c)}-r_{(b,c)}=r_{(a^s,c^s)}-r_{(b^s,c^s)}$$

for any vector c in W. By lemma 3.5, we get

$$r_{(a,c)}=r_{(a^s,c^s)} \text{ if } r_{(a,c)}\neq r_{(b,c)}.$$

This implies that if a vector b exists in W such that

$$(a, c)\neq(b, c) \text{ then } (a, c)=(a^s, c^s).$$

Since the inner product is non-degenerate, such a vector b always exists in W provided $c\neq 0$. On the other hand, it is easy to see that $0^s=0$. So we conclude that

$$(a, c)=(a^s, c^s)$$

for any vectors a and c in W. By lemma 3.5, we complete the proof.

Next, we construct an a. a. algebra V associated to a given abstract group G. We assume $G \neq 1$ for the rest of this section.

For a given finite group G, let V be a vector space over the complex number field with a basis $\{v_g | g \in G\}$. Define an a. a. algebra structure on V as follows:

$$(v_g)(v_g) = v_g,$$
$$(v_g)(v_h) = v_{gh} - v_{hg} \text{ if } g \neq h.$$

Let G act on V by conjugation;

$$(v_g)^x = v_{(x^{-1}gx)},$$

the algebra structure on V is G-invariant.

We see that $\mathrm{Aut}(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(V)$. Conversely, any element a in $\mathrm{Aut}(V)$ induces a permutation on the basis elements: for any element g in G, we define g^a by

$$v_{(g^a)} = (v_g)^a.$$

We consider that when $\mathrm{Aut}(V)$ induces automorphisms on G. Namely our goal is to prove the following:

THEOREM 3.7 *If $Z(G)$ is trivial, then* $\mathrm{Aut}(V)$ *of the a. a. algebra V defined above is isomorphic to $Aut(G)$.*

We start with a few basic properties of this algebra.

LEMMA 3.8. *Let a be an element in* $\mathrm{Aut}(V)$. *For any elements x and y in G, x and y commute if and only if x^a and y^a commute. Moreover, if x and y do not commute, then*

$$(xy)^a = x^a y^a.$$

PROOF. Notice that x and y do not commute if and only if $(v_x)(v_y) = v_{xy} - v_{yx} \neq 0$. Apply a to the both sides and compare, we get the conclusions.

LEMMA 3.9. *Suppose that for an element z in G there exists an element w which does not commute with z. Then for any element a in* $\mathrm{Aut}(V)$ *the following holds:*

$$(z^{-1})^a = (z^a)^{-1}.$$

PROOF. The hypothesis implies that z^{-1} does not commute with zw. By the previous lemma,

$$w^a = (z^{-1}zw)^a = (z^{-1})^a (zw)^a = (z^{-1})^a z^a w^a.$$

Thus, we get the result.

LEMMA 3.10 *Let x and y be commutative elements of G. Suppose that there exists z in G such that z does not commute with x, y and xy. Then for any element a in* Aut(V),

$$(xy)^{a}=x^{a}y^{a}.$$

PROOF. The hypothesis implies that y does not commute with z^{-1}. It also implies that xz and $z^{-1}y$ do not commute. By the previous lemmas, we have

$$(xy)^{a}=(xz)^{a}(z^{-1}y)^{a}=x^{a}z^{a}(z^{a})^{-1}y^{a}=x^{a}y^{a}.$$

The next proposition is key to our theorem:

PROPOSITION 3.11. *Suppose that $Z(G)=1$. If x and y in G commute, then there exists z in G such that z does not commute with x, y and xy.*

PROOF. Suppose that the assertion is false. Then G is the union of $C_G(x)$, $C_G(y)$ and $C_G(xy)$. Note that these three subgroups are all distinct and proper subgroups of G. Put $K=C_G(x)\cap C_G(y)$. By counting elements, we have

$$(1)\quad |G|=|C_G(x)|+|C_G(y)|+|C_G(xy)|-2|K|.$$

Divide both sides of (1) by $|K|$, we get

$$(2)\quad |G|/|K|=|C_G(x)|/|K|+|C_G(y)|/|K|+|C_G(xy)|/|K|-2.$$

Suppose that all the indices of $C_G(x)$, $C_G(y)$ and $C_G(xy)$ in G are greater than 2, it contradicts to (1). So we may assume $|G|/|C_G(x)|=2$.

Comparing the size of the conjugacy classes of x in G, in $C_G(y)$ and in $C_G(xy)$, we get

$$(3)\quad |G|/|C_G(x)|\geq|C_G(xy)|/|K| \text{ and}$$
$$(4)\quad |G|/|C_G(x)|\geq|C_G(y)|/|K|.$$

By the assumption, we have

$$2=|C_G(xy)|/|K|=|C_G(y)|/|K|.$$

By (2), we have

$$|G|/|K|=|C_G(x)|/|K|+2.$$

By (3), we have

$$|G|/|K|\geq(|C_G(xy)|/|K|)\cdot(|C_G(x)|/|K|)=2|C_G(x)|/|K|.$$

So we get

$$2|C_G(x)|/|K|\leq|C_G(x)|/|K|+2.$$

Thus, we obtain $|C_G(x)|/|K|=2$. Therefore, the index of K in G is 4, and the index of K in each of the three subgroups is 2. So K is a normal subgroup of G. Then $A=G/K$ is a four-group. By conjugation, A acts on $Z(K)$, the center of K, which contains x, y and xy. If an element g in $Z(K)$ is fixed by A, then g must belong to $Z(G)$, which is a trivial group. So A acts on $Z(K)$ fixed-point-freely. A four-group can not act on a group of even order fixed-point-freely (theorem 6.2.3 [1]), therefore $Z(K)$ is of odd order.

For any element h in $C_G(xy)\backslash K$, we have that h acts on the normal subgroups $Z(C_G(x))$ and $Z(C_G(y))$. The quotient group $G/C_G(x)$ is of order 2. The action of h on $Z(C_G(x))$ is fixed-point-free, as any fixed point of $Z(C_G(x))$ is contained in $Z(G)$. Then by theorems 6.2.3 and 10.1.4 [1], $Z(C_G(x))$ is abelian of odd order and h inverts every element of $Z(C_G(x))$. Namely, h inverts x and y. Since x and y commute, h inverts xy.

On the other hand, h belongs to $C_G(xy)$. This implies that xy is an element of order 2. This contradicts to the fact that $Z(K)$ is of odd order. This completes the proof of the theorem.

The author thanks to Prof. D. Tambara who shows the following theorem:

THEOREM 3.12 (D. TAMBARA) *Let G be any finite group. Define an a. a. algebra V on G as follows:*

$$v_g v_g = v_g$$

$$v_g v_h = \sum_{a\in G}(r(ga^{-1})-r(ha^{-1}))v_a \text{ for } g\neq h,$$

where $\{r(g)\}$ *is a set as in lemma* 3.4, *namely* $A(|G|)$. *Then* Aut(V) *is isomorphic to* G.

PROOF. First we show that Aut(V) contains G. Let x be any element of G. The action on the basis element is as follows:

$$(v_g)^x = v_{gx}.$$

It is easily verified that this action preserves the algebra operation.

Next we show that G contains Aut(V). Let s be any element of

Aut(V), that is,

$$(v_g v_h)^s = (v_g)^s (v_h)^s.$$

Comparing the coefficients of v_x for x in G, we obtain

$$gx^{-1} = g^s (x^s)^{-1}.$$

In particular, putting $g=1$, we have

$$x^s = x1^s \text{ for all } x.$$

Thus we can identify the action of s on G by the right multiplication of 1^s. This correspondence gives an isomorphism from Aut(V) to G.

References

[1] D. GORENSTEIN ; Finite Groups, second edition, Chelsea, 1980.

[2] K. HARADA ; On a commutative nonassociative algebra associated with a multiply transitive group, J. Fac. Sci., Univ. of Tokyo, 28 (1982) 843-949.

[3] M. WAJIMA ; Non-associative algebras and their automorphism groups, Ph. D. Dissertation, The Ohio State University, June, 1985.

Hokkaido Institute of Technology
Sapporo, Hokkaido