A theorem on doubly transitive permutation groups with application to universal algebras

by

G. Grätzer (Budapest)

There is a certain class of groups, namely the class of doubly transitive minimal permutation groups (1), which are related to certain projective plains as well as to certain universal algebras. Under an additional hypothesis a complete description of this class of groups was given in the excellent book [2] of M. Hall, Jr. This theorem introduces two operations, $+$ and $\cdot$, in the set K, on which $\mathfrak{G}$ acts as a doubly transitive minimal group in such a way that $\mathfrak{G}$ is isomorphic with the linear group over K, i. e. with the group of linear substitutions $x \to xm+b$ $(m \neq 0)$, and it is proved that $(K; +, \cdot)$ is a near-field (1) in which $x = xm+b$ $(m \neq 0, 1)$ always has a solution. The additional hypothesis is that given $a, b \in K$, $a \neq b$ there is at most one element α of $\mathfrak{G}$ which takes a into b and which displaces every element of K. Whether or not this condition is necessary for the validity of the theorem is not settled there and it is not my aim to solve this problem here.

In this note I would like to give a „coordinatization theorem" for an arbitrary doubly transitive and minimal group $\mathfrak{G}$. This theorem is (at least, apparently) more general than that of M. Hall. However, the impetus for proving this result was given not by M. Hall's theorem but by the work [6] of S. Świerczkowski on algebras independently generated by every n distinct elements. He gave a complete description of this class of universal algebras for $n \neq 2$. Namely, he proved that an algebra independently generated by every n distinct elements is the trivial algebra with n elements if $n > 3$. For $n = 3$ there exists a unique non-trivial algebra independently generated by every three distinct elements. For $n = 2$ the problem remained open, but he proved that if the algebra $\mathfrak{A}$ is independently generated by every two distinct elements then the group $\mathfrak{G}$ of all automorphisms of $\mathfrak{A}$ is doubly transitive and minimal. Since a partial converse of this statement can be proved, we can apply

(1) For the notions, see § 1.

the "coordinatization theorem" to give a description of this class of universal algebras.

I have tried to make this paper self-complete; therefore every notion and notation used is collected in § 1. In § 2 the coordinatization theorem is proved (Theorems 1 and 2) and then the algebraic equivalent of M. Hall's problem is discussed in detail (Theorems 3 and 4). An almost trivial result (Theorem 7) establishes a one-to-one correspondence between doubly transitive minimal groups and a certain class of algebras independently generated by every two elements, which we call reduced 2-algebras. The main theorem of this paper is the representation theorem for reduced 2-algebras (Theorems 6 and 8). Theorems 9-11 lead to the determination of the cardinality of the set of non-isomorphic algebras independently generated by every two elements and with a given automorphism group. It turns out that even in the simplest case where the automorphism group is the symmetric group on two letters there are $2^{\aleph_0}$ such algebras.

§ 1. Preliminaries. Groups. Let A be a set and G the collection of certain one-to-one mappings of A onto A, i.e. let the elements of G be permutations of A. Small Greek letters will denote the elements of G, while small Roman letters the elements of A. If $\alpha \in G$, $a \in A$, $a\alpha$ denotes the „image" of a under α; sometimes we write $\alpha\colon a \to b$ to denote $b = a\alpha$. The product $\alpha\beta$ of two elements α, β of G is defined by $\alpha\beta\colon a \to (a\alpha)\beta$; obviously, $\alpha\beta$ is also a permutation of A. The identical permutation is denoted by ε, i.e. $a\varepsilon = a$ $(a \in A)$. The inverse α^{-1} of α is $\alpha^{-1}\colon a\alpha \to a$. A *permutation* group $\mathfrak{G}$ (or simply, a *group*) is a collection G of permutations, G is not void and $\alpha, \beta \in G$ implies $\alpha\beta^{-1} \in G$; thus always $\varepsilon \in G$.

$\mathfrak{G}$ is called *n-ply transitive* if, given $a_1, b_1, a_2, b_2, \ldots, a_n, b_n \in A$, $a_i \neq a_j$, $b_i \neq b_j$ if $i \neq j$, there is an $\alpha \in G$ with

$$a_i\alpha = b_i\,, \qquad i = 1, 2, \ldots, n\,. \tag{1}$$

We will mostly be interested in *doubly transitive groups* ($n = 2$). If $n = 1$ then $\mathfrak{G}$ is called *transitive*.

An n-ply transitive group is called *minimal* if (1) is satisfied by a unique $\alpha \in G$.

Let $\mathfrak{G}$ be a group of permutations of A. We define an equivalence relation on A, $a \sim b$ $(a, b \in A)$ if an $\alpha \in G$ exists with $a\alpha = b$. The equivalence classes $\{C_\lambda;\ \lambda \in \Lambda\}$ will be called the *transitive constituents of* A. Thus, if $a \in C_\lambda$, $b \in C_\mu$, $\lambda \neq \mu$ $(\lambda, \mu \in \Lambda)$ then $a\alpha = b$ holds for no $\alpha \in G$. The group $\mathfrak{G}$ is *transitive* if there is only one class $C_1 = A$.

If A, B are sets, $A \cup B$, $A \cap B$, $A \setminus B$ denote the set-theoretical union, intersection and difference, respectively; $\{a_1, a_2, \ldots\}$ denotes the set whose elements are $a_1, a_2, \ldots$; hence if $x \in A$ then $A \setminus \{x\}$ denotes the set consisting of all elements of A distinct from x. The cardinality of the set A is denoted by $|A|$.

Universal algebras.

A *universal algebra* [2] (briefly: *algebra*) is a couple $(A; \boldsymbol{F})$ where A is a set and $\boldsymbol{F}$ is a collection of *finitary operations* [3] on A; a finitary operation $f = f(x_1, \ldots, x_n)$ assigns to every n-tuple $(a_1, \ldots, a_n)$ of elements of A a unique element of A denoted by $f(a_1, \ldots, a_n)$.

If we do not require that $f(a_1, \ldots, a_n)$ be defined for *every* n-tuple, then f is a *partial-operation* and $(A; \boldsymbol{F})$ is called a *quasi algebra* [4]. Sometimes, we write $(A; f_1, f_2, \ldots; a_1, a_2, \ldots)$ to denote an algebra, where $f_1, f_2, \ldots$ are operations (partial operations), and $a_1, a_2, \ldots$ are elements of A which occur in the definition of $f_1, f_2, \ldots$ [5]. Let $(A; \boldsymbol{F})$, $(B; \boldsymbol{F})$ be algebras with the same set of operations and h a many-one mapping $x \to xh$ of A into B; h is a *homomorphism* if $f(a_1, \ldots, a_n)\, h = f(a_1 h, \ldots, a_n h)$ for every $f \in \boldsymbol{F}$, $a_1, \ldots, a_n \in A$. If h is one-to-one and $Ah = B$, then it is an *isomorphism*. An *automorphism* is an isomorphism of $(A; \boldsymbol{F})$ with itself; the set of all automorphisms is denoted by $\mathfrak{G}\big((A, \boldsymbol{F})\big)$ (briefly: $\mathfrak{G}(A, \boldsymbol{F})$, or $\mathfrak{G}$), which is a permutation group on A.

Let $(A; \boldsymbol{F})$ be an algebra and B a subset of A such that $f \in \boldsymbol{F}$, $b_1, \ldots, b_n \in B$ implies $f(b_1, \ldots, b_n) \in B$. Then $(B; \boldsymbol{F})$ is again an algebra; it is called a *subalgebra* of $(A; \boldsymbol{F})$. Given $H \subseteq A$ there is a smallest subalgebra $(B; \boldsymbol{F})$ with B containing H. If $A = B$, H is a *generating system* of $(A; \boldsymbol{F})$.

$\boldsymbol{A}^{(n)}\big((A; \boldsymbol{F})\big)$ (or, briefly, $\boldsymbol{A}^{(n)}$) will denote the class of all *algebraic n-ary operations* [6] in $(A; \boldsymbol{F})$, i.e. the smallest class of n-ary operations satisfying the conditions:

O1. *The n-ary operation* [7] e_i^n *defined by* $e_i^n(x_1, \ldots, x_n) = x_i$ *is in* $\boldsymbol{A}^{(n)}$ *for* $i = 1, 2, \ldots, n$.

O2. *If* $g_1, \ldots, g_m \in \boldsymbol{A}^{(n)}$ *and* $f = f(x_1, \ldots, x_m) \in \boldsymbol{F}$ *then*

$$f(g_1, \ldots, g_m) = f\big(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)\big) \in \boldsymbol{A}^{(n)}\,.$$

We put $\boldsymbol{A} = \boldsymbol{A}^{(1)} \cup \boldsymbol{A}^{(2)} \cup \ldots$ and $\boldsymbol{F}^{(n)} = \boldsymbol{F} \cap \boldsymbol{A}^{(n)}$, thus $\boldsymbol{F} = \boldsymbol{F}^{(1)} \cup \boldsymbol{F}^{(2)} \cup \ldots$ $\boldsymbol{A}^{(0)}$ is the class of 0-ary operations; their values are called *algebraic constants*.

The algebra $(A; \boldsymbol{F})$ is *trivial* if $\boldsymbol{A}^{(n)}$ contains only *trivial operations*, i.e. those listed in O1.

[2] It is also called *abstract algebra* and universal algebraic system by many authors.

[3] Also called *functions*.

[4] Partial abstract algebra and partial algebra are also adopted terminologies.

[5] E.g. a ring is $(R; +, \cdot; 0)$. It is sometimes useful to indicate which element is the zero.

[6] Also called *derived* operations.

[7] These are the *trivial* operations.

The function $f(g_1, \ldots, g_m)$ defined in O2 shows that $\mathfrak{A}^{(n)} = (A^{(n)}; F)$ is an algebra. One can easily prove that $\mathfrak{A}^{(n)}$ is a *free algebra* with n generators, $e_1^n, \ldots, e_n^n$. This means that if p is an arbitrary mapping of $e_1^n, \ldots, e_n^n$ into A then there exists a unique homomorphism h mapping $\mathfrak{A}^{(n)}$ into $(A; F)$ such that $e_i^n p = e_i^n h$, $i = 1, 2, \ldots, n$.

With Marczewski [3] [8] we call the elements $a_1, \ldots, a_n$ of $(A; F)$ *independent* if the homomorphism h induced by $e_i^n p = a_i$, $i = 1, \ldots, n$, is one-to-one. An equivalent definition is

(I) $a_1, \ldots, a_n$ are independent if $f, g \in A^{(n)}$, $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ implies $f(b_1, \ldots, b_n) = g(b_1, \ldots, b_n)$ for every $b_1, \ldots, b_n \in A$, i. e. $f = g$.

A generating system $a_1, \ldots, a_n$ is called a *basis* if $a_1, \ldots, a_n$ are independent.

The algebraic operation f $(\in A^{(n)})$ *depends on the variable* x_i if there exists elements $a_1, \ldots, a_n, a_i'$ of A such that $f(a_1, \ldots, a_i, \ldots, a_n) \neq f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$.

$A^{(n,1)}$ denotes those operations in $A^{(n)}$ which depend only on one variable. Similarly, if $f, g \in A^{(n)}$, we say that $f = g$ *depends on* x_1 if there exist $a_1, \ldots, a_n, a_1' \in A$ such that $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ and $f(a_1', a_2, \ldots, a_n) \neq g(a_1', a_2, \ldots, a_n)$. A class of algebras in which independence has many properties similar to the usual properties of independence in vector spaces was defined by E Marczewski [5]:

An algebra $(A; F)$ is called a *v-algebra* [9] when, for each pair of algebraic operations $f, g \in A^{(n)}$, if $f = g$ depends on x_1 then there exists an algebraic operation $h \in A^{(n-1)}$ such that $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ is equivalent to $x_1 = h(x_2, \ldots, x_n)$.

Now we define the notion of *n-algebra*: $(A; F)$ is an n-algebra, n being an integer, if any n distinct elements of A form a basis of $(A; F)$. We will be interested in case $n = 2$. Let us repeat the definition:

The algebra $(A; F)$ is a *2-algebra* if any two distinct elements are independent and any two distinct elements generate the whole $(A; F)$.

A special kind of algebras, namely the *near-fields*, will be needed: a near-field is an algebra $(A; +, \cdot; 0, 1)$ in which all laws of a division ring excepting the right-distributivity hold [10]. More explicitly, $(A; +; 0)$ is an Abelian group; $(A; \cdot; 0)$ is a semigroup with 0 as a zero, $(A \setminus \{0\}; \cdot; 1)$ is a group with the unit element 1; and we have the rule $a(b+c) = ab + ac$.

[8] See also [4]. This notion was originally used by G. Birkhoff [1] to define free algebras. It's usefulness to universal algebras was pointed out by E. Marczewski [3]. A thoroughgoing research in this field was made by Marczewski and his colleagues in Wrocław, namely by A. Goetz, W. Narkiewicz, W. Nitka, C. Ryll-Nardzewski, S. Świerczkowski and K. Urbanik.

[9] In [7], *v*-algebras are also called *Marczewski's algebras*. I prefer the original name, *v* for vector spaces, since Urbanik proved that with a trivial exception (when $A^{(3)} = A^{(3,1)}$) *v*-algebras are indeed vector spaces.

[10] In [2] the dual notion is used, namely, the right distribution law is postulated. For my purposes the definition adopted is more convenient.

§ 2. The coordinatization theorem. We will consider algebras $(A; -, \cdot; 0, 1)$ defined as follows:

A0. $-$ *and* $\cdot$ *are binary operations on* A; 0 *and* 1 *are elements of* A.
A1. $(A; \cdot; 0)$ *is a semigroup with* 0 *as the zero-element.*
A2. $(A \setminus \{0\}; \cdot; 1)$ *is a group with* 1 *as the unit element.*
A3. $a - 0 = a$.
A4. $a(b-c) = ab - ac$.
A5. $a-(b-c) = c$ *if* $a = b$,
$a-(b-c) = (a-b)-(a-b)(b-a)^{-1}c$ *if* $a \neq b$.

In A5, $(b-a)^{-1}$ denotes the multiplicative inverse of $b - a \neq 0$ which exists by A2, A3 and A5. In axioms A4 and A5, xy is an abbreviated form of $x \cdot y$, which convention will be adopted in the sequel.

It is obvious that if $(K; +, \cdot; 0, 1)$ is a division ring or a near field and $-$ denotes substraction, then $(K; -, \cdot; 0, 1)$ satisfies A0-A5. In this case in A5 the element $(a-b)(b-a)^{-1}$ is -1 and A5 merely says that $a-(b-c) = a-b+c$.

Algebras with properties A0-A5 can be used to construct doubly transitive minimal groups.

THEOREM 1. *Let* $(A; -, \cdot; 0, 1)$ *be an algebra satisfying* A0-A5. *Then the linear substitutions* $x \to b - ax$ $(a \neq 0)$ *are permutations on* A. *The set* $\mathfrak{LS}(A)$ *of all linear substitutions being regarded as permutations form a group* $\mathfrak{LS}(A)$ *which is doubly transitive and minimal.*

To prove this theorem we need some consequences of axioms A0-A5.

(1) $a - x = b$ *has a unique solution,* $x = a - b$ *in* A.

Indeed, $x = a - b$ is a solution by A5. Again by A5 if x is any solution then $a - b = a - (a - x) = x$; hence the uniqueness

(2) $$a - a = 0 .$$

By A5, $x = a - a$ is a solution of $a - x = a$ and so is 0 by A3. Thus (1) implies $a - a = 0$.

Let $-a$ denote the element $0 - a$; then

(3) $x \to -x$ *is a permutation of* A *leaving* 0 *fixed and* $-(-x) = x$.

Indeed, $0 - x = a$ by (1) has a unique solution; therefore $x \to -x$ is a permutation on A. By (2) we get $-0 = 0$; thus 0 is a fixed element of this permutation. Finally, putting $a = b = 0$ in A5 we get $-(-c) = c$, as stated.

(4) $$x(-y) = -xy .$$

Put $a = x$, $b = 0$, $c = y$ in A4. Since, by A1, $x0 = 0$, we conclude that $x(-y) = 0 - xy = -xy$

(5) *$x \to b - ax$ is a permutation of A if $a \neq 0$.*

If $b - ax_1 = b - ax_2$ then (1) implies $ax_1 = ax_2$ and, by A2, $x_1 = x_2$. Hence it remains to prove that $b - ax = c$ ($a \neq 0$) always has a solution. Indeed, if a^{-1} denotes the multiplicative inverse of a which exists by A2, then $x = a^{-1}(b-c)$ is a solution since $b - aa^{-1}(b-c) = b-(b-c) = c$ by A5.

(6) *Let $\alpha, \beta \in \mathfrak{LS}(A)$, i.e. $x\alpha = b_1 - a_1 x$, $x\beta = b_2 - a_2 x$ ($a_1, a_2 \neq 0$). Then $\alpha\beta \in \mathfrak{LS}(A)$.*

By definition, $x(\alpha\beta) = (x\alpha)\beta = b_2 - a_2(b_1 - a_1 x) =$ (by A4) $= b_2 - (a_2 b_1 - a_2 a_1 x)$. Now if $b_2 = a_2 b_1$, then by A5 we get $x(\alpha\beta) = a_2 a_1 x =$ (by (3)) $= 0 - (-a_2 a_1 x)$ and $-a_2 a_1 \neq 0$; thus $\alpha\beta \in \mathfrak{LS}(A)$.

If $b_2 \neq a_2 b_1$ then by A5

$$x(\alpha\beta) = (b_2 - a_2 b_1) - (b_2 - a_2 b_1)(a_2 b_1 - b_2)^{-1} a_2 a_1 x$$

and since $b_2 - a_2 b_1$, $(a_2 b_1 - b_2)^{-1}$, a_2 and a_1 are different from 0 then by A2 so is their product, and thus $\alpha\beta \in \mathfrak{LS}(A)$.

(7) *$\mathfrak{LS}(A)$ is a semigroup with unit element.*

Indeed, (3) shows that $-(-1) = 1$, thus $-(-1)x = x$ and so $\varepsilon\colon x \to x = 0 - (-1)x$, the identical mapping, is a linear substitution; thus $\varepsilon \in \mathfrak{LS}(A)$.

(8) *There exists an $\alpha \in \mathfrak{LS}(A)$ with $a\alpha = 0$, $b\alpha = 1$ ($a \neq b$).*

Put $x\alpha = (a-b)^{-1}a - (a-b)^{-1}x$; then $\alpha \in \mathfrak{LS}(A)$, and further $a\alpha = (a-b)^{-1}a - (a-b)^{-1}a = 0$ and $b\alpha = (a-b)^{-1}a - (a-b)^{-1}b =$ (by A4) $= (a-b)^{-1}(a-b) = 1$.

(9) *There exists a unique $\beta \in \mathfrak{LS}(A)$ with $0\beta = a$, $1\beta = b$ ($a \neq b$).*

Put $x\beta = a - (a-b)x$; then $\beta \in \mathfrak{LS}(A)$ and $0\beta = a - (a-b)0 = a$, $1\beta = a - (a-b) =$ (by A5) $= b$. Conversely, if $x\beta = e - fx$, $f \neq 0$, and $0\beta = a$, $1\beta = b$, then $e = 0\beta = a$, $e - f = 1\beta = b$, thus $f = e - b = a - b$, and we conclude that $x\beta = a - (a-b)x$.

(10) *$\mathfrak{LS}(A)$ is doubly transitive.*

Given $a \neq b$, $c \neq d$ we choose α and $\beta \in \mathfrak{LS}(A)$ with $a\alpha = 0$, $b\alpha = 1$, $0\beta = c$, $1\beta = d$. The linear substitutions α and β exist by (8) and (9).

Then $a(\alpha\beta) = c$, $b(\alpha\beta) = d$, $\alpha\beta \in \mathfrak{LS}(A)$, whence the statement.

(11) *$\mathfrak{LS}(A)$ is a group.*

Let α and β denote the same as in (8) and (9). Then $x(\alpha\beta) = a - -(a-b)\big((a-b)^{-1}a - (a-b)^{-1}x\big) =$ (by A4) $= a - (a-x) =$ (by A5) $= x$; thus $\alpha\beta = \varepsilon$. Similarly, $x(\beta\alpha) = (a-b)^{-1}a - (a-b)^{-1}\big(a - (a-b)x\big) =$ (by A4) $= (a-b)^{-1}a - \big((a-b)^{-1}a - x\big) =$ (by A5) $= x$; thus $\beta\alpha = \varepsilon$, which means that $\alpha = \beta^{-1}$. Now let $\gamma \in \mathfrak{LS}(A)$, $x\gamma = a - cx$ and put $b = a - c$. Then $0\gamma = a$, $1\gamma = b$ and thus $\gamma = \beta$ of (9) of which α is the inverse. Thus every element $\gamma \in \mathfrak{LS}(A)$ has an inverse.

(12) *$\mathfrak{LS}(A)$ is minimal.*

Suppose $a \neq b$, $c \neq d$ and $a\alpha = a\beta = c$, $b\alpha = b\beta = d$; we have to prove $\alpha = \beta$. Obviously, $a(\alpha\beta^{-1}) = a$, $b(\alpha\beta^{-1}) = b$; thus putting $\gamma = \alpha\beta^{-1}$ we find that γ fixed a and b. Let δ and φ satisfy $a\delta = 0$, $b\delta = 1$, $0\varphi = a$, $1\varphi = b$; then $\varphi\gamma\delta = \lambda$ fixed 0 and 1. Let $x\lambda = e - fx$; then

$$0\lambda = e - f0 = e = 0, \quad 1\lambda = e - f1 = e - f = 1, \quad \text{i.e.} \quad e = 0,\ f = -1,$$

we conclude that $\lambda = \varepsilon$. Hence $\varphi\gamma\delta = \varepsilon$, $\gamma = \varphi^{-1}\varepsilon\delta^{-1} = \varepsilon$ since δ is the inverse of φ (as noted in (11)). Thus $\alpha\beta^{-1} = \varepsilon$, $\alpha = \beta$, which was to be proved.

The statements in Theorem 1 are: (5), (11), (10) and (12); hence the proof of Theorem 1 is completed.

The main result of § 1 says that every doubly transitive minimal group is of the form $\mathfrak{LS}(A)$.

THEOREM 2 (THE COORDINATIZATION THEOREM). *Let $\mathfrak{G}$ be a doubly transitive and minimal group on A, and let 0 and 1 be fixed but arbitrary elements of A, $0 = 1$ only if $|A| = 1$. Then two binary operations, $-$ and $\cdot$, can be defined such that $(A; -, \cdot; 0, 1)$ satisfy conditions A0-A5 and $\mathfrak{G}$ is idential with $\mathfrak{LS}(A)$.*

We may suppose that A has at least two elements; let 0 and 1 denote two distinct elements of A. Given $a \neq b$ there exists a unique $\alpha_{ab} \in G$ with $a\alpha_{ab} = 0$, $b\alpha_{ab} = 1$. We will denote α_{0a}^{-1} by α^a. This α^a leaves 0 fixed and takes 1 into a. Further α_a will designate $\alpha_{0a}\alpha_{a0}^{-1}$. This α_a interchanges 0 and a. We define two operations on A:

(13) $ax = x\alpha^a$ if $a \neq 0$ and $0x = 0$

(14) $a - x = x\alpha_a$ if $a \neq 0$ and $0 - x = x$.

We are going to verify that $(A; -, \cdot; 0, 1)$ has properties A0-A5. A0 needs no verification. To prove A1 and A2 we exhibit an isomorphism between $(A\backslash\{0\}, \cdot)$ and $\mathfrak{G}$:

(15) *Let $\alpha \in G_0$ if $0\alpha = 0$. Then $\mathfrak{G}_0$ is a subgroup of $\mathfrak{G}$ and $\mathfrak{G}_0$ is transitive on $A\backslash\{0\}$.*

Both of the statements are trivial.

(16) *$a \to \alpha^{a^{-1}}$ is an isomorphism between $(A\backslash\{0\}; \cdot)$ and $\mathfrak{G}_0$.*

The elements of $\mathfrak{G}_0$ are all of the form α^a, and if $a \neq b$ then $1\alpha^a = a$, $1\alpha^b = b$, and thus $\alpha^a \neq \alpha^b$. Conversely, every α^a is an element of $\mathfrak{G}_0$ provided $a \neq 0$. Thus $a \to \alpha^{a^{-1}}$ is one-to-one from $A\backslash\{0\}$ onto $\mathfrak{G}_0$. It remains to prove $\alpha^{a^{-1}} \cdot \alpha^{b^{-1}} = \alpha^{(ab)^{-1}}$. Since $0(\alpha^{a^{-1}}\alpha^{b^{-1}}) = 0\alpha^{(ab)^{-1}} = 0$ and G is minimal, it is enough to show that $1\alpha^{a^{-1}}\alpha^{b^{-1}} = 1\alpha^{(ab)^{-1}}$. Indeed,

$$1\alpha^{a^{-1}}\alpha^{b^{-1}} = a^{-1}\alpha^{b^{-1}} = b^{-1}a^{-1}; \quad 1\alpha^{(ab)^{-1}} = (ab)^{-1}$$

thus $1\alpha^{a^{-1}}\alpha^{b^{-1}} = 1\alpha^{(ab)^{-1}}$ is equivalent to $b^{-1}a^{-1} = (ab)^{-1}$ which is valid in $\mathfrak{G}$.

(17) $$a0 = 0a = 0 .$$

Indeed, $a0 = 0\alpha^a = 0$, while $0a = 0$ is contained in (13)

(18) *$(A; \cdot; 0)$ is a semigroup with 0 as zero-element.*

Let $a, b, c \in A$; if $0 \in \{a, b, c\}$ then $(ab)c = a(bc)$ by (17); if $0 \neq \{a, b, c\}$ then the associativity follows from (16). Hence $(A; \cdot)$ is a semigroup. Further, 0 is zero, as was shown in (17).

(16) and (18) establish properties A1 and A2.

(19) $$a - 0 = a .$$

Indeed, $a - 0 = 0\alpha_a = a$.

(20) *$a - x = b$ has a unique solution.*

Let $a \neq 0$. Then α_a is a permutation of A; therefore there exists a unique c with $c\alpha_a = b$, i.e. with $a - c = b$ and c is unique. If $a = 0$, $0 - x = x$; therefore $x = b$ is the unique solution.

(21) $$a - a = 0 .$$

If $a = 0$, $0 - 0 = 0$ by definition. If $a \neq 0$ then $a - a = a\alpha_a = 0$.

(22) $$a - (a - b) = b .$$

Let $a \neq 0$. Obviously, $a - (a - x) = x\alpha_a\alpha_a$. Since α_a is the permutation interchanging a and 0, $(\alpha_a)^2$ leaves 0 and a fixed, which implies by the minimality of G that $(\alpha_a)^2 = \varepsilon$, thus $a - (a - x) = x(\alpha_a)^2 = x\varepsilon = x$. Now if $a = 0$ then $0 - (0 - x) = 0 - x = x$ by definition.

(23) *Let $a \neq b$; then* $a - (b - c) = (a - b) - (a - b)(b - a)^{-1}c$.

Put $x\alpha = a - (b - x)$, $x\beta = (a - b) - (a - b)(b - a)^{-1}\, x$. Then, $\alpha, \beta \in G$, since $\alpha = \alpha_b\alpha_a$ and $\beta = \alpha^{(b-a)^{-1}}\alpha^{(b-a)}\alpha_{(a-b)}$. Now compute

$$0\alpha = a - (b - 0) = (\text{by } (19)) = a - b ,$$

$$0\beta = (a - b) - (a - b)(b - a)^{-1}0 = a - b ,$$

$$(b - a)\alpha = a - [b(b - a)] = (\text{by } (22)) = a - a = (\text{by } (21)) = 0 ,$$

$$(b - a)\beta = (a - b) - (a - b)(b - a)^{-1}(b - a) = (a - b) - (a - b) = (\text{by } (21)) = 0 .$$

Thus we see that $0\alpha = 0\beta$, $(b - a)\alpha = (b - a)\beta$ and $a \neq b$; thus from (20) and (21) we get $b - a \neq 0$. Using the fact that G is minimal we infer $\alpha = \beta$, which was to be proved.

(24) $$a(b - c) = ab - ac .$$

If $a = 0$ we get $0 = 0 - 0$, which is included in (14). If $a \neq 0$ but $b = 0$ we get $a(-c) = -ac$, which is trivial, both sides being equal to ac. Now let $a \neq 0$, $b \neq 0$ and put

$$x\alpha = a(b - x), \quad x\beta = ab - ax .$$

We have $\alpha, \beta \in G$ since $\alpha = \alpha_b\alpha^a$, $\beta = \alpha^a\alpha_{ab}$. $0\alpha = a(b - 0) = (\text{by } (19)) = ab$ and $0\beta = ab - a0 = (\text{by } (13)) = ab - 0 = (\text{by } (19)) = ab$; $b\alpha = a(b - b) = (\text{by } (21)) = a \cdot 0 = (\text{by } (13)) = 0$, $b\beta = ab - ab = (\text{by } (21)) = 0$. Thus $0\alpha = 0\beta$, $b\alpha = b\beta$, $0 \neq b$ and again we infer $\alpha = \beta$, and the proof of (24) is finished. Since axioms A3, A4, A5 are the same as (19), (24), (22) and (23), the proof of the first statement of Theorem 2 is completed.

To complete the proof we will show that $\mathfrak{G}$ and $\mathfrak{LS}(A)$ (as defined in Theorem 1) are identical. Indeed, if $\alpha \in \mathfrak{LS}(A)$, $x\alpha = b - ax$, $a \neq 0$ then $\alpha = \alpha^a\alpha_b$, whence $\alpha \in \mathfrak{G}$. Conversely, choose an $\alpha \in \mathfrak{G}$ and put $c = 0\alpha$, $d = 1\alpha$. Then $\alpha = \alpha^{(c-d)}\alpha_c$ and since $\alpha^{(c-d)}$, $\alpha_c \in \mathfrak{LS}(A)$ we conclude that $\alpha \in \mathfrak{LS}(A)$.

Now I want to make a few comments on Theorems 1 and 2. To my opinion the natural base for studying doubly transitive minimal groups is not the algebra $(A; -, \cdot; 0, 1)$ with properties A0-A5 but the following one:

Let A be a quasi algebra $(A; -, \cdot; 0, 1)$ in which $\cdot$ is a binary operation, but $a - b$ is defined only for $a \neq 0$. The following axioms are required:

A^x0. *$a - b$ is defined whenever $a \neq 0$; $\cdot$ is a binary operation; 0 and 1 are elements of A.*

A^x1. *$(A; \cdot; 0)$ is a semigroup with 0 as the zero element.*

A^x2. *$(A\backslash\{0\}; \cdot; 1)$ is a group with 1 as the unit element.*

A^x3. *$a - 0 = a$ if $a \neq 0$.*

A^x4. *$a(b - c) = ab - ac$ if $a \neq 0$, $b \neq 0$* [11],

A^x5. *$a - (b - c) = c$ if $a = b \neq 0$,*
$a - (b - c) = (a - b) - (a - b)(b - a)^{-1}c$ if $a \neq b$, $a \neq 0$, $b \neq 0$.

It is easy to see that Theorems 1 and 2 remain valid if by linear substitution we mean $x \to ax$, $a \neq 0$, and $x \to b - ax$, $b \neq 0$, $a \neq 0$. The proof is a bit more involved, e.g. verifying (6) we have to distinguish four cases; the details will be omitted.

[11] The right side of the equation is well defined since $a \neq 0$, $b \neq 0$ implies by A^x2 that $ab \neq 0$.

Suppose we start with a division ring $\mathfrak{D} = (D; +, \cdot; 0, 1)$ and form $\mathfrak{LS}(\mathfrak{D})$ then $(D; -, \cdot; 0, 1)$. $\mathfrak{D}$ will not be recovered in Theorem 2 since we define $0-x = x$ which is not true in $\mathfrak{D}$. But the definition of ab and $a-b$, $a \neq 0$, coincides with the multiplication and substraction of $\mathfrak{D}$. Now we seen what is the advantage of considering systems with axioms A^x0-A^x5.

To formulate this observation in a precise way let A be a set, $\mathfrak{G}$ a doubly transitive and minimal group on A and $\mathfrak{A}_1 = (A; -, \cdot; 0, 1)$, $\mathfrak{A}_2 = (A; \ominus, \odot; 0, 1)$ be two systems satisfying A^x0-A^x5, further let

$$\mathfrak{LS}(\mathfrak{A}_1) = \mathfrak{LS}(\mathfrak{A}_2) = \mathfrak{G} .$$

Corollary to Theorem 2. *Under the conditions listed above $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are identical, i.e. $a-b = a \ominus b$ if $a \neq 0$ and $a \cdot b = a \odot b$ for all $a, b \in A$.*

Indeed, if A^x0-A^x5 hold true $x \to a \cdot x$ and $x \to a \odot x$, both must be permutations leaving 0 fixed and taking 1 into a, whence $a \cdot x = a \odot x = xa^a$. Similarly, $x \to a-x$ $(a \neq 0)$ must be a permutation interchanging 0 and a, whence $a-x = a \ominus x = xa_a$ if $a \neq 0$.

If we are given a system satisfying axioms A^x0-A^x5, there might be several ways of defining $0-x = -x$ so as to get a system satisfying A0-A5. Let us discuss this problem. We put $\varphi(x) = 0-x = -x$. If the resulting system satisfies axioms A0-A5, then

(25) *$x \to \varphi(x)$ is a permutation leaving 0 fixed and $\varphi(\varphi(x)) = x$.*

Indeed, (25) is the same as (3), which is a consequence of A0-A5, whence (25) must be true. In the same way (4) implies

$$a\varphi(x) = \varphi(ax) . \tag{26}$$

Let $\varphi(1) = u$. Then by (26) we get

$$\varphi(a) = au . \tag{27}$$

Rewriting (25) we get

$$au^2 = a ; \tag{28}$$

thus $u^2 = 1$.

Now we use A5 with $b = 0$, $c = 1$:

$$a-(0-1) = a-a(0-a)^{-1};$$

it follows that

$$\varphi(1) = a\varphi(a)^{-1}, \quad \text{i.e.} \quad u = au^{-1}a^{-1};$$

since $u^{-1} = u$, it follows that $ua = au$.

Theorem 3. *A system $(A; -, \cdot; 0, 1)$ satisfying axioms A^x0-A^x5 can be extended to a system satisfying axioms A0-A5 by defining $0-x = \varphi(x)$ if and only if $\varphi(x) = xu$, where u is an element of order two in the centre of $(A\backslash\{0\}; \cdot)$.*

The necessity of the conditions has already been proved, while the sufficiency follows by easy computation, which is left to the reader.

It follows from Theorem 2 that at least one extension always exists; indeed, $u = 1$ is of order two and is in the centre of $(A\backslash\{0\}; \cdot)$. Of course, this is what we chose in (14). Without an additional hypothesis I do not see how one can prove that the centre of $(A\backslash\{0\}; \cdot)$ contains an element of order two different from 1.

Thus, an algebraic way to prove the necessity of an additional hypothesis in M. Hall's theorem would be to consider a free system $(A; -, \cdot; 0, 1)$ with properties A0-A5 and to prove that $u = (a-b)(b-a)^{-1}$ $(a \neq b)$ does depend on a and b.

In this context I can prove

Theorem 4. *Let $(A; -, \cdot; 0, 1)$ satisfy axioms A^x0-A^x5 and suppose that $u = (a-b)(b-a)^{-1}$ $(a \neq b)$ does not depend on a and b, u is of order two and u is in the centre of $(A\backslash\{0\}; \cdot)$. We define addition by*

$$a+b = a-bu \tag{29}$$

and $-a$ by

$$0-a = au . \tag{30}$$

Then (and only then) $(A; +, \cdot; 0, 1)$ is a near-field.

By Theorem 3 the definition $0-a = au$ defines a system satisfying axioms A0-A5. To verify that $(A; +, \cdot; 0, 1)$ is a near-field it remains to prove that $(A; +; 0)$ is an Abelian group.

Let us substitute $c = bu$ in (29); we get

$$a+b = a-c \tag{31}$$

since $u^2 = 1$.

Further, $0-(b-a) = -b-(-b)b^{-1}a = -b-ua = bu-au = (b-a)u$, thus

$$a-b = (b-a)u . \tag{32}$$

Hence

$$a+b = a-bu = (bu-a)u = b-au = b+a ,$$

and the addition is commutative. If $a+b = a+c$, i.e. $a-bu = a-cu$, then $a-(a-bu) = a-(a-cu)$; thus, by A5, $bu = cu$ and multiplying by u we conclude that $b = c$. Finally, $a+x = b$ always has a solution, namely $x = (a-b)u$, since by A5 and (31) $a+(a-b)u = a-(a-b) = b$. The theorem is completely proved.

Corollary. *Let $\mathfrak{G}$ be a doubly transitive and minimal group acting on A. The condition that there is at most one element displacing all letters and taking a into b $(a, b \in A, a \neq b)$ is equivalent to the statement that in the system $(A; -, \cdot; 0, 1)$ constructed in Theorem 2 the element $u = (a-b)(b-a)^{-1}$ $(a \neq b)$ does not depend on a and b, $u^2 = u$ and u is in the centre of $(A\backslash\{0\}, \cdot)$.*

§ 3. 2-algebras. First we establish the connection between 2-algebras and doubly transitive minimal groups.

THEOREM 5. *Let $\mathfrak{A} = (A, \boldsymbol{F})$ be an algebra generated by any two distinct elements and let $\mathfrak{G}$ be the automorphism group of $\mathfrak{A}$. If $\mathfrak{A}$ is a 2-algebra then $\mathfrak{G}$ is doubly transitive. Conversely, if $\mathfrak{G}$ is doubly transitive and $|A| > 2$, then $\mathfrak{A}$ is a 2-algebra. If $\mathfrak{A}$ is a 2-algebra $\mathfrak{G}$ is also minimal.*

Remark. The first part of Theorem 5 was proved by Świerczkowski [6]. For completeness' sake we repeat his argument.

First, we suppose that $\mathfrak{A}$ is a 2-algebra. Let $a, b, c, d \in A$, $a \neq b$, $c \neq d$. Then $\{a, b\}$ generates $\mathfrak{A}$ and, since a, b are independent, every mapping p of a and b into A can be extended to a homomorphism of $\mathfrak{A}$ into itself. Put $ap = c$, $bp = d$; then the homomorphism h uniquely induced by p maps $\mathfrak{A}$ onto $\mathfrak{A}$. Since $cp^{-1} = a$, $dp^{-1} = b$ *can also be extended uniquely to a homomorphism of* $\mathfrak{A}$ *onto* $\mathfrak{A}$, we infer tlrat h is one-to-one, i.e. $h \in \mathfrak{G}$. Thus $\mathfrak{G}$ is doubly transitive and minimal, the latter being equivalent to the unicity of a homomorphism induced by a mapping.

Secondly, we suppose $\mathfrak{G}$ to be doubly transitive and let $a, b \in A$, $a \neq b$, $f, g \in \mathfrak{A}^{(2)}$, $f(a, b) = g(a, b)$. To prove the independence of a, b by (I) of § 1 we have to verify $f = g$.

Let $c, d \in A$; we will prove $f(c, d) = g(c, d)$. If $c = d$ this is obvious for $c = f(c, c) = g(c, c)$ since $c \neq f(c, c)$, for example, leads to a contradiction as follows: let $e \neq f(c, c)$, $e \neq c$ and let $\alpha \in G$ with $c\alpha = c$, $f(c, c)\alpha = e$; such an α exists since G is doubly transitive and such an e exists because $|A| > 2$ but α is an automorphism, and thus $e = f(c, c)\alpha = f(c\alpha, c\alpha) = f(c, c)$, which conflicts with $e \neq f(c, c)$.

Thus we may suppose that $c \neq d$ and then we may choose an $\alpha \in \mathfrak{G}$ with $a\alpha = c$, $b\alpha = d$. Obviously,

$$f(c, d) = f(a\alpha, b\alpha) = f(a, b)\alpha = g(a, b)\alpha = g(a\alpha, b\alpha) = g(c, d)\,,$$

which completes the proof of $f = g$.

COROLLARY. *Let $\mathfrak{A}$ and $\mathfrak{G}$ as in Theorem 5, $\mathfrak{G}_1$ a subgroup of $\mathfrak{G}$ which is doubly transitive on A. Then $\mathfrak{A}$ is a 2-algebra and $\mathfrak{G}_1 = \mathfrak{G}$.*

It follows from Theorem 5 that $\mathfrak{A}$ is a 2-algebra since if $\mathfrak{G}_1$ is doubly transitive then so is $\mathfrak{G}$. Again by Theorem 5, $\mathfrak{G}$ is also minimal, which implies $\mathfrak{G} = \mathfrak{G}_1$.

The following problem arises naturally from Theorem 5:

Prove (or disprove) the existence of an algebra $\mathfrak{A}$ ($|A| > 2$) the automorphisms group of which is doubly transitive and minimal, and $\mathfrak{A}$ is not a 2-algebra.

Of course, if such an $\mathfrak{A}$ exists, then by Theorem 5 there are two distinct elements in $\mathfrak{A}$ not generating $\mathfrak{A}$.

An example of 2-algebras, which was found by A. M. Macbeath (see Świerczkowski [6]; these algebras occur already in Urbanik [7]) is the following:

Let $\mathfrak{K}$ be a field, let A be the set of all elements of $\mathfrak{K}$ and let $\boldsymbol{F}$ be the class of all operations $f(x_1, x_2) = x_1\lambda + x_2(1-\lambda)$, $\lambda \in A$. Then $(A; \boldsymbol{F})$ is a 2-algebra.

Since it is obvious that $\mathfrak{G}(A; \boldsymbol{F}) = \mathfrak{LS}(K)$, which is doubly transitive, further any two distinct elements of $(A; \boldsymbol{F})$ form a generating system, the statement follows from Theorem 5.

Now we use Theorem 1 to generalize this example:

THEOREM 6. *Let $(A; -, \cdot; 0, 1)$ satisfy axioms* A0-A5. *Let $\boldsymbol{F}$ be the class of operations $f(x_1, x_2) = x_1 - (x_1 - x_2)\lambda$, $\lambda \in A$. Then $(A; \boldsymbol{F})$ is a 2-algebra.*

First we observe that any two distinct elements of A generate A. Indeed, if $a, b, c \in A$, $a \neq b$, then put $\lambda = (a-b)^{-1}(a-c)$; then $f(a, b) = a-(a-b)\lambda = a-(a-b)(a-b)^{-1}(a-c) = a-(a-c) =$ (by A5) $= c$.

Next we prove that $\alpha \in \mathfrak{LS}(A)$ is an automorphism of $(A; \boldsymbol{F})$. Obviously, $f(0, 1) =$ (by (3)) $= \lambda$. For every $\beta \in \mathfrak{LS}(A)$ we have $f(0\beta, 1\beta) = f(0, 1)\beta$. To verify this let $0\beta = a$, $1\beta = b$; we have to prove $\lambda\beta = a-(a-b)\lambda$. But in the proof of (9) (combined with (12)) we have seen that $0\beta = a$, $1\beta = b$ implies $x\beta = a-(a-b)x$, thus $\lambda\beta = a-(a-b)\lambda$. Now let $f(a, b) = a-(a-b)\lambda$ and define $\beta \in \mathfrak{LS}(A)$ by $0\beta = a$, $1\beta = b$. Then, as we have proved, $f(0\beta\alpha, 1\beta\alpha) = \lambda\beta\alpha$; now we substitute $0\beta = a$, $1\beta = b$, $\lambda\beta = f(a, b)$ and we get $f(a\alpha, b\alpha) = f(a, b)\alpha$, which means that every $\alpha \in \mathfrak{LS}(A)$ is an automorphism of $(A; \boldsymbol{F})$. Applying Theorem 1 and Corollary to Theorem 5 we infer that $(A, \boldsymbol{F})$ is a 2-algebra.

COROLLARY 1. *Let $(A; \boldsymbol{F})$ be as in Theorem 6. Then $\mathfrak{G}(A; \boldsymbol{F})$, the automorphism group of $(A; \boldsymbol{F})$, is identical with $\mathfrak{LS}(A)$.*

This follows immediately from Corollary to Theorem 5.

COROLLARY 2. *Given a doubly transitive and minimal group $\mathfrak{G}$ one can find a 2-algebra $\mathfrak{A}$ the automorphism group of which is isomorphic to $\mathfrak{G}$.*

Theorem 6 is more general even in the finite case than the example of A. M. Macbeath; this is obvious since we can construct $(A; -, \cdot; 0, 1)$ from a near-field, and the existence of finite near-fields which are not fields was proved by Zassenhaus [8].

Now we prove

THEOREM 7. *An algebra $(A; \boldsymbol{F})$ is a 2-algebra if and only if $(A; \boldsymbol{A}^{(2)})$ is a 2-algebra.*

Indeed, $(A; \boldsymbol{F})$ is a 2-algebra if given $a, b, c \in A$, $a \neq b$ there exists an $f \in \boldsymbol{A}^{(2)}$ with $c = f(a, b)$, and further, $g, h \in \boldsymbol{A}^{(2)}$, $g(a, b) = h(a, b)$ implies $g = h$. Since both conditions are imposed upon $\boldsymbol{A}^{(2)}$, the statement of Theorem 7 is obvious.

We call the 2-algebra $A = (A; \boldsymbol{F})$ *reduced* if $\boldsymbol{F} = \boldsymbol{A}^{(2)}$. Since $(A; \boldsymbol{A}^{(2)})$ is a reduced 2-algebra we infer

COROLLARY 1. *To every 2-algebra $\mathfrak{A}_1 = (A; \boldsymbol{F}_1)$ there corresponds a unique reduced 2-algebra $\mathfrak{A}_2 = (A; \boldsymbol{F}_2)$ such that $\mathfrak{G}(\mathfrak{A}_1) = \mathfrak{G}(\mathfrak{A}_2)$.*

Indeed, owing to Theorem 7 we have only to verify the uniqueness of $\mathfrak{A}_2$. Even more is true than that, namely:

COROLLARY 2. *Given a set A and a doubly transitive minimal group $\mathfrak{G}$ acting on A, there exists a unique reduced 2-algebra $\mathfrak{A}$ with $\mathfrak{G}(\mathfrak{A}) = \mathfrak{G}$*

This follows from the fact that the class of binary operations of a reduced 2-algebra is identical with the class of all possible binary operations admissible by $\mathfrak{G}$ (in the sense of Theorem 9), whence it depends only on $\mathfrak{G}$.

Let A_1, A_2 be sets and $x \to x'$ a one-to-one mapping of A_1 onto A_2. If $\mathfrak{G}_1$ is a permutation group on A_1 then let $\mathfrak{G}_2$ denote the corresponding permutation group on A_2, i.e. to every $\alpha \in G_1$ we define an $\alpha' \in G_2$ by the rule $x'\alpha' = (x\alpha)'$. Then $\alpha \to \alpha'$ is an isomorphism between $\mathfrak{G}_1$ and $\mathfrak{G}_2$; we say that this is induced by $x \to x'$. Now we can formulate

COROLLARY 3. *Let $\mathfrak{A}_1 = (A_1; \boldsymbol{F}_1)$, $\mathfrak{A}_2 = (A_2; \boldsymbol{F}_2)$ be reduced 2-algebras with the automorphism groups $\mathfrak{G}_1, \mathfrak{G}_2$, respectively. The algebras $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are isomorphic if and only if there exists a one-to-one mapping $x \to x'$ of $\mathfrak{A}_1$ onto $\mathfrak{A}_2$ which induces an isomorphism of $\mathfrak{G}_1$ and $\mathfrak{G}_2$.*

To sum up, every reduced 2-algebra $\mathfrak{A}$ is determined up to an isomorphism by its automorphism group $\mathfrak{G}$ and by the set upon which it acts (Corollary 3 to Theorem 7); further, by Theorem 5, $\mathfrak{G}$ is doubly transitive and minimal; finally, by Corollary 2 of Theorem 7, given a doubly transitive minimal group $\mathfrak{G}$ acting on A, the algebra $(A; \boldsymbol{F})$ constructed in Theorem 6 is the unique reduced 2-algebra defined on A with $\mathfrak{G}$ as an automorphism group. Thus we have proved the main result of this paper:

THEOREM 8 (REPRESENTATION THEOREM FOR REDUCED 2-ALGEBRAS). *Given a reduced 2-algebra $\mathfrak{A} = (A; \boldsymbol{F})$, one can define operations $-$ and $\cdot$ on A such that $(A; -, \cdot)$ satisfies axioms A0-A5 and $\boldsymbol{F}$ consists of operations of the form $f(x_1, x_2) = x_1 - (x_1 - x_2)\lambda$.*

Finally, we take up the problem how one can construct all possible 2-algebras. Since we know that every 2-algebra is associated with a doubly transitive and minimal group, we can formulate our problem in the following way:

Given a set A and a doubly transitive minimal group $\mathfrak{G}$ on A, describe every 2-algebra defined on A with $\mathfrak{G}$ as an automorphism group.

A rather trivial answer is given by

THEOREM 9. *Let $\mathfrak{G}$ be doubly transitive and minimal on the set A, and let $\boldsymbol{F}$ denote the class of operations defined in Theorem 6. The algebra $\mathfrak{A} = (A; \boldsymbol{H})$ is a 2-algebra with $\mathfrak{G} = \mathfrak{G}(\mathfrak{A})$ if and only if*

B1. *$\boldsymbol{F}$ is algebraic with respect to $\boldsymbol{H}$;*

B2. *$\boldsymbol{H}$ is admissible by $\mathfrak{G}$.*

Condition B1 means that $\boldsymbol{F} \subseteq \boldsymbol{A}^{(2)}(\mathfrak{A})$, i.e. we can construct the operations in $\boldsymbol{F}$ from those in $\boldsymbol{H}$. Condition B2 means that given $h = h(x_1, \ldots, x_n) \in \boldsymbol{H}$, and an $\alpha \in \mathfrak{G}$ we have $h(x_1, \ldots, x_n)\alpha = h(x_1\alpha, \ldots, x_n\alpha)$.

One more remark before we prove the theorem: in constructing $\boldsymbol{F}$ we first have to fix $0, 1 \in A$, then we form $(A; -, \cdot; 0, 1)$ satisfying A0-A5, finally we define $\boldsymbol{F}$. However, it follows from Corollary 2 to Theorem 7 that $\boldsymbol{F}$ is independent of the choice of 0 and 1; this justifies the fact that, given A and $\mathfrak{G}$, we speak of $\boldsymbol{F}$ without fixing 0 and 1.

By Theorem 7, $\mathfrak{A} = (A; \boldsymbol{H})$ is a 2-algebra if and only if $\left(A; \boldsymbol{A}^{(2)}(\mathfrak{A})\right)$ is one. Since the automorphism groups of $\mathfrak{A}$ and of $\left(A, \boldsymbol{A}^{(2)}(\mathfrak{A})\right)$ are identical, we infer from Corollary 2 to Theorem 7 that $\boldsymbol{A}^{(2)}(\mathfrak{A}) = \boldsymbol{F}$, whence B1 is verified. It easily follows from B1 that $\mathfrak{G}(\mathfrak{A})$ is a subgroup of $\mathfrak{G}$ and B2 guarantees $\mathfrak{G} = \mathfrak{G}(\mathfrak{A})$, completing the proof of the theorem.

The question arises how one can construct an operation admissible by $\mathfrak{G}$. Let A^n denote the set of all n-tuples of elements of A. We define $\mathfrak{G}$ on A^n: if $\alpha \in G$, $(a_1, \ldots, a_n) \in A^n$ then $(a_1, \ldots, a_n)\alpha = (a_1\alpha, \ldots, a_n\alpha)$. Let this permutation group of A^n be denoted by $\mathfrak{G}_n$.

Let C_λ, $\lambda \in \Lambda$ $(= \Lambda_n)$ denote the transitive constituents of A^n. Let us select a representative $c_\lambda = (c_\lambda^1, \ldots, c_\lambda^n)$ of C_λ. Let C_1 be the class of $(a_1, \ldots, a_n)$ with $a_1 = a_2 = \ldots = a_n$.

THEOREM 10. *The operations $f(x_1, \ldots, x_n)$, $n > 1$, which are admissible [12] by $\mathfrak{G}$, are in a one-to-one correspondence with the mappings p of the set $\{c_\lambda; \lambda \in \Lambda\}$ into A satisfying $c_1 p = c_1^1$ $(= c_1^2 = \ldots = c_1^n)$.*

Indeed, given an f admissible by $\mathfrak{G}$ and a $c_\lambda = (c_\lambda^1, \ldots, c_\lambda^n)$, we define a mapping of the set $\{c_\lambda; \lambda \in \Lambda\}$ into A by $c_\lambda p = f(c_\lambda^1, \ldots, c_\lambda^n)$.

Conversely, let p be a mapping of $\{c_\lambda; \lambda \in \Lambda\}$ into A; then we define

$$f(c_\lambda^1, \ldots, c_\lambda^n) = c_\lambda p .$$

Given $(a_1, \ldots, a_n) \in A^{(n)}$, there exists a unique c_λ and an $\alpha \in \mathfrak{G}$ with $a_i\alpha = c_\lambda^i$. We put

$$f(a_1, \ldots, a_n) = (c_\lambda p)\alpha^{-1} .$$

We have to prove that f is uniquely defined. Indeed, if $a_i \neq a_j$ for some $i \neq j$, then $c_\lambda^i \neq c_\lambda^j$, and since $\mathfrak{G}$ is minimal, α is uniquely determined by the condition $c_\lambda^i = a_i$, $c_\lambda^j = a_j$. Thus $f(a_1, \ldots, a_n)$ is unique. If $a_1 = \ldots = a_n$ then $c_\lambda^1 = \ldots = c_\lambda^n$, whence $\lambda = 1$ and by hypothesis $c_1 p = c_1^1$, whence $f(a_1, \ldots, a_n) = a_1$, which is independent of the choice of α.

[12] It should not be forgotten that $\mathfrak{G}$ is a doubly transitive and minimal group.

Now we are going to determine the cardinality of $A = A_n$. If $c_\lambda^1 \neq c_2^\lambda$ then the rest can be arbitrarily chosen since $(c_\lambda^1, c_\lambda^2, \ldots, c_\lambda^n)\, a = (c_\lambda^1, c_\lambda^2, d^3, \ldots, d^n)$ implies $c_\lambda^i = d^i$, $i = 3, \ldots, n$. (This follows from the minimality of $\mathfrak{G}$.) Therefore the cardinality of c_λ with $c_\lambda^1 \neq c_2^\lambda$ is $|A|^{n-2}$. Obviously, the cardinality of c_λ with $c_\lambda^1 = c_2^\lambda$ equals that of A_{n-1}; thus we get

$$|A_n| = |A_{n-1}| + |A|^{n-2}.$$

Since $|A_2| = 2$, we infer

$$|A_n| = \begin{cases} 1 + \dfrac{|A|^{n-1}-1}{|A|-1}, & \text{if } |A| \text{ is finite, } |A| > 1, \\ |A| & \text{if } |A| \text{ is infinite.} \end{cases}$$

Since by Theorem 10 the cardinality of all different operations of n-variable which are admissible by $\mathfrak{G}$ is $|A|^{|A_n|-1}$, we get

THEOREM 11. *Let $\boldsymbol{H}_n$ denote the set of all operations of n-variable $(n>1)$ admissible by $\mathfrak{G}$. Then*

$$|\boldsymbol{H}_n| = \begin{cases} |A|^{\frac{|A|^{n-1}-1}{|A|-1}} & \text{if } |A| \text{ is finite, } |A| > 1, \\ |A|^{|A|} & \text{if } |A| \text{ is infinite.} \end{cases}$$

Hence if $\boldsymbol{H} = \boldsymbol{H}_1 \cup \boldsymbol{H}_2 \cup \ldots$ then

$$|\boldsymbol{H}| = \begin{cases} \aleph_0, & \text{if } |A| \text{ is finite, } |A| > 1, \\ |A|^{|A|} & \text{if } |A| \text{ is infinite.} \end{cases}$$

COROLLARY. *Let A be a set with $|A| > 1$ and $\mathfrak{G}$ a doubly transitive and minimal group on A. The cardinality of the set of all non-isomorphic 2-algebras which are defined on A and whose automorphism groups coincide with $\mathfrak{G}$ is*

$$\begin{array}{ll} 2^{\aleph_0} & \text{if } |A| \text{ is finite,} \\ 2^{|A|^{|A|}} & \text{if } |A| \text{ is infinite.} \end{array}$$

E.g. if $|A| = 2$ then we have $2^{\aleph_0}$ non-isomorphic 2-algebras which are defined on the set of two elements. One of them was found by M. Marczewski, see Świerczkowski [6].

We now turn our attention to the problem when a 2-algebra is a v-algebra. Since $f(x, y) = z$ always has an "inverse" $x = g(y, z)$ which satisfies $f(x, y) = z$ if and only if $x = g(y, z)$, one would expect that a reduced 2-algebra is always a v-algebra. This is not the case as is shown by

THEOREM 12. *Let $(A; \boldsymbol{F})$ be a reduced 2-algebra. "Coordinatize" $(A; \boldsymbol{F})$ by $A = (A; -, \cdot; 0, 1)$ as in Theorem 8. Then $(A, \boldsymbol{F})$ is a v-algebra if and only if a division ring $\mathfrak{A}_1 = (A; +, \cdot; 0, 1)$ can be defined by $a+b = a-bu$, where u is a fixed element of A.*

If a division ring $\mathfrak{A}_1 = (A; +, \cdot; 0, 1)$ can be defined by $a+b = a-bu$, then the operations in $\boldsymbol{F}$ are of the form $f(x_1, x_2) = x_1(1-\lambda) + x_2\lambda$; thus $(A; \boldsymbol{F})$ is a v-algebra (see also [7]), since the algebraic operations are of the form $f(x_1, \ldots, x_n) = \sum x_i \lambda_i$, $\sum \lambda_i = 1$, and if $g(x_1, \ldots, x_n) = \sum x_i \mu_i$, then $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ depends on x_1 if $\lambda_1 \neq \mu_1$, and in this case $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ if and only if

$$x_1 = h(x_2, \ldots, x_n) = \sum x_i \frac{\mu_i - \lambda_i}{\lambda_1 - \mu_1} \quad \text{and} \quad \sum \frac{\mu_i - \lambda_i}{\lambda_1 - \mu_1} = 1.$$

Conversely, suppose that $(A; \boldsymbol{F})$ is a reduced v-algebra. Then $\boldsymbol{A}^{(0)}$ is void, $\boldsymbol{A}^{(2)} \neq \boldsymbol{A}^{(2,1)}$, whence $\boldsymbol{A}^{(3)} \neq \boldsymbol{A}^{(3,1)}$. Using the results of Urbanik [7], we conclude that there exists a division ring K such that A is a linear space over K. Further, there exists a linear subspace A_0 of A such that $\boldsymbol{F}$ is the class of functions $f(x_1, x_2) = x_1(1-\lambda) + x_2\lambda + a$, $\lambda \in K$, $a \in A_0$. Since $f(x, x) = x$ for every $f \in \boldsymbol{F}$, we conclude that $A_0 = \{0\}$ and $f(x_1, x_2) = x_1(1-\lambda) + x_2\lambda$. Fix an arbitrary element of A different from 0 and call it 1. We identify $\lambda \in K$ with $1 \cdot \lambda$. Since $(A; \boldsymbol{F})$ is a 2-algebra, $f(0, 1) = a$ holds with a suitable $f \in \boldsymbol{F}$; thus $a = 0(1-\lambda) + 1 \cdot \lambda = 1 \cdot \lambda$, i.e. every $a \in A$ is of the form $1 \cdot \lambda$. Since A is a vector-space $1 \cdot \lambda + 1 \cdot \mu = 1(\lambda + \mu)$ and $(1 \cdot \lambda) \cdot \mu = 1(\lambda \cdot \mu)$, $\lambda \to 1 \cdot \lambda$ is a homomorphism of K onto A; obviously, it is also an isomorphism. Hence $(A; +, \cdot; 0, 1)$ is a division ring. Since the choice of 0 and 1 was arbitrary (see [7]), we have constructed a system $(A; -, \cdot; 0, 1)$ which satisfies A^x0-A^x5. Since such a system is unique by the Corollary to Theorem 2, we conclude that any $(A; -, \cdot; 0, 1)$ satisfying A^x0-A^x5 can be extended to a division ring, which completes the proof of our theorem.

References

[1] G. Birkhoff, *Lattice theory*, New York 1948.

[2] M. Hall, Jr., *The theory of groups*, New York 1959.

[3] E. Marczewski, *A general scheme of the notions of independence in mathematics*, Bull. Acad. Pol. Sci. Ser. Math. Astr. Phys. 6 (1958), pp. 731-736.

[4] — *Independence and homomorphism in abstract algebras*, Fund. Math. 50 (1961), pp. 45-61.

[5] — *Independence in some abstract algebras*, Bull. Acad. Pol. Sci. Ser. Math. Astr. Phs. 7 (1959), pp. 611-616.

[6] S. Świerczkowski, *Algebras independently generated by every n elements*, Bull. Acad. Pol. Sci. Ser. Math. Astr. Phys. 7 (1959), pp. 499-500 and Fund. Math. 49 (1960), pp. 93-104.

[7] K. Urbanik, *Representation theorem for Marczewski's algebras*, Bull. Acad. Pol. Sci. Ser. Math. Phys. 7 (1959), pp. 617-619, and Fund. Math. 47 (1960), pp. 147-167.

[8] H. Zassenhaus, *Über endliche Fastkörper*, Abh. Math. Sem. Hamburg 11 (1936), pp. 187-220.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES

Reçu par la Rédaction le 25. 6. 1962