The $T_h$ and $S_h$ tests given by Dickson, Townes, and Hall are derivable from these tests by consideration of the requirements imposed by test (d) on the $T_h$ and $S_h$.

Using a small linear congruence machine developed by D. H. Lehmer, and with the kind assistance of Prof. and Mrs. Lehmer, the author checked the possible discriminants to $10^7$, verifying the following theorem.

**Theorem:** There are no discriminants with a single class in each genus, $3315 < \Delta < 10,000,000$.

The largest prime necessary in this test was 79.

California Institute of Technology

---

**ON FINITE EXTENDING GROUPS**

**ALBERT NEWHOUSE**

In his paper *Non-associative algebras*, A. A. Albert defined extending groups $\mathcal{G}$ for algebras $\mathfrak{A}$ with a unity element. Such groups are merely finite multiplicative groups of nonsingular linear transformations on a linear space $\mathfrak{A}$ of order $n > 1$ over a field $\mathfrak{F}$ defined so that all the transformations leave the unity element $e$ of $\mathfrak{A}$ unaltered. With respect to the basis $(e, u_2, u_3, \ldots, u_n)$ of $\mathfrak{A}$ over $\mathfrak{F}$ these groups are then isomorphic to finite groups $\mathcal{G}$ of $n$-rowed square matrices of the form

$$G = \begin{pmatrix} 1 & 0 \\ B & M \end{pmatrix},$$

where $M$ is an $(n-1)$-rowed nonsingular square matrix and $B$ a 1 by $n-1$ matrix.

In his paper Albert has raised the question of the existence of such groups $\mathcal{G}$ "such that no basis of $\mathfrak{A}$ exists for which $\mathcal{G}$ may be regarded as a permutation group."
We shall prove that such groups exist for every algebra $\mathfrak{A}$ whose order $n>2$ over $\mathfrak{F}$ and shall completely settle the case $n=2$.

If $n>2$ and the characteristic of $\mathfrak{F}$ is different from 2 then the matrix

$$G = \begin{bmatrix}
I_{n-2} & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & -1
\end{bmatrix},$$

where $I_{n-2}$ is the identity matrix of order $n-2$, generates a cyclic group $\mathfrak{C}$ of order 2. The minimum function of $G$ is $x^2 - 1$, its characteristic function is $(x-1)^{n-2}(x+1)^2$. This group is isomorphic to the permutation group of order 2, $\mathfrak{P} = [I_n, P]$, with $P$ similar to

$$\begin{bmatrix}
I_{n-2} & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{bmatrix}.$$ 

The minimum function of $P$ is $x^3 - 1$, its characteristic function is $(x-1)^{n-2}(x^2 - 1) = (x-1)^{n-1}(x+1)$. Thus $G$ is not similar to $P$ and $\mathfrak{C}$ is not a permutation group on any base of $\mathfrak{A}$.

Now let the characteristic of $\mathfrak{F}$ be 2. If $n$ is not a power of 2 then there exists an integer $m$ such that $2^m > n > 2^{m-1}$. Let $M_m$ be the companion matrix of $x^{2^{m-1}} + 1$, a square matrix of $2^{m-1}$ rows. Now let

$$N_m = \begin{bmatrix}
1 & 0 & 0 & \cdots & 0 \\
1 & 0 & M_m & & \\
& \vdots & & \ddots & \vdots \\
0 & & & & 1
\end{bmatrix},$$

a square matrix of $2^{m-1}+1$ rows.

Then

$$G = \begin{bmatrix}
I_{n-2^{m-1}+1} & 0 \\
0 & N_m
\end{bmatrix}$$

will generate a cyclic group of order $2^m$ since the characteristic and minimum function of $N_m$ is $(x+1)^{2^{m-1}+1}$, a divisor of $(x+1)^{2^m} = x^{2^m} + 1$ and not a divisor of $(x+1)^{2^{m-1}} = x^{2^{m-1}} + 1$. Thus $G$ is of order $2^m$ and $G$ cannot be any permutation of $n$ letters since one cycle would have to have $2^m > n$ letters.

If $n = 2^m > 4$, let
whose characteristic and minimum function is $x^2 + x + 1$. Then let

$$G = \begin{pmatrix} I_{2^{m-1}-3} & 0 & 0 \\ 0 & N_m & 0 \\ 0 & 0 & N \end{pmatrix},$$

an $n$-rowed square matrix. Its characteristic function is $(x+1)^{2^{m-1}}$ $(x^2+x+1)$, its minimum function is $(x+1)^{2^m-1} (x^2+x+1)$ which is a divisor of $x^{2^m+1} = (x^4+1)^{2^m} = (x+1)^{2^m} (x^2+x+1)^{2^m}$. Thus $G$ is of order $3 \cdot 2^m$. No permutation on $n = 2^m$ letters is of order $3 \cdot 2^m$ since one cycle would have to have 3 letters and one cycle $2^m$ letters.

If $n = 4$ let

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Its characteristic and minimum function is $x^4 + x^3 + x + 1$, a divisor of $x^4+1 = (x^4+x^3+x+1)(x^2+x+1)$. Thus $G$ is of order 6 and not similar to a permutation matrix since the corresponding permutation matrix would have to have cycles of 3 and 2 letters each, and there are only 4 letters.

If $n = 2$ the extending group $\mathfrak{G}$ consists of 2-rowed square matrices

$$G = \begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}.$$

Let $m$ be the order of $\mathfrak{G}$, then $G^m = I_2$, but

$$G^m = \begin{pmatrix} 1 & 0 \\ a(1 + b + \cdots + b^{m-1}) & b^m \end{pmatrix},$$

thus $b^m = 1$ and $b$ is an $m$th root of unity. Thus if $\mathfrak{G}$ contains a primitive $m$th root of unity $b$ for $m > 2$ then

$$G = \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$$

generates a cyclic group of order $m$. The characteristic function of $G$ is $x^2 - (b+1)x + b$, different from the characteristic function of any
If $\Psi$ does not contain any roots of unity besides 1 and $-1$, $b${must be 1 or $-1$ and $G$ has the form}

$$G_1 = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \text{ or } G_2 = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix},$$

so that

$$G_1^n = \begin{pmatrix} 1 & 0 \\ ma & 1 \end{pmatrix}, \quad G_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

If $\Psi$ is non-modular $\mathfrak{G}$ can only contain elements of form $G_2$. Now let

$$S = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ b & -1 \end{pmatrix}, \quad a \neq b, \quad S^2 = T^2 = I,$$

then

$$ST = \begin{pmatrix} 1 & 0 \\ a - b & 1 \end{pmatrix}.$$ 

$ST$ is of form $G_1$ and cannot be in $\mathfrak{G}$. Thus for $n=2$ and $\Psi$ non-modular there exist finite extending groups only if $\Psi$ contains a primitive $m$th root of unity for $m>2$.

If $\Psi$ is of characteristic $p>2$,

$$G = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

generates a cyclic group of order $p$. This group is not a permutation group on two letters since such a group has order two.

If $\Psi$ is of characteristic 2 and contains an extension of the prime field $GF(2)$ then $\Psi$ contains at least four elements $0$, $1$, $a$, $1+a$, $(a \neq 0, 1)$. Then

$$I, \quad R = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 1 + a & 1 \end{pmatrix},$$

$$RS = SR = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad R^2 = S^2 = (RS)^2 = (SR)^2 = I,$$

form a group of order 4 not a permutation group on two letters, since two letters have only two permutations.

If $\Psi = GF(2)$, the only nonsingular linear transformations of the prescribed form are
However, the characteristic and minimum function of $G$ is $(x+1)^2 = x^2 + 1$ and $G$ is similar to the permutation matrix

$$P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$ 

Thus we have the following theorem.

**Theorem.** For every finite algebra $\mathcal{A}$ over $\mathbb{F}$ there exist finite extending groups $\mathcal{G}$ which are not permutation groups on any basis of $\mathcal{A}$ if the order of $\mathcal{A}$ over $\mathbb{F}$ is greater than 2.

If the order of $\mathcal{A}$ over $\mathbb{F}$ is 2 there exist such extending groups if and only if

(a) $\mathbb{F}$ is non-modular and contains a primitive $m$th root of unity for $m > 2$, 

(b) $\mathbb{F}$ is of characteristic $p$ and contains more than two elements.

University of Houston