**A NECESSARY CONDITION FOR THE EXISTENCE OF
PARTIALLY BALANCED INCOMPLETE BLOCK
DESIGNS WITH AN m -SUBSET
ASSOCIATION SCHEME**

By

Koichi YAMAMOTO

(Received June 30, 1965)

Introduction. A necessary condition for the existence of partially balanced incomplete block designs with the triangular association scheme, in terms of the Hilbert norm residue symbol, was obtained by Ogawa [1]. The present paper generalizes the result for the case of partially balanced incomplete block designs with an m -subset association scheme, in which there appear m association classes, as described below, and the result of Ogawa corresponds to the special case $m=2$.

1. — Let $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$ be the set of n symbols, and let 2^Ω the set of all subsets of Ω . If a subset α of Ω consists of m elements $\omega_{a_1}, \dots, \omega_{a_m}$, then we write $\alpha = \omega_{a_1} \cdots \omega_{a_m}$, and we define $|\alpha| = m$. In this case we say that α is an m -subset of Ω . Furthermore, the join of two subsets α, β of Ω will be denoted by $\alpha\beta$, the complement of α in Ω by Ω/α , with $\Omega = \omega_1\omega_2 \cdots \omega_n$. The empty subset will be denoted by 1.

Consider the vector space W of 2^n dimensions over Q , the rational number field, spanned by the 2^n elements of 2^Ω . By defining the multiplication of basic elements α, β as above, we may regard W as a commutative algebra over Q .

If $\alpha \in 2^\Omega$ and i is a nonnegative integer, then the i -th elementary symmetric polynomial $\varphi_i(\alpha)$ is defined as the sum of all elements σ of power i such that $\sigma \subset \alpha$.

2. — Special emphasis is laid on the sub-system S_m of 2^Ω , consisting of all subsets σ of Ω such that $|\sigma| = m$.

If two elements α and β of S_m have exactly i elements in common, we say that α and β are i -associates.

We assume in this paper that $n \geq 2m$. Let $v = \binom{n}{m}$ and consider the total matrix algebra $\mathfrak{M}_v$ over Q , the field of rational numbers, of degree v . We consider the underlying vector space V_v of $\mathfrak{M}_v$ is the subspace of W , defined in 1, spanned by the v elements α of 2^Q such that $|\alpha| = m$. Therefore the row and column indices of a matrix X of $\mathfrak{M}_v$ are to be taken from the set S_m .

Define the characteristic matrix X_i of the i -th associates, by letting its (α, β) -entry be 1 or 0 according as α and β are i -th associates or not. Note that

$$(1) \quad X_i X_j = \sum_{k=0}^m c_{ijk} X_k,$$

with

$$c_{ijk} = \sum_{\lambda} \binom{k}{\lambda} \binom{m-k}{i-\lambda} \binom{m-k}{j-\lambda} \binom{n-2m+k}{m-i-j+\lambda}.$$

Thus $X_0, X_1, \dots, X_m$ generate a commutative subalgebra of degree $m+1$ of the algebra W . This subalgebra will be denoted by $\mathfrak{A}_m = \mathfrak{A}$.

Frequent use will be made of the matrix Γ_i where the (α, β) -entry is defined to be $\binom{|\alpha \cap \beta|}{i}$.

Note that

$$(2) \quad \Gamma_j = \sum_{i=0}^m \binom{i}{j} X_i,$$

$$(2) \quad X_j = \sum_{i=0}^m (-1)^{i+j} \binom{i}{j} \Gamma_i.$$

So, the $m+1$ matrices $\Gamma_0, \Gamma_1, \dots, \Gamma_m$ can be taken as a base of the algebra $\mathfrak{A}_m$.

§ 1. The algebra $\mathfrak{A}_m$.

3. — First we list several combinatorial lemmas.

LEMMA 1. If $a \geq b \geq 0, f \geq 0$ and $b = c + d$, then

$$\sum_i \binom{a-i}{b} \binom{c}{f-i} \binom{d}{i} = \binom{a-f}{a-b} \binom{a-d}{f},$$

summation being taken over all $i \geq 0$.

PROOF. Since $\binom{a-i}{b} = \sum_j \binom{d-i}{j} \binom{a-d}{b-j}$

and

$$\binom{d}{i} \binom{d-i}{j} = \binom{d}{j} \binom{d-j}{i},$$

we have

$$\begin{aligned}
& \sum_i \binom{a-i}{b} \binom{c}{f-i} \binom{d}{j} = \sum_i \sum_j \binom{d}{i} \binom{d-i}{j} \binom{a-d}{b-j} \binom{c}{f-i} \\
& = \sum_j \binom{d}{j} \binom{a-d}{b-j} \sum_i \binom{d-j}{i} \binom{c}{f-i} = \sum_j \binom{d}{j} \binom{a-d}{b-j} \binom{c+d-j}{f} \\
& = \sum_j \binom{d}{j} \binom{a-d}{b-j} \binom{b-j}{f} = \binom{a-d}{f} \sum_j \binom{d}{j} \binom{a-d-f}{b-f-j} \\
& = \binom{a-d}{f} \binom{a-f}{b-f} = \binom{a-d}{f} \binom{a-f}{a-b}.
\end{aligned}$$

LEMMA 2.
$$\binom{a-s}{b} = \sum_{i=0}^s (-1)^i \binom{s}{i} \binom{a-i}{b-i}.$$

PROOF. The right-hand side member is

$$= \sum_{i=0}^s (-1)^i \binom{s}{i} \binom{-a-b-1}{b-i} = (-1)^b \binom{-a-b+s-1}{b} = \binom{a-s}{b}.$$

Next we observe following

LEMMA 3.
$$\sum_{|\alpha|=j} \alpha \varphi_{m-i}(\Omega/\alpha) = \binom{m-i+j}{j} \varphi_{m-i+j}(\Omega).$$

PROOF. On the left-hand side member appears each element $\alpha\xi$ with $\xi \subset \Omega/\alpha$, $|\alpha\xi| = m-i+j$. On the other hand for each $(m-i+j)$ -subset η there are exactly $\binom{m-i+j}{j}$ ways to write $\eta = \alpha\xi$ with $|\alpha| = j$, $\xi \subset \Omega/\alpha$.

4. — Now let σ be a typical element of S_m . Define

$$\Gamma_i(\sigma) = \sum_{\substack{|\alpha|=i \\ \alpha \subset \sigma}} \alpha \varphi_{m-i}(\Omega/\alpha),$$

and extend Γ_i to a linear transformation of the vector space V_v .

We note that $\Gamma_i(\sigma) = \sum_{\tau \in S_m} \binom{|\sigma \frown \tau|}{i} \tau$, i.e., $\Gamma_i(\sigma)$ is the sum of elements τ of S_m with the coefficients $\binom{j}{i}$, if σ and τ are j -th associates. Therefore, the corresponding matrix form of the linear transformation is precisely (2), if we consider in reference to the natural basis S_m of V_v .

In this connection we need the following

LEMMA 4.
$$\Gamma_i(\sigma) = \sum_{l=i}^m \binom{l}{i} \varphi_l(\sigma) \varphi_{m-l}(\Omega/\sigma).$$

PROOF. We have,

$$\begin{aligned}
\Gamma_i(\sigma) &= \sum_{\substack{|\alpha|=i \\ \alpha \subset \sigma}} \alpha \varphi_{m-i}(\Omega/\alpha) = \sum_{\substack{|\alpha|=i \\ \alpha \subset \sigma}} \alpha \varphi_{m-i}((\Omega/\sigma)(\sigma/\alpha)) \\
&= \sum_{\substack{|\alpha|=0 \\ \alpha \subset \sigma}} \sum_{l=0}^{m-i} \varphi_l(\Omega/\sigma) \varphi_{m-i-l}(\sigma/\alpha)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{l=0}^{m-i} \varphi_l(\Omega/\sigma) \sum_{\substack{|\alpha|=i \\ \alpha \subset \sigma}} \alpha \varphi_{m-i-l}(\sigma/\alpha) \\
&= \sum_{l=0}^{m-i} \varphi_l(\Omega/\sigma) \binom{m-l}{i} \varphi_{m-l}(\sigma),
\end{aligned}$$

by using Lemma 3.

5. — Our aim is to express $\Gamma_i \Gamma_j$ as a linear combination of Γ_k . It is readily seen that $\Gamma_j \Gamma_i = \Gamma_i \Gamma_j$ from (2), (3). However we have to determine the precise coefficients.

If we introduce the incidence function ε_σ by

$$\begin{aligned}
\varepsilon_\sigma(\alpha) &= 1 & \text{for } \alpha \subset \sigma, \\
\varepsilon_\sigma(\alpha) &= 0 & \text{for } \alpha \not\subset \sigma,
\end{aligned}$$

then $\Gamma_i(\sigma)$ can be written as

$$\Gamma_i(\sigma) = \sum_{|\alpha|=i} \varepsilon_\sigma(\alpha) \alpha \varphi_{m-i}(\Omega/\alpha).$$

Moreover if we define

$$H_k(\sigma) = \sum_{|\sigma \cap \tau|=k} \tau,$$

the sum of k -th associates of σ , then we have

$$\begin{aligned}
\Gamma_j(\Gamma_i(\sigma)) &= \Gamma_j\left(\sum_{k=0}^m \binom{k}{i} H_k(\sigma)\right) = \sum_{k=0}^m \binom{k}{i} \Gamma_j(H_k(\sigma)) \\
&= \sum_{k=0}^m \binom{k}{i} \sum_{|\sigma \cap \tau|=k} \Gamma_j(\tau) = \sum_{k=0}^m \binom{k}{i} \sum_{|\tau \cap \sigma|=k} \sum_{|\alpha|=j} \varepsilon_\tau(\alpha) \alpha \varphi_{m-j}(\Omega/\alpha),
\end{aligned}$$

i.e.,

$$(4) \quad \Gamma_j(\Gamma_i(\sigma)) = \sum_{|\alpha|=j} \theta(\alpha) \alpha \varphi_{m-j}(\Omega/\alpha),$$

where

$$(5) \quad \theta(\alpha) = \sum_{k=0}^m \binom{k}{i} \sum_{|\tau \cap \sigma|=k} \varepsilon_\tau(\alpha).$$

The inner sum in (5) practically enumerates τ 's in S_m such that $\tau \supset \alpha$, $|\tau \cap \sigma| = k$.

We carry this enumeration out by the classification on $\beta = \tau \cap \sigma$.

First consider the number $A_{\alpha\beta}$ of τ 's in S_m such that $\tau \supset \alpha$ and $\tau \cap \sigma = \beta$, assuming that α , β and σ are fixed in such away that $|\alpha| = j$, $|\beta| = k$, $|\sigma| = m$, and $\sigma \supset \beta \supset \alpha \cap \sigma$. Then $\tau = \alpha \beta \rho$ with $\rho \subset \Omega/(\sigma \alpha)$. Here $|\rho| = m - k - j + u$, $|\Omega/(\sigma \alpha)| = n - m - j + u$, if $u = |\alpha \cap \beta| = |\alpha \cap \sigma|$. Thus $A_{\alpha\beta} = \binom{n-m-j+u}{m-k-j+u}$, which is independent of β , as long as $\sigma \supset \beta \supset \alpha \cap \sigma$. The number of choices of β in this manner is $\binom{m-u}{k-u}$. Therefore, returning to (5) we have that

$$\begin{aligned}
\theta(\alpha) &= \sum_{k=0}^m \binom{k}{i} \binom{m-u}{k-u} \binom{n-m-j+u}{m-k-j+u} \\
&= \sum_{k=0}^m \sum_{l=0}^u \binom{h-u}{i-l} \binom{u}{l} \binom{m-u}{k-u} \binom{n-m-j+u}{m-k-j+u} \\
&= \sum_{l=0}^u \binom{u}{l} \sum_{k=0}^m \binom{m-u}{k-u} \binom{k-u}{i-l} \binom{n-m-j+u}{m-k-j+u} \\
&= \sum_{l=0}^u \binom{u}{l} \binom{m-u}{i-l} \sum_{k=0}^m \binom{m-u-i+l}{k-u-i+l} \binom{n-m-j+u}{m-k-j+u} \\
&= \sum_{l=0}^u \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l}.
\end{aligned}$$

Thus, returning to (4) we have that

$$(6) \quad \Gamma_j(\Gamma_i(\sigma)) = \sum_{u=0}^m \left(\sum_{l=0}^u \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \right) \sum_{\substack{|\alpha|=j \\ |\alpha \frown \sigma|=u}} \alpha \varphi_{m-j}(\Omega/\alpha).$$

6. — In order to evaluate the last sum in (6), let $\beta = \alpha \frown \sigma$ and consider the partial sum for a fixed β . If $|\beta| = u$, then we have

$$\begin{aligned}
\sum_{\substack{|\alpha|=j \\ \alpha \frown \sigma = \beta}} \alpha \varphi_{m-j}(\Omega/\alpha) &= \sum_{\substack{|\gamma|=j-u \\ \gamma \subset \Omega/\sigma}} \beta \gamma \varphi_{m-j}(\Omega/(\beta\gamma)) \\
&= \beta \sum_{\substack{|\gamma|=j-u \\ \gamma \subset \Omega/\sigma}} \gamma \varphi_{m-j}((\Omega/\beta)/\gamma) \\
&= \beta \sum_{\substack{|\gamma|=j-u \\ \gamma \subset \Omega/\sigma}} \gamma \sum_{t=0}^{m-j} \varphi_t(\sigma/\beta) \varphi_{m-j-t}(\Omega/(\sigma\gamma)) \\
&= \beta \sum_{t=0}^{m-j} \varphi_t(\sigma/\beta) \sum_{\substack{|\gamma|=j-u \\ \gamma \subset \Omega/\sigma}} \gamma \varphi_{m-j-t}((\Omega/\sigma)/\gamma) \\
&= \beta \sum_{t=0}^{m-j} \varphi_t(\sigma/\beta) \binom{m-t-u}{j-u} \varphi_{m-t-u}(\Omega/\sigma),
\end{aligned}$$

by using Lemma 3. Returning to the last sum in (9) we have

$$\begin{aligned}
\sum_{\substack{|\alpha|=j \\ |\alpha \frown \sigma|=u}} \alpha \varphi_{m-j}(\Omega/\alpha) &= \sum_{|\alpha|=j} \sum_{u=0}^j \sum_{\substack{|\beta|=u \\ \beta = \alpha \frown \sigma}} \alpha \varphi_{m-j}(\Omega/\alpha) \\
&= \sum_{\substack{|\beta|=u \\ \beta \subset \sigma}} \sum_{\substack{|\alpha|=j \\ \alpha \frown \sigma = \beta}} \alpha \varphi_{m-j}(\Omega/\alpha) \\
&= \sum_{\substack{|\beta|=u \\ \beta \subset \sigma}} \beta \sum_{t=0}^{m-j} \binom{m-t-u}{j-u} \varphi_t(\sigma/\beta) \varphi_{m-t-u}(\Omega/\sigma) \\
&= \sum_{t=0}^{m-j} \binom{m-t-u}{j-u} \varphi_{m-t-u}(\Omega/\sigma) \sum_{\substack{|\beta|=u \\ \beta \subset \sigma}} \beta \varphi_t(\sigma/\beta)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{t=0}^{m-j} \binom{m-t-u}{j-u} \varphi_{m-t-u}(\Omega/\sigma) \binom{u+t}{u} \varphi_{u+t}(\sigma) \\
&= \sum_{t=0}^{m-j} \binom{m-t-u}{j-u} \binom{t+u}{u} \varphi_{t+u}(\sigma) \varphi_{m-t-u}(\Omega/\sigma).
\end{aligned}$$

Thus (6) is now written as

$$\begin{aligned}
(7) \quad & \Gamma_j \Gamma_i(\sigma) \\
&= \sum_{u=0}^m \left(\sum_{l=0}^u \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \right) \sum_{t=0}^{m-j} \binom{t+u}{u} \binom{m-t-u}{j-u} \varphi_{t+u}(\sigma) \varphi_{m-t-u}(\Omega/\sigma) \\
&= \sum_{w=0}^m \left(\sum_{u=0}^m \sum_{l=0}^u \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \binom{w}{u} \binom{m-w}{j-u} \right) \varphi_w(\sigma) \varphi_{m-w}(\Omega/\sigma).
\end{aligned}$$

7. — Let us consider the inner sum in (7). By applying Lemma 2 we have that, for $w=u+t$,

$$\begin{aligned}
\binom{w}{u} \binom{m-w}{j-u} &= \binom{w}{u} \binom{m-u-t}{j-u} = \sum_{r=0}^t (-1)^r \binom{w}{u} \binom{t}{r} \binom{m-u-r}{j-u-r} \\
&= (-1)^u \sum_{s=0}^w (-1)^s \binom{w}{s} \binom{m-s}{j-s}.
\end{aligned}$$

Thus we can transform (7) as follows:

$$\begin{aligned}
& \Gamma_j(\Gamma_i(\sigma)) \\
&= \sum_{w=0}^w \sum_{u=0}^m \sum_{l=0}^u \sum_{s=0}^w (-1)^{u+s} \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \binom{w}{s} \binom{s}{u} \binom{m-s}{j-s} \varphi_w(\sigma) \varphi_{m-w}(\Omega/\sigma) \\
&= \sum_{u=0}^m \sum_{l=0}^u \sum_{s=0}^m (-1)^{u+s} \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \binom{s}{u} \binom{m-s}{j-s} \sum_{s=0}^w \binom{w}{s} \varphi_w(\sigma) \varphi_{m-w}(\Omega/\sigma) \\
&= \sum_{s=0}^m \left(\sum_{u=0}^m \sum_{l=0}^u (-1)^{s+u} \binom{u}{l} \binom{m-u}{i-l} \binom{n-i-j+l}{m-i-j+l} \binom{s}{u} \binom{m-s}{j-s} \right) \Gamma_s(\sigma),
\end{aligned}$$

by using Lemma 4. The above is written as

$$\Gamma_j(\Gamma_i(\sigma)) = \sum_{s=0}^m d_{ji,s} \Gamma_s(\sigma),$$

or

$$\Gamma_j \Gamma_i = \sum_{s=0}^m d_{ji,s} \Gamma_s$$

with

$$d_{ji,s} = (-1)^s \sum_{l=0}^m \left(\sum_{u=0}^m (-1)^u \binom{u}{l} \binom{s}{u} \binom{m-u}{i-l} \right) \binom{m-s}{j-s} \binom{n-i-j+l}{m-i-j+l}.$$

For the inner sum over u we have

$$\begin{aligned}
& \sum_{u=l}^m (-1)^u \binom{u}{l} \binom{s}{u} \binom{m-u}{i-l} \\
&= \binom{s}{l} \sum_{u=l}^m (-1)^u \binom{s-l}{u-l} (-1)^{i-1+m-u} \binom{-i+l-1}{m-u-i+1} \\
&= (-1)^{i+l+m} \binom{s}{l} \binom{s-i-l}{m-i} = (-1)^l \binom{s}{l} \binom{m-s}{m-i}.
\end{aligned}$$

Hence

$$\begin{aligned}
d_{ji,s} &= \sum_{l=0}^m (-1)^{s+l} \binom{s}{l} \binom{m-s}{m-i} \binom{m-s}{j-s} \binom{n-i-j+l}{m-i-j+l} \\
&= \binom{m-s}{i-s} \binom{m-s}{j-s} \sum_{l=0}^m (-1)^{s+l} \binom{s}{l} \binom{n-i-j+l}{m-i-j+l} \\
&= \binom{m-s}{i-s} \binom{m-s}{j-s} (-1)^{s+m+i+j} \sum_{l=0}^m \binom{s}{s-l} \binom{-n+m-l}{m-i-j+l} \\
&= (-1)^{s+m+i+j} \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{s-n+m-1}{s+m-i-j} \\
&= \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s}.
\end{aligned}$$

Thus we have proved

$$\text{THEOREM 1. } \Gamma_i \Gamma_j = \sum_{s=0}^{\min(i,j)} \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} \Gamma_s.$$

Compare this with the tremendously complicated multiplication constants in (1) for the basic elements X_i of the algebra $\mathfrak{A}_m$.

8. — We pause here to determine the rank of the matrices Γ_i . In fact, the rank of Γ_i , namely $\dim \Gamma_i V$ is $\binom{n}{i}$.

In order to show this we begin with

LEMMA 5. *The subspace of V , spanned by the $\binom{n}{i}$ vectors $\alpha \varphi_{m-i}(\Omega/\alpha)$, corresponding to $\binom{n}{i}$ i -subsets α of Ω , has dimension $\binom{n}{i}$.*

PROOF. We have to show that the $\binom{n}{i}$ vectors $\alpha \varphi_{m-i}(\Omega/\alpha)$ are linearly independent. Now, if $\sum_{\alpha} c_{\alpha} \alpha \varphi_{m-i}(\Omega/\alpha) = 0$, then since $\alpha \varphi_{m-i}(\Omega/\alpha) = \sum_{\tau \supset \alpha} \tau$ we have that $\sum_{\tau} (\sum_{\alpha \subset \tau} c_{\alpha}) \tau = 0$, $\sum_{\alpha \subset \tau} c_{\alpha} = 0$ for all τ in S_m .

We prove the assertion

$$(9) \quad \sum_{\alpha \subset \tau} c_{\alpha} = 0 \text{ for all } \tau \text{ in } S_m \longrightarrow c_{\alpha} = 0 \text{ for all } i\text{-subsets } \alpha,$$

by an induction on i . If $i=0$, then (9) is obvious since then there is only one 0-subset, namely 1.

Therefore assume $i \geq 1$ and assume the validity of (9) for $i-1$. We note

here that $n \geq 2m \geq 2i$, so $m \geq 1$. Let $\tau = p\vartheta$, $|p|=1$, $|\vartheta|=m-1$, then $\alpha \supset \tau$ implies that $\alpha \subset \vartheta$ or $\alpha = p\beta$ with $\beta \subset \vartheta$. So if $\sum_{\alpha \subset \tau} c_\alpha = 0$, then

$$\sum_{\alpha \subset \tau} c_\alpha = \sum_{\substack{\alpha \subset \vartheta \\ |\alpha|=i}} c_\alpha + \sum_{\substack{\beta \subset \vartheta \\ |\beta|=i-1}} c_{p\beta} = 0$$

for all p and ϑ such that $|p|=1$, $|\vartheta|=m-1$, and $p \notin \vartheta$. Thus,

$$\sum_{\substack{\alpha \subset \vartheta \\ |\alpha|=1}} c_\alpha + \sum_{\substack{\beta \subset \vartheta \\ |\beta|=i-1}} c_{p\beta} = \sum_{\substack{\alpha \subset \vartheta \\ |\alpha|=i}} c_\alpha + \sum_{\substack{\beta \subset \vartheta \\ |\beta|=i-1}} c_{q\beta}$$

if $p \notin \vartheta$, $q \notin \vartheta$ and $|q|=1$. Hence

$$\sum_{\substack{\beta \subset \vartheta \\ |\beta|=i-1}} (c_{p\beta} - c_{q\beta}) = 0 \quad \text{for } p \notin \vartheta, q \notin \vartheta$$

By assumption the above implies that $c_{p\beta} = c_{q\beta}$ if $p \notin \vartheta$, $q \notin \vartheta$. This means that $c_\alpha = c_{\alpha'}$, if α and α' differ from each other by only one element. Therefore c_α is a constant for all i -subset α . This constant is 0 since $\sum_{\alpha \subset \tau} c_\alpha = 0$. This completes the proof of Lemma 5.

THEOREM 2. $\Gamma_0 V \subset \Gamma_1 V \subset \dots \subset \Gamma_m V$.

$$\text{rank } \Gamma_i = \binom{n}{i} \quad \text{for } i=0, 1, \dots, m.$$

PROOF. Let A be the incidence matrix of the system S_m and the system S_i of the $\binom{n}{i}$ i -subsets of Ω . If $|\tau|=m$, $|\alpha|=i$, then the (τ, α) -entry of A is 1 or 0 according as $\tau \supset \alpha$ or not. We have seen that the rank of the matrix A is $\binom{n}{i}$. Therefore we can select $\binom{n}{i}$ m -subsets $\sigma_1, \sigma_2, \dots, \sigma_N$, $N = \binom{n}{i}$ such that the corresponding rows are linearly independent. We assert that the vectors $\Gamma_i(\sigma_1), \Gamma_i(\sigma_2), \dots, \Gamma_i(\sigma_N)$ are linearly independent. Indeed if $\sum_{j=1}^N c_j \Gamma_i(\sigma_j) = 0$, then

$$0 = \sum_{j=1}^N c_j \sum_{\alpha \subset \sigma_j} \alpha \varphi_{m-i}(\Omega/\alpha) = \sum_{|\alpha|=i} \left(\sum_{\sigma_j \supset \alpha} c_j \right) \alpha \varphi_{m-i}(\Omega/\alpha).$$

This implies $\sum_{\sigma_j \supset \alpha} c_j = 0$ by Lemma 5. If $\varepsilon(\tau, \alpha)$ is the (τ, α) -entry of the incidence matrix A above then

$$\sum_{j=1}^N \varepsilon(\sigma_j, \alpha) c_j = 0 \quad \text{for all } \alpha \in S_i.$$

Since $\det(\varepsilon(\sigma_j, \alpha)) \neq 0$, by the choice of the rows $\sigma_1, \dots, \sigma_N$, the above implies $c_j = 0$ for $j=1, \dots, N$. Thus $\Gamma_i(\sigma_1), \Gamma_i(\sigma_2), \dots, \Gamma_i(\sigma_N)$ are linearly independent, and the rank of Γ_i is precisely $N = \binom{n}{i}$. This proves the second part of Theorem 2. Note that $\Gamma_i V$ is spanned by $\alpha \varphi_{m-i}(\Omega/\alpha)$ with $\alpha \in S_i$.

Now the first part is evident since for the basic elements of $\Gamma_i V$. We have

$$\alpha\varphi_{m-i}(\mathcal{Q}/\alpha) = \sum_{p \subset \mathcal{Q}/\alpha} \alpha p \varphi_{m-i-1}(\mathcal{Q}/(p\alpha))$$

as long as $m-i \geq 1$, or $\Gamma_i V \subset \Gamma_{i+1} V$ as long as $i \leq m-1$.

§ 2. Decomposition of the algebra $\mathfrak{A}_m$ into sum of fields.

9. — The commutative algebra $\mathfrak{A}_m$ can be decomposed into a direct sum of $m+1$ fields each isomorphic with Q . The actual decomposition is based on the $m+1$ mutually orthogonal idempotents of $\mathfrak{A}_m$.

LEMMA 6. *If we define $E_i^{(t)}$ for $0 \leq i \leq m$, $0 \leq t \leq m$ inductively by*

$$(10) \quad E_i^{(0)} = \Gamma_i \quad (0 \leq i \leq m),$$

$$(11) \quad E_i^{(t+1)} = E_i^{(t)} - \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t}}{\binom{n-2t}{m-t}} E_i^{(t)} \quad (0 \leq t \leq m, 0 \leq i \leq m),$$

then we have the relations

$$\text{i) } E_i^{(t)} = 0 \quad \text{if } i < t,$$

$$\text{ii) } E_i^{(t)} E_{i-1}^{(t-1)} = 0 \quad \text{for } 0 \leq i \leq m, 1 \leq t \leq m,$$

$$\text{iii) } E_i^{(t)} E_i^{(t)} = \binom{n-2t}{m-t} E_i^{(t)} \quad \text{for } 0 \leq t \leq m,$$

$$\text{iv) } E_i^{(t)} E_j^{(t)} = \sum_{s=t}^m \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} E_i^{(t)} \\ \text{for } 0 \leq t \leq m, 0 \leq i \leq m, 0 \leq j \leq m.$$

PROOF. We proceed by an induction on t . If $t=0$, then i) and ii) assert nothing, iv) is exactly Theorem 1, iii) is a special case of iv). Thus all the assertions are valid if $t=0$. Therefore assume $t \geq 0$, $t < m$ and assume the validity of i), ii), iv) for t . Then we have

$$E_i^{(t+1)} = E_i^{(t)} - \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t}}{\binom{n-2t}{m-t}} E_i^{(t)} = 0 \quad (\text{if } i < t),$$

$$E_i^{(t+1)} = E_i^{(t)} - \frac{\binom{n-2t}{m-t} \binom{m-t}{0}}{\binom{n-2t}{m-t}} E_i^{(t)} = 0.$$

Thus i) is valid for $t+1$. As for ii), we have only to consider the case where $i \leq t+1$:

$$\begin{aligned}
E_i^{(t+1)} E_i^{(t)} &= E_i^{(t)} E_i^{(t)} - \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t}}{\binom{n-2t}{m-t}} E_i^{(t)} E_i^{(t)} \\
&= \binom{m-t}{i-t} \binom{n-t-i}{m-i} E_i^{(t)} - \binom{n-t-i}{m-i} \binom{m-t}{i-t} E_i^{(t)} = 0
\end{aligned}$$

by assumption. iii) is again a special case of iv). As for iv), we may assume $i \geq t+1$ and $j \geq t+1$ in view of i). Now, from (11) we have

$$\begin{aligned}
E_i^{(t)} E_j^{(t)} &= \left(E_i^{(t+1)} + \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t}}{\binom{n-2t}{m-t}} E_i^{(t)} \right) \left(E_j^{(t+1)} + \frac{\binom{n-t-j}{m-j} \binom{m-t}{j-t}}{\binom{n-2t}{m-t}} E_j^{(t)} \right) \\
&= E_i^{(t+1)} E_j^{(t+1)} + \frac{\binom{n-t-i}{m-i} \binom{n-t-j}{m-j} \binom{m-t}{i-t} \binom{m-t}{j-t}}{\binom{n-2t}{m-t}} E_i^{(t)}
\end{aligned}$$

by using ii) and iii) for the case of t . Therefore

$$\begin{aligned}
E_i^{(t+1)} E_j^{(t+1)} &= E_i^{(t)} E_j^{(t)} - \frac{\binom{n-t-i}{m-i} \binom{n-t-j}{m-j} \binom{m-t}{i-t} \binom{m-t}{j-t}}{\binom{n-2t}{m-t}} E_i^{(t)} \\
&= \sum_{s=t}^m \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} \left(E_s^{(t+1)} + \frac{\binom{n-t-s}{m-s} \binom{m-t}{s-t}}{\binom{n-2t}{m-t}} E_s^{(t)} \right) \\
&\quad - \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t} \binom{n-t-j}{m-j} \binom{m-t}{j-t}}{\binom{n-2t}{m-t}} E_i^{(t)} \\
&= \sum_{s=t+1}^m \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} E_s^{(t+1)} \\
&\quad + \left(\sum_{s=t}^m \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} \frac{\binom{n-t-s}{m-s} \binom{m-t}{s-t}}{\binom{n-2t}{m-t}} \right. \\
&\quad \left. - \frac{\binom{n-t-i}{m-i} \binom{m-t}{i-t} \binom{n-t-j}{m-j} \binom{m-t}{j-t}}{\binom{n-2t}{m-t}} \right) E_i^{(t)},
\end{aligned}$$

and we have only to show that

$$\begin{aligned}
(12) \quad & \sum_{s=t}^m \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} \binom{n-s-t}{m-s} \binom{m-t}{s-t} \\
&= \binom{m-t}{i-t} \binom{m-t}{j-t} \binom{n-t-i}{m-i} \binom{n-t-j}{m-j}.
\end{aligned}$$

On the left-hand side member of (12) we note that

$$\begin{aligned} & \binom{m-s}{i-s} \binom{m-s}{j-s} \binom{n-i-j}{m-i-j+s} \binom{n-s-t}{m-s} \binom{m-t}{s-t} \\ &= \binom{n-t-i}{m-i} \binom{m-t}{j-t} \binom{n-t-s}{n-t-i} \binom{n-i-j}{n-m-s} \binom{j-t}{s-t}, \end{aligned}$$

so that the left-hand side member of (12) is

$$\begin{aligned} &= \binom{n-t-i}{m-i} \binom{m-t}{j-t} \sum_{s=t}^m \binom{n-t-s}{n-t-i} \binom{n-i-j}{n-m-s} \binom{j-t}{s-t} \\ &= \binom{n-t-i}{m-i} \binom{m-t}{j-t} \sum_{u=0}^{m-t} \binom{n-2t-u}{n-t-i} \binom{n-i-j}{n-m-t-u} \binom{j-t}{u} \\ &= \binom{n-t-i}{m-i} \binom{m-t}{j-t} \binom{m-t}{i-t} \binom{n-t-j}{m-j}, \end{aligned}$$

by using Lemma 2. This shows that iv) is true for $t+1$, and the Lemma 8 is now proved.

10. — The following Lemma gives an explicit expression for the quantity $E_i^{(t)}$.

LEMMA 7. *If $i > t \geq 0$ then*

$$E_i^{(t+1)} = \Gamma_i - \sum_{j=0}^t (-1)^j \frac{\binom{i-t+j-1}{j} \binom{m-t+j}{i-t+j}^2}{\binom{n-2t+j}{i-t+j}} \Gamma_{i-j}.$$

PROOF. First we note that the inductive definition (11) of $E_i^{(t+1)}$ may be written as

$$(13) \quad E_i^{(t+1)} = E_i^{(t)} - \frac{\binom{m-t}{i-t}^2}{\binom{n-t}{i-t}} E_i^{(t)}$$

in case $i > t$.

Now the Lemma is proved by an induction on t . If $t=0$, then the assertion of the Lemma is that

$$E^{(1)} = \Gamma_i - \frac{\binom{m}{i}}{\binom{n}{i}} \Gamma_0,$$

which is nothing but (13). So, let $t \geq 1$ and assume the validity of the Lemma for $t-1$. Now, it follows from (13) that

$$\begin{aligned}
E_i^{(t+1)} &= \Gamma_i - \sum_{j=0}^{t-1} (-1)^j \frac{\binom{i-t+j}{j} \binom{m-t+1+j}{i-t+1+j}^2}{\binom{n-2t+2+j}{i-t+1+j}} \Gamma_{i-t-1-j} \\
&\quad - \frac{\binom{m-t}{i-t}^2}{\binom{n-2t}{i-t}} \left(\Gamma_i - \sum_{j=0}^{t-1} (-1)^j \frac{\binom{m-t+1+j}{j+1}^2}{\binom{n-2t+2+j}{j+1}} \Gamma_{i-t-1-j} \right) \\
&= \Gamma_i - \frac{\binom{m-t}{i-t}^2}{\binom{n-2t}{i-t}} \Gamma_i + \\
&\quad \sum_{j=1}^{t-1} (-1)^j \left(\frac{\binom{m-t}{i-t}^2 \binom{m-t+1+j}{j+1}^2}{\binom{n-2t}{i-t} \binom{n-2t+2+j}{j+1}} - \frac{\binom{i-t+j}{j} \binom{m-t+1+j}{i-t+1+j}^2}{\binom{n-2t+2+j}{i-t+j+1}} \right) \Gamma_{i-t-j} \\
&= \Gamma_i - \frac{\binom{m-t}{i-t}^2}{\binom{n-2t}{i-t}} \Gamma_i - \sum_{j=1}^t (-1)^j P_j \Gamma_{i-j},
\end{aligned}$$

where

$$(14) \quad P_j = \frac{\binom{m-t}{i-t}^2 \binom{m-t+j}{j}^2}{\binom{n-2t}{i-t} \binom{n-2t+j+1}{j}} - \frac{\binom{i-t+j-1}{j-1} \binom{m-t+j}{i-t+j}^2}{\binom{n-2t+j+1}{i-t+j}}.$$

Here we note in the numerator of the first summand that

$$\binom{m-t}{i-t} \binom{m-t+j}{j} = \binom{m-t+j}{i-t+j} \binom{i-t+j}{j}.$$

and in the denominator that

$$\begin{aligned}
\binom{n-2t+j+1}{j} \binom{n-2t}{i-t} &= \binom{n-2t+j+1}{n-2t+1} \binom{n-2t}{i-t} \\
&= \frac{n-2t+j+1}{n-2t+1} \binom{n-2t+j}{n-2t} \binom{n-2t}{i-t} \\
&= \frac{n-2t+j+1}{n-2t+1} \binom{n-2t+j}{i-t+j} \binom{i-t+j}{j}.
\end{aligned}$$

Thus P_j in (14) is written as

$$\begin{aligned}
P_j &= \binom{n-t+j}{j+i-t} \left(\frac{n-2t+1}{n-2t+j+1} \frac{\binom{i-t+j}{j}}{\binom{n-2t+j}{i-t+j}} - \frac{\binom{i-t+j-1}{j-1}}{\binom{n-2t+j+1}{i-t+j}} \right) \\
&= \frac{\binom{m-t+j}{i-t+j}^2 \binom{i-t+j}{j}}{\binom{n-2t+j}{i-t+j}} \left(\frac{n-2t+1}{n-2t+j+1} - \frac{n-t-i+1}{n-2t+j+1} \frac{j}{i-t+j} \right)
\end{aligned}$$

$$= \frac{\binom{m-t+j}{i-t+j}^2 \binom{i-t+j}{j}}{\binom{n-2t+j}{i-t+j}} \cdot \frac{i-t}{i-t+j} = \frac{\binom{m-t+j}{i-t+j}^2 \binom{i-t+j-1}{j}}{\binom{n-2t+j}{i-t+j}}$$

Thus we have

$$E_i^{(t+1)} = \Gamma_i - \frac{\binom{m-t}{i-t}^2}{\binom{n-2t}{i-t}} \Gamma_i - \sum_{j=1}^t (-1)^j \frac{\binom{m-t+j}{i-t+j}^2 \binom{i-t+j-1}{j}}{\binom{n-2t+j}{i-t+j}} \Gamma_{i-j},$$

proving Lemma 7.

11. — LEMMA 8. *If we put*

$$F_i = \sum_{j=0}^i (-1)^j \frac{\binom{m-i+j}{j}^2}{\binom{n-2i+j+1}{j}} \Gamma_{i-j},$$

then we have that $F_i F_j = 0$ for $i \neq j$, and

$$F_i^2 = \binom{n-2i}{m-i} F_i.$$

PROOF. F_i is nothing but $E_i^{(i)}$. Thus, $\frac{F_i}{\binom{n-2i}{m-i}} = E_i$ ($i=0, 1, 2, \dots, m$)

are mutually orthogonal idempotents of $\mathfrak{A}_m$.

LEMMA 9. *The element E_i defined above is orthogonal to $\Gamma_0, \Gamma_1, \dots, \Gamma_{i-1}$.*

PROOF. A little bit more precise form of Lemma 8 is

$$\begin{aligned} F_0 &= \Gamma_0, \\ F_1 &= \Gamma_1 - \frac{m^2}{n} \Gamma_0, \\ F_2 &= \Gamma_2 - \frac{\binom{m-1}{1}^2}{\binom{n-2}{1}} \Gamma_1 + \frac{\binom{m}{2}^2}{\binom{n-1}{2}} \Gamma_0, \\ F_3 &= \Gamma_3 - \frac{\binom{m-2}{1}^2}{\binom{n-4}{1}} \Gamma_2 + \frac{\binom{m-1}{2}^2}{\binom{n-3}{2}} \Gamma_1 - \frac{\binom{m}{3}^2}{\binom{n-2}{3}} \Gamma_0, \\ &\dots\dots\dots \end{aligned}$$

Thus the matrix transforming $\Gamma_0, \Gamma_1, \dots, \Gamma_m$ to $F_0, F_1, \dots, F_m$ is of a triangular form, so Γ_i is a linear combination of $F_0, F_1, \dots, F_i$. Thus $F_j \Gamma_i = 0$ if $i < j$.

LEMMA 9. $E_0 + E_1 + \dots + E_i$ induces an identity transformation of the subspace $\Gamma_i V$. In particular

$$E_0 + E_1 + \dots + E_m = I$$

is the identity matrix.

PROOF. In view of Lemma 8, we have $E_0V + E_1V + \dots + E_iV = \Gamma_0V + \Gamma_1V + \dots + \Gamma_iV$. The last space is Γ_iV by Theorem 2, so we have

$$\Gamma_iV = E_0V + E_1V + \dots + E_iV.$$

Here the sum is a direct sum since E_j for $j=0, 1, \dots, i$ are mutually orthogonal idempotents.

LEMMA 10. $\text{rank } E_i = \binom{n}{i} - \binom{n}{i-1}$. for $i \geq 1$, $\text{rank } E_0 = 1$.

PROOF. We have $\text{rank } (E_0 + E_1 + \dots + E_i) = \text{rank } \Gamma_i = \binom{n}{i}$ by Theorem 2. Since $E_0 + \dots + E_{i-1}$ and E_i are mutually orthogonal idempotents we have that $\text{rank } E_i = \text{rank } (E_0 + \dots + E_i) - \text{rank } (E_0 + \dots + E_{i-1}) = \binom{n}{i} - \binom{n}{i-1}$.

Combining the above results we have

THEOREM 3. If we define

$$E_i = \frac{1}{\binom{n-2i}{m-i}} \sum_{j=0}^i (-1)^j \frac{\binom{m-i+j}{j}^2}{\binom{n-2i+j+1}{j}} \Gamma_{i-j}$$

for $i=0, 1, \dots, m$, then $E_0, E_1, \dots, E_m$ are mutually orthogonal primitive idempotents of the algebra $\mathfrak{A}_m$ and $E_0 + E_1 + \dots + E_m$ is the identity of $\mathfrak{A}_m$.

The rank of the $v \times v$ matrix E_i is $\binom{n}{i} - \binom{n}{i-1}$ for $i \geq 1$ and 1 for $i=0$.

12. — We conclude our investigation of the algebra $\mathfrak{A}_m$ with the following Lemma, which gives an expression of Γ_i in terms of the basic idempotents E_i .

LEMMA 11.

$$\Gamma_i = \sum_{j=0}^i \binom{m-j}{m-i} \binom{n-i-j}{m-i} E_j.$$

PROOF. We first note the following transformation of Theorem 3.

$$(15) \quad E_i = (-1)^i (n-2i+1) \sum_{k=0}^i \frac{(-1)^k}{n-i-k+1} \frac{\binom{m-k}{i-k}}{\binom{n-k-i}{m-k}} \Gamma_k.$$

Indeed we have from Lemma 8 that

$$E_i = \frac{1}{\binom{n-2i}{m-i}} \sum_{k=0}^i (-1)^{i-k} \frac{\binom{m-k}{i-k}^2}{\binom{n-i-k+1}{i-k}} \Gamma_k.$$

The coefficient of Γ_k is

$$\begin{aligned}
&= (-1)^{i-k} \frac{\binom{m-k}{i-k}^2}{\binom{n-2i}{m-i} \binom{n-i-k+1}{n-2i+1}} \\
&= (-1)^{i-k} \frac{n-2i+1}{n-i-k+1} \frac{\binom{m-k}{i-k}^2}{\binom{n-2i}{m-i} \binom{n-i-k}{n-2i}} \\
&= (-1)^{i-k} \frac{n-2i+1}{n-i-k+1} \frac{\binom{m-k}{i-k}^2}{\binom{n-i-k}{m-k} \binom{m-k}{i-k}} \\
&= (-1)^{i-k} \frac{n-2i+1}{n-i-k+1} \frac{\binom{m-k}{i-k}}{\binom{n-i-k}{m-k}}.
\end{aligned}$$

Now write (15) simply

$$E_i = \sum_{k=0}^i a_{ik} \Gamma_k,$$

with

$$a_{jk} = (-1)^{i-k} \frac{n-2i+1}{n-i-k+1} \frac{\binom{m-k}{i-k}}{\binom{n-i-k}{m-k}}.$$

In order to show that

$$\Gamma_i = \sum_{k=0}^i b_{ik} E_k$$

with

$$b_{ik} = \binom{m-k}{m-i} \binom{n-i-k}{m-i} = \binom{m-i-k}{m-i} \binom{m-k}{i-k},$$

we have only to verify that $\sum_{j=0}^i a_{ij} b_{jk} = \delta_{ik}$. Now, since both matrices are diagonal we may assume $i \geq k$. Moreover if $i=k$, then it is evident that $a_{ii} b_{ii} = 1$. So we may even assume $i > k$. Now, if $i > k$ then

$$a_{ij} b_{jk} = (-1)^{i-j} \frac{n-2i+1}{i-k} \frac{\binom{m-k}{m-i} \binom{i-k}{j-k} \binom{n-j-k}{n-i-j+1}}{\binom{n-m-k}{n-m-i}}$$

as is easily found. Thus we have

$$\sum_{j=k}^i a_{ij} b_{jk} = (-1)^i \frac{n-2i+1}{i-k} \frac{\binom{m-k}{m-i}}{\binom{n-m-k}{n-m-i}} \sum_{j=k}^i (-1)^j \binom{i-k}{j-k} \binom{n-j-k}{n-i-j+1}$$

the sum being equal to

$$(-1)^{n-i+1} \sum_{j=k}^i \binom{i-k}{j-k} \binom{-i+k}{n-i-j+1} = (-1)^{n-i+1} \binom{0}{n-i-k+1} = 0,$$

We have used the fact that $i+k \leq 2m < n+1$, which follows from our assumption $n \geq 2m$.

§ 3. Rational congruence of positive definite matrices

13. — Let $\mathfrak{P}_v$ the set of all symmetric positive definite rational matrices of order v . Two matrices A and B in $\mathfrak{P}_v$ are called rationally congruent if there is a nonsingular rational matrix U such that $B = U'AU$. This is an equivalence relation.

We write $A \sim B$ if A and B are rationally congruent. In this context the following fundamental theorem of Hasse is known.

A and B are rationally congruent if and only if firstly they have the same determinant except for a square factor and secondly the Minkowski-Hasse invariant

$$\psi_p(A) = \prod_{i=0}^{m-1} (D_i, -D_{i+1})_p$$

have the same value $\psi_p(A) = \psi_p(B)$, for any prime number p , where $D_0 = 1$, and D_i for $i \geq 1$ is the i -th principal minor determinant of A , and $(a, b)_p$ is the Hilbert norm residue symbol.

If the two nonzero rational numbers a, b differ only by a square factor, then the 1×1 matrices (a) and (b) are rationally congruent and conversely.

So we write $a \sim b$ if this is the case, i.e., if $(a) \sim (b)$. Because of the Hasse theorem we sometimes omit the subscript p for the Hilbert norm residue symbol, also we write simply $\psi(A)$ if p is understood to be known. Also, we do not specify the degree v in such relations and in such symbols, by adjoining another subscript to indicate the degree v .

We list several useful Lemmas on the Hasse-Minkowski invariants $\psi(A)$.

LEMMA 13. *If $A_1, A_2, \dots, A_n$ are positive definite rational and symmetric, then*

$$\psi \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_n \end{pmatrix} = \psi(A_1) \psi(A_2) \cdots \psi(A_n) \psi \begin{pmatrix} \det A_1 & & & \\ & \det A_2 & & \\ & & \ddots & \\ & & & \det A_n \end{pmatrix}.$$

LEMMA 14. If $a_1, \dots, a_n$ are positive rational numbers, then

$$\psi \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} = \prod_{i < j} (a_i, a_j).$$

LEMMA 15. If $a_1, \dots, a_n, b_1, \dots, b_n$ are positive rational numbers, then

$$\begin{aligned} \psi \begin{pmatrix} a_1 b_1 & & & \\ & a_2 b_2 & & \\ & & \ddots & \\ & & & a_n b_n \end{pmatrix} \\ = \psi \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \psi \begin{pmatrix} b_1 & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_n \end{pmatrix} \left(\prod_{i=1}^n a_i, \prod_{i=1}^n b_i \right) \prod_{i=1}^n (a_i, b_i). \end{aligned}$$

In particular if a is positive rational number and A is positive definite symmetric rational matrix of degree n then

$$\psi(aA) = (-1, a)^{\frac{n(n-1)}{2}} \psi(A)(a, \det A)^{n-1}.$$

14. — We need an explicit form for the determinant of the $v \times v$ matrices X contained in the algebra $\mathfrak{A}_m$. We recall that $\mathfrak{A}_m$ was generated the $m+1$ characteristic matrices $X_0, X_1, \dots, X_m$ of the m -subset association scheme, and similarly generated by the $m+1$ matrices $\Gamma_0, \Gamma_1, \dots, \Gamma_m$. We note first

LEMMA 16. If $X = \sum_{i=0}^m \lambda_i X_i$, then $X = \sum_{i=0}^m \Delta^i \lambda_0 \Gamma_i$ and conversely where Δ is the difference operator such that $\Delta f(x) = f(x+1) - f(x)$.

PROOF. It is seen from (3) that

$$X = \sum_{i=0}^m \lambda_i \sum_{j=i}^m (-1)^{i+j} \binom{j}{i} \Gamma_j = \sum_{j=0}^m \left(\sum_{i=0}^j (-1)^{j-i} \binom{j}{i} \lambda_i \right) \Gamma_j = \sum_{j=0}^m \Delta^j \lambda_0 \Gamma_j.$$

THEOREM 4. If $X = \sum_{i=0}^m \lambda_i X_i$, then the determinant of the $v \times v$ matrix X is given by

$$\det X = \prod_{i=0}^m \left(\sum_{j=i}^m \Delta^j \lambda_0 \binom{m-i}{m-j} \binom{n-i-j}{m-j} \right)^{\binom{n}{i} - \binom{n-1}{i-1}}.$$

PROOF. We observe from Lemma 11 and 12 that

$$(16) \quad X = \sum_{i=0}^m \left(\sum_{j=0}^m \Delta^j \lambda_0 \binom{m-i}{m-j} \binom{n-i-j}{m-j} \right) E_i,$$

with the idempotents E_i of Theorem 3.

Now, the underlying vector space V is decomposed into $m+1$ linear subspaces $E_i V$ of dimensions $n_i = \binom{n}{i} - \binom{n}{i-1}$, as is seen from Lemmas 9 and 10. If we choose a basis $b_1^{(i)}, \dots, b_{n_i}^{(i)}$ of the subspace $E_i V$ for $i=0, 1, \dots, m$, then the whole set of all these $n_0 + \dots + n_m = \binom{n}{m}$ vectors $b_{\nu_i}^{(i)}$ for $\nu_i=1, 2, \dots, n_i$, $i=0, 1, \dots, m$ form a base of V . Consider $b_{\nu_i}^{(i)}$ as column vectors and let U be the $v \times v$ matrix $(b_1^{(0)}, b_1^{(1)}, \dots, b_{n_1}^{(1)}, b_1^{(m)}, \dots, b_{n_m}^{(m)})$. Then since

$$E_i b_{\nu_j}^{(j)} = \delta_{i,j} b_{\nu_j}^{(j)}$$

with the Kronecker delta $\delta_{i,j}=1$ or $=0$ according as $i=j$ or not, we seen that

$$(17) \quad XU = U \begin{pmatrix} \rho_0 I_{n_0} & & & \\ & \rho_1 I_{n_1} & & \\ & & \ddots & \\ & & & \rho_m I_{n_m} \end{pmatrix}.$$

where $\rho_i = \sum_{j=i}^m \lambda_j \binom{m-i}{m-j} \binom{n-i-j}{m-j}$, and I_r is the $r \times r$ unit matrix. Therefore $\det X = \prod_{i=0}^m \rho_i^{n_i}$, which proves our Theorem.

15. — In the above Proof we note that the vectors $b_{\nu_i}^{(i)}$ and $b_{\nu_j}^{(j)}$ are orthogonal to each other provided that $i \neq j$. Indeed, since the matrices E_i are symmetric as elements of $\mathfrak{A}_m$, and the inner product $b_i' b_j$ for $b_i \in E_i V$, $b_j \in E_j V$ satisfies that

$$b_i' b_j = (E_i b_i)' (E_j b_j) = b_i' E_i' E_j b_j = b_i' E_i E_j b_j = 0.$$

This means that the Gramian matrix $U'U$ of the base $b_1^{(0)}, b_1^{(1)}, \dots, b_{n_1}^{(1)}, \dots, b_1^{(m)}, \dots, b_{n_m}^{(m)}$ is of the form

$$(18) \quad U'U = \begin{pmatrix} Y_0 & & & \\ & Y_1 & & \\ & & \ddots & \\ & & & Y_m \end{pmatrix},$$

where Y_i is the $n_i \times n_i$ Gramian matrix of the base $b_1^{(i)}, \dots, b_{n_i}^{(i)}$. Therefore if X is positive definite then we have

$$X \sim U'XU = U'U \begin{pmatrix} \rho_0 I_{n_0} & & & \\ & \rho_1 I_{n_1} & & \\ & & \ddots & \\ & & & \rho_m I_{n_m} \end{pmatrix},$$

$$\begin{aligned}
&= \begin{pmatrix} Y_0 & & & \\ & Y_1 & & \\ & & \ddots & \\ & & & Y_m \end{pmatrix} \begin{pmatrix} \rho_0 I_{n_0} & & & \\ & \rho_1 I_{n_1} & & \\ & & \ddots & \\ & & & \rho_m I_{n_m} \end{pmatrix} \\
&= \begin{pmatrix} \rho_0 Y_0 & & & \\ & \rho_1 Y_1 & & \\ & & \ddots & \\ & & & \rho_m Y_m \end{pmatrix},
\end{aligned}$$

by means of (17) and (18). Note that ρ_i is necessarily positive and that Y_i is positive definite symmetric. This together with Lemma 13, 14, 15 prove the following.

THEOREM 5. *If $X = \sum_{i=0}^m \lambda_i X_i$, with rational numbers λ_i is positive definite, it is necessary that*

$$P_i = \sum_{j=i}^m A^j \lambda_0 \binom{m-i}{m-j} \binom{n-i-j}{m-j}$$

is positive for $i=0, 1, \dots, m$, and the Hasse-Minkowski invariant $\phi(X)$ is given by

$$\phi(X) = \prod_{i=0}^m (-1, \rho_i)^{\frac{n(n-1)}{2}} \prod_{0 \leq i < j \leq m} (\rho_i, \rho_j)^{n_i n_j} \prod_{i=0}^m (\rho_i, \det Y_i)$$

with $n_i = \binom{n}{i} - \binom{n}{i-1}$.

PROOF. We have

$$\begin{aligned}
\phi(X) &= \phi \begin{pmatrix} \rho_0 Y_0 & & & \\ & \rho_1 Y_1 & & \\ & & \ddots & \\ & & & \rho_m Y_m \end{pmatrix} = \prod_{i=0}^m \phi(\rho_i Y_i) \phi \begin{pmatrix} \rho_0^{n_0} \det Y_0 & & & \\ & \rho_1^{n_1} \det Y_1 & & \\ & & \ddots & \\ & & & \rho_m^{n_m} \det Y_m \end{pmatrix} \\
&= \prod_{i=0}^m (-1, \rho_i)^{\frac{n(n-1)}{2}} \prod_{i=0}^m \phi(Y_i) \prod_{i=0}^m (\rho_i, \det Y_i)^{n_i-1} \phi \begin{pmatrix} \rho_0^{n_0} & & & \\ & \rho_1^{n_1} & & \\ & & \ddots & \\ & & & \rho_m^{n_m} \end{pmatrix} \\
&\quad \times \phi \begin{pmatrix} \det Y_0 & & & \\ & \det Y_1 & & \\ & & \ddots & \\ & & & \det Y_m \end{pmatrix} \left(\prod_{i=0}^m \rho_i^{n_i}, \prod_{i=0}^m \det Y_i \right) \prod_{i=0}^m (\rho_i \det Y_i)^{n_i},
\end{aligned}$$

by means of Lemmas 13, 14 and 15. On the other hand we have

$$\phi(I) = \phi(U'U) = \phi \begin{pmatrix} Y_0 & & \\ & Y_1 & \\ & & \ddots \\ & & & Y_m \end{pmatrix} = 1, \text{ since obviously } \phi(I) = 1.$$

Note also that $1 \sim \det U'U = \prod_{i=0}^m \det Y_i$. Here we have from Lemma 13 that

$$1 = \phi \begin{pmatrix} Y_0 & & \\ & Y_1 & \\ & & \ddots \\ & & & Y_m \end{pmatrix} = \prod_{i=0}^m \phi(Y_i) \phi \begin{pmatrix} \det Y_0 & & \\ & \det Y_1 & \\ & & \ddots \\ & & & \det Y_m \end{pmatrix}.$$

Therefore, by combining this with the previous formula for $\phi(X)$ we concluded that

$$\phi(X) = \prod_{i=0}^m (-1, \rho_i)^{\frac{n(n-1)}{2}} \prod_{0 \leq i < j \leq m} (\rho_i^* \rho_j^*) \prod_{i=0}^m (\rho_i, \det Y_i).$$

16. — Next our task is to find the Gramian determinants $\det Y_i$ up to square factors. The class of the Gramian determinant is determined by the linear subspace generated by the linearly independent vectors involved, so $\det Y_i$ is the Gramian determinant of the linear subspace $E_i V$ of V .

We determine the Gramian determinant of the linear subspace $I_i V$ by the following consideration.

It is known by Theorem 2 that $I_i V$ is spanned by the $\binom{n}{i}$ vectors $G_\alpha = \alpha \varphi_{m-i}(\mathcal{Q}/\alpha)$ for $\alpha \in S_i$, the set of i -subsets of $\mathcal{Q}$. We assert that the inner product

$$(18) \quad G_\alpha \cdot G_\beta = \binom{n-2i+\nu}{m-2i+\nu} \text{ with } \nu = |\alpha \triangleright \beta|$$

for two elements α, β of S_i . Indeed, $G_\alpha = \sum_{\tau \supset \alpha} \tau$, $G_\beta = \sum_{\tau \supset \beta} \tau$, so that $G_\alpha \cdot G_\beta$ is the number of m -subsets τ such that $\tau \supset \alpha\beta$. Note that $|\alpha\beta| = 2i - \nu$. Thus $\tau = \alpha\beta\rho$ with $\rho \subset \mathcal{Q}/(\alpha\beta)$, $|\rho| = m - 2i + \nu$, $|\mathcal{Q}/(\alpha\beta)| = n - 2i + \nu$. Therefore there are exactly $\binom{n-2i+\nu}{m-2i+\nu}$ m -subsets τ in S_m satisfying $\tau \supset \alpha\beta$.

The relation (19) implies that the inner product $G_\alpha \cdot G_\beta$ is determined by the "association number" ν of α and β in the i -subset association scheme defined over the set S_i . The requirement $n \geq 2i$ is satisfied. If we denote the characteristic matrix of the ν -th associates in the i -subset association scheme

by $\tilde{X}_\nu$, Then the $\binom{n}{i} \times \binom{n}{i}$ Gramian matrix $Z_i = \|G_\alpha \cdot G_\beta\|$ is written as

$$Z_i = \sum_{\nu=0}^i \binom{n-2i+\nu}{m-2i+\nu} \tilde{X}_\nu.$$

And $\det Z_i$ is given by Theorem 4. Thus $\det Z_i = \prod_{j=0}^i \tilde{\rho}_j^{n_j}$, where

$$\tilde{\rho}_j = \sum_{u=0}^i A^u \tilde{\lambda}_0 \binom{i-j}{i-u} \binom{n-j-u}{i-u}, \quad \tilde{\lambda}_\nu = \binom{n-2i+\nu}{m-2i+\nu}.$$

Here we have

$$\begin{aligned} A^j \tilde{\lambda}_0 &= (-1)^j \sum_{u=0}^i (-1)^u \binom{j}{u} \binom{n-2i+u}{m-2i+u} = (-1)^j \sum_{u=0}^j \binom{j}{j-u} (-1)^m \binom{-n+m-1}{m-2i+u} \\ &= (-1)^{j+m} \binom{-n+m+j-1}{m-2i+j} = \binom{n-2i}{m-2i+j}, \end{aligned}$$

hence

$$\begin{aligned} \tilde{\rho}_j &= \sum_{u=0}^i \binom{n-2i}{m-2i+u} \binom{i-j}{i-u} \binom{n-j-u}{n-i-j} \\ &= \binom{m-j}{i-j} \binom{n-i-j}{m-i} = \binom{m-j}{m-i} \binom{n-i-j}{m-i}, \end{aligned}$$

by using Lemma 3. Thus we have seen that the Gramian determinant of the subspace $I_i V$ is given by

$$(19) \quad \det Z_i = \prod_{j=0}^i \left(\binom{m-j}{m-i} \binom{n-i-j}{m-i} \right)^{n_j}$$

By Theorem 2, the subspace $I_i V$ is the direct sum of $E_0 V, E_1 V, \dots, E_i V$. So, the Gramian determinant $\det Z_i$ is equal to the product of the Gramian determinants of $E_0 V, E_1 V, \dots, E_i V$. Thus we have $\det Z_i \sim \prod_{j=0}^i \det Y_j$, and from (19) we see that

$$\begin{aligned} \det Y_i &\sim \det Z_i / \det Z_{i-1} \\ &\sim \binom{n-2i}{m-i}^{n_i} \prod_{j=0}^{i-1} \left(\binom{m-j}{m-i} \binom{m-j}{m-i+1} \binom{n-i-j}{m-i} \binom{n-i-j+1}{m-i+1} \right)^{n_j} \\ &\sim \binom{n-2i}{m-i}^{n_i} \prod_{j=0}^{i-1} ((i-j)(n-i-j+1))^{n_j}. \end{aligned}$$

Putting this in Theorem 5 we have immediately

THEOREM 6. *If $X = \sum_{i=0}^m \lambda_i X_i$, λ_i being rational is positive definite, then the Hasse-Minkowski invariant $\phi(X)$ is given by*

$$\begin{aligned} \phi(X) &= \prod_{i=0}^m (-1, \rho_i)^{\frac{n(n-1)}{2}} \prod_{0 \leq i < j \leq m} (\rho_i, \rho_j)^{n_i n_j} \\ &\times \prod_{i=0}^m \left(\rho_i, \binom{n-2i}{m-i}^{n_i} \prod_{j=0}^{i-1} ((i-j)(n-i-j+1))^{n_j} \right), \end{aligned}$$

where ρ_i is the eigenvalue of X corresponding to the eigenspace $E_i V$ and $n_i = \binom{n}{i} - \binom{n}{i-1}$.

§ 4. Partially balanced incomplete block designs with the m -subset association scheme.

17. — Let S_m be defined as before. Let D be a system of subsets $B_1, \dots, B_b$ of S_m such that each B_ν contains the same number k of elements, each element α of S_m is contained in the same number r of the subsets B_ν , and furthermore, for any two element α, β of S_m there are exactly λ_i subsets B_ν containing both α and β , where i is the “association number”, i.e., i is the integer such that α and β are i -th associates and λ_i depends only on i . Such a system D is called a *partially balanced incomplete block design with an m -subset association scheme over the set Ω* .

Let N be the incidence matrix of D , defined as follows. N is a $b \times v$ matrix where the row index runs over the set $\{1, 2, \dots, b\}$, the column index runs over the set S_m , and the (ν, α) -entry is 1 or 0 according as the subset B_ν contains α or not.

If we denote the $s \times 1$ matrix with all its components equal to 1 by J_s , then N satisfies the relations

$$(19) \quad \begin{aligned} NJ_v &= kJ_v, \quad N'J_b = rJ_b, \\ N'N &= \sum_{i=0}^m \lambda_i X_i, \end{aligned}$$

where X_i is the characteristic matrix of the i -th association defined over the set S_m .

We consider the special case where $b=v$, $k=r$, and N is a nonsingular matrix. In this case $N'N=X$ is positive definite and rationally congruent to I , the unit matrix. In this connection we note that the vector $J_v = G_1 = \varphi_m(\mathcal{Q})$ in our previous notation (cf. Introduction), and $\varphi_m(\mathcal{Q}) = G_1$ spans the eigenspace $E_0 V$ of X , corresponding to the eigenvalue ρ_0 . However, the relation (19) shows that $\varphi_m(\mathcal{Q}) = J_v$ is an eigenvector of both N and N' , corresponding to the eigenvalue r . Thus $\varphi_m(\mathcal{Q}) = J_v$ is an eigenvector of $X = N'N$ corresponding to the eigenvalue r^2 . This means that $\rho_0 = r^2$. Since X is nonsingular symmetric positive definite and is rationally congruent to I , we have

$$\prod_{i=0}^m \rho_i^{n_i} \sim 1$$

and $\phi_p(X)=1$ for all prime number p . We have seen $\rho_0 \sim 1$ above, so the conditions

$$\prod_{i=1}^m \rho_i^{n_i} \sim 1, \quad \phi_p(X)=1$$

are necessary conditions by Hasse's Theorem.

Theorem 6 implies that

$$\prod_{i=1}^m (-1, \rho_i)^{\frac{n_i(n_i-1)}{2}} \prod_{1 \leq i < j \leq m} (\rho_i, \rho_j)^{n_i n_j} \prod_{i=1}^m \left(\rho_i, \binom{n-2i}{m-i}^{n_i} \prod_{j=1}^{i-1} ((i-j)(n-i-j+1))^{n_i} \right) = 1$$

for all prime p . We have finally proved

THEOREM 7. *If there exists a symmetric nonsingular partially balanced incomplete block design in $\binom{n}{m}$ variates with the m -subset association scheme, such that any two variates appear together in exactly λ_i blocks where i is the association number of the two variates, then the conditions*

$$\begin{aligned} & \rho_i > 0, \\ & \prod_{i=1}^m (-1, \rho_i)^{\frac{n_i(n_i-1)}{2}} \prod_{1 \leq i < j \leq m} (\rho_i, \rho_j)^{n_i n_j} \prod_{i=1}^m \left(\rho_i, \binom{n-2i}{m-i}^{n_i} \prod_{j=1}^{i-1} ((i-j)(n-i-j+1))^{n_i} \right) \\ & = 1, \text{ for all primes } p \text{ are necessary, where} \end{aligned}$$

$$\rho_i = \sum_{j=i}^m \Delta^j \lambda_0 \binom{m-i}{m-j} \binom{n-i-j}{m-j},$$

$$n_i = \binom{n}{i} - \binom{n}{i-1}.$$

In conclusion the author wishes to point out that he did not succeed in finding a suitable explicit orthogonal basis for the eigenspaces $E_i V$ in Theorem 3, which may greatly simplify our results.

Reference

- [1] J. OGAWA, *A necessary condition for existence of regular and symmetrical experimental designs of triangular type, with partially balanced incomplete blocks*, Ann. Math. Stat., vol. 30 (1959), pp. 1063-1071.