2. STRENGTHENING THE FOUNDATIONS

§2.1. The Direct Sum of Matrices

A square matrix written in the form $\left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right)$ where A, D are square, is said to be **partitioned**. If two matrices are partitioned in the same way their sum and product can be obtained by treating them as 2×2 matrices whose components are matrices.

$$\left(\begin{array}{c|c} A_1 & B_1 \\ \hline C_1 & D_1 \end{array}\right) + \left(\begin{array}{c|c} A_2 & B_2 \\ \hline C_2 & D_2 \end{array}\right) = \left(\begin{array}{c|c} A_1 + A_2 & B_1 + B_2 \\ \hline C_1 + C_2 & D_1 + D_2 \end{array}\right) \text{ and}$$

$$\left(\begin{array}{c|c} A_1 & B_1 \\ \hline C_1 & D_1 \end{array}\right)\left(\begin{array}{c|c} A_2 & B_2 \\ \hline C_2 & D_2 \end{array}\right) = \left(\begin{array}{c|c} A_1A_2 + B_1C_2 & A_1B_2 + B_1D_2 \\ \hline C_1A_2 + D_1C_2 & C_1B_2 + D_1D_2 \end{array}\right).$$

This can be extended to more than two partitions of the rows and columns.

The **direct sum** of two matrices is obtained by writing them diagonally and filling up the remaining components with zeros. In symbols: $A \oplus B = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$.

If A is $m \times m$ and B is $n \times n$ then $A \oplus B$ is $(m + n) \times (m + n)$.

If A, B are invertible, $(A \oplus B)^{-1} = A^{-1} \oplus B^{-1}$.

It is easy to show that $\chi_{A\oplus B}(\lambda) = \chi_A(\lambda).\chi_B(\lambda)$ and so $tr(A \oplus B) = tr(A) + tr(B)$ and $|A \oplus B| = |A|.|B|$. The eigenvalues of $A\oplus B$ are the eigenvalues of A together with the eigenvalues of B.

Example 1: If $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ and $B = \begin{pmatrix} 10 & 20 \\ 30 & 40 \end{pmatrix}$ then $A \oplus B = \begin{pmatrix} 1 & 2 & 3 & 0 & 0 \\ 4 & 5 & 6 & 0 & 0 \\ 7 & 8 & 9 & 0 & 0 \\ 0 & 0 & 0 & 10 & 20 \\ 0 & 0 & 0 & 30 & 40 \end{pmatrix}$.

§2.2. The Tensor Product of Matrices

If $A = (a_{ij})$ is $m \times n$ and $B = (b_{ij})$ is $r \times s$, the **tensor product** of A and B is the $mr \times ns$ matrix $A \otimes B = (c_{ij})$ where $c_{(i\text{-}1)n+s,\,(j\text{-}1)n+t} = a_{ij}b_{st}$.

We can write it in partitioned form as $A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B... \\ a_{21}B & a_{22}B... \\ ... & ... \end{pmatrix}$.

This makes it much easier to understand!

Example 2: If $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $A \oplus B = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$ and $A \otimes B = \begin{pmatrix} a & b & 2a & 2b \\ c & d & 2c & 2d \\ 3a & 3b & 4a & 4b \\ 3c & 3d & 4c & 4d \end{pmatrix}$

Theorem 1: Assuming the sizes are compatible**:**
(1) $AB \otimes CD = (A \otimes C)(B \otimes D)$
(2) $\oplus$ and $\otimes$ are associative
(3) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$
(4) $\mathrm{tr}(A \otimes B) = \mathrm{tr}A \times \mathrm{tr}B$.
Proof:

§ 2.3. Algebraic Integers

You need to know the familiar divisibility concepts and facts about integers, such as prime numbers and greatest common divisors. In particular you need to know that the greatest common divisor of integers *a*, *b*, or GCD(*a*, *b*) for short, can be expressed in the form *ah* + *bk* for some integers *h*, *k*. You also need to know something about algebraic integers. These are not quite the same as algebraic numbers. Here's a short account of them.

An **algebraic integer** is a complex number that is a zero of a monic polynomial with integer coefficients. If we allow the coefficients to be rational the definition becomes that of an algebraic number.

Example 1: $\frac{-1+\sqrt{5}}{2}$ is an algebraic integer but $\frac{-2+\sqrt{5}}{2}$ is an algebraic number, but not an algebraic integer. This is because $\frac{-1+\sqrt{5}}{2}$ is a zero of the monic integer polynomial

$x^2 + x - 1$. But if $x = \frac{-2+\sqrt{5}}{2}$ then $x^2 + 2x - ¼ = 0$, showing that x is an algebraic number, but clearly it isn't an algebraic number. Roots of unity, such as $e^{2\pi i/5}$, are clearly algebraic integers.

Theorem 1: A complex number is an algebraic integer if and only if it is an eigenvalue of an integer matrix.

Proof: If α is a non-zero eigenvalue of the integer matrix A it's a zero of the characteristic polynomial of A. The coefficients of this polynomial are sums and differences of products of the coefficients of A and hence are integers. Moreover the leading coefficient of a characteristic polynomial is 1. So, such eigenvalues are algebraic integers.

Now suppose that α is a zero of the integer polynomial $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$.

Consider the matrix:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ -a_0 & -a_1 & -a_2 & -a_3 & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix}$$ and the vector $\mathbf{v}$ $= \begin{pmatrix} 1 \\ \alpha \\ \dots \\ \alpha^{n-1} \end{pmatrix}$.

Then $A\mathbf{v} = \alpha\mathbf{v}$ and so α is an eigenvalue of the integer matrix A. ✋☺

Theorem 2: $\mathbb{Q} \cap \mathbb{Z}^* = \mathbb{Z}$.
Proof: Clearly $\mathbb{Z} \leq \mathbb{Q} \cap \mathbb{Z}^*$.

Now let $\alpha \in \mathbb{Q} \cap \mathbb{Z}^*$ and suppose $\alpha = \frac{r}{s}$ where r, s are coprime integers.
For some $a_0, \dots a_{n-1} \in \mathbb{Z}$, $(r/s)^n + a_{n-1}(r/s)^{n-1} \dots + a_1(r/s) + a_0 = 0$ whence
$r^n + a_{n-1}r^{n-1}s + \dots + a_1rs^{n-1} + a_0s^n = 0$ and so $s \mid r^n$.
Since GCD(s, r) = 1, $s = 1$ and so $\alpha \in \mathbb{Z}$. ✋☺

The set of multiples of the complex number λ is denoted by $\mathbb{Z}\lambda$ and the set of all integer linear combinations of the complex numbers $\lambda_1, \lambda_2, \dots, \lambda_n$ is denoted by:
$\mathbb{Z}\lambda_1 + \dots + \mathbb{Z}\lambda_n$.

Theorem 3: $\mathbb{Z}^*$ is a ring.

Proof: We first show that if $R = \mathbb{Z}\lambda_1 + \ldots + \mathbb{Z}\lambda_n$ is a ring then each $\lambda_k \in \mathbb{Z}^*$.

Suppose R is a ring. Then for each i, k the product $\lambda_i\lambda_k \in R$ and hence is an integral linear combination of the λ_i. Hence $\lambda_i\lambda_k = \sum_j a_{ijk}\lambda_j$ for some $a_{ijk} \in \mathbb{Z}$.

So if $A_k = (a_{ijk})$ and $\mathbf{v} = (\lambda_i)$ then $A_k\mathbf{v} = \lambda_k\mathbf{v}$. Since A is an integer matrix, each λ_k is an algebraic integer.

Now let $\alpha, \beta \in \mathbb{Z}^*$ where $\alpha^n \in \mathbb{Z}\alpha^{n-1} + \ldots + \mathbb{Z}$ and $\beta^m \in \mathbb{Z}\beta^{m-1} + \ldots + \mathbb{Z}$.

Then $\mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{n-1} + \mathbb{Z}\alpha\beta + \ldots + \mathbb{Z}\alpha^{n-1}\beta^{m-1}$ is a ring.

Since it contains $\alpha + \beta$ and $\alpha - \beta$.

$R = \mathbb{Z} + \mathbb{Z}\alpha + \ldots + \mathbb{Z}\alpha^{n-1} + \mathbb{Z}\alpha\beta + \ldots + \mathbb{Z}\alpha^{n-1}\beta^{m-1} + \mathbb{Z}(\alpha + \beta) + \mathbb{Z}(\alpha - \beta)$.

Hence $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$ are algebraic integers. ✋☺

§2.4. Babylonian Equations

If we want to investigate all the character tables of a given size we need to find all groups with a given number of conjugacy classes. We shall see that there are only finitely many possible orders for a group with k conjugacy classes, and hence only finitely many $k \times k$ character tables for any k. For small values of k it is possible to catalogue them.

The **class equation** of a finite group is:

$|G| = n_1 + n_2 + \ldots n_k$

where the n_i's are the sizes of the conjugacy classes and $n_1 \leq n_2 \leq \ldots \leq n_k$.
When there are c classes of a given size n, we sometimes write $n*c$ instead of $n + n + \ldots + n$.

Example 1:
The class equation of S_4 is $24 = 1 + 3 + 6*2 + 8$ and for D_{16} it is $16 = 1*2 + 2*3 + 4*2$.

Often the class equation completely characterises the group, but there are some groups that share the same class equation.

Example 2:
Both $D_8 = \langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle$ and $Q_8 = \langle A, B \mid A^4 = 1, B^2 = A^2, BA = A^{-1}B \rangle$ have the class equation $8 = 1*2 + 2*3$.

Now each n_i is the index of the corresponding centraliser in G and so divides $|G|$. If we divide a class equation by $|G|$ we get an equation of the form:

$$1 = \frac{1}{m_1} + \ldots + \frac{1}{m_k}$$

where each m_i is a positive integer.

A **Babylonian equation** is an equation of the form:

$$1 = \frac{1}{m_1} + \ldots + \frac{1}{m_k}$$

where each $m_i \in \mathbb{Z}^+$ and $m_1 \leq m_2 \leq .. \leq m_k$. The **length** of such an equation is k.

Example 3: The class equation for S_4 is $24 = 1 + 3 + 6 + 6 + 8$ which gives the Babylonian equation: $1 = \frac{1}{3} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{24}$.

Theorem 1: There are only finitely many Babylonian equations of a given length.

Proof: For a Babylonian equation of length k: $1 = \frac{1}{m_1} + \ldots + \frac{1}{m_k}$ suppose we have proved that there are finitely many choices for $m_1, m_2, \ldots m_i$.

Let $i < k$ and let $M = 1 - \frac{1}{m_1} - \frac{1}{m_2} - \ldots - \frac{1}{m_i}$. Then $\frac{1}{m_{i+1}} + \ldots + \frac{1}{m_k} = M$ and we have finitely many choices for M.

Since $\frac{1}{m_{i+1}} \geq \ldots \geq \frac{1}{m_k}$ we have $M \leq \frac{k-i}{m_{i+1}}$.

So $\frac{1}{1-M} < m_{i+1} \leq \frac{k-i}{M}$, giving only finitely many choices for m_{i+1}.

Corollary: There are only finitely many class equations of a given length and hence only finitely many character tables of a given size.

Example 3: Babylonian equations of length ≤ 4:

Length 1	**Length 2**
$1 = 1$	$1 = \frac{1}{2} + \frac{1}{2}$

Length 3		
$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$	$1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{4}$	$1 = \frac{1}{3} +$

Length 4		
$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{42}$	$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{8} + \frac{1}{24}$	$1 = \frac{1}{2} +$
$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{10} + \frac{1}{15}$	$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{12} + \frac{1}{12}$	$1 = \frac{1}{2} +$
$1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{12}$	$1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8}$	$1 = \frac{1}{2} +$
$1 = \frac{1}{2} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6}$	$1 = \frac{1}{3} + \frac{1}{3} + \frac{1}{4} + \frac{1}{12}$	$1 = \frac{1}{3} +$
$1 = \frac{1}{3} + \frac{1}{4} + \frac{1}{4} + \frac{1}{6}$	$1 = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}$	

Example 4: Class equations of length ≤ 3:
1 = 1 corresponds to the trivial group;
$1 = \frac{1}{2} + \frac{1}{2}$ gives the class equation 2 = 1 + 1 which corresponds to C_2 only;.
$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$ gives the class equation 6 = 1 + 2 + 3 which corresponds to S_3 only;
$1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{4}$ gives the class equation 4 = 1 + 1 + 2 which doesn't arise in either of the two groups of order 4;
$1 = \frac{1}{3} + \frac{1}{3} + \frac{1}{3}$ gives the class equation 3 = 1 + 1 + 1 which corresponds to C_3 only.

§2.5. Some Elementary Tests for Potential Class Equations

Much of the material in this chapter arose in the 1980s from my teaching a course on group theory.

It's a routine exercise to generate all Babylonian equations of a given length and to obtain a list of possible class equations. The problem is to exclude those that do not arise. A subsequent problem is to identify the groups that give rise to the potential class equations.

We'll focus on the first problem by investigating properties that class equations must satisfy. Each such property will give rise to a test. Then when we have a potential class equation we put it through the battery of

tests. Only if it survives do we go in search for possible groups. If, after a reasonable amount of effort, we can find no such group we might then look for another reason to exclude that class equation. The set of tests we shall develop will catch the vast majority of false class equations – quite probably no such set of tests will ever catch them all, for as the number of conjugacy classes increases there appear to be more and more subtle reasons that exclude a given class equation.

Theorem 2 (Z Test): Suppose $|G| = N$ and $|Z(G)| = m$.
If the class equation for G is $N = 1*m + n_{m+1} + n_{m+2} + \ldots + n_m$ where each $n_{m+1} > 1$ then m must properly divide N/n_i for each i.
Proof: Suppose $g \notin Z(G)$. Then $|C_G(g)| = N/n_i$ for some $i > m$.
Since $g \in C_G(g)$, $Z(G) < C_G(g)$ and so m properly divides N/n_i. ✋☺

Example 5: $84 = 1 + 1 + 12 + 21 + 21 + 28$ is not a class equation.

Theorem 3 (*pq* Test): Suppose $N = 1 + n_2 + n_3 + \ldots + n_k$ is the class equations for a group G and, for some $i > 1$, $N/n_i = p^a q^b$, where p, q are distinct primes and $a, b \geq 1$.
Then the number of j for which pq divides N/n_j is at least 4.
Proof: We need to find four conjugacy classes where the orders of the centralisers are all divisible by pq.

Suppose $|C_G(g)| = p^a q^b$ where $g \neq 1$ and suppose that g has order d.
Then either p or q divides d.
Suppose, without loss of generality,p divides d, in which case some power of g has order p.
By Cauchy's theorem $C_G(g)$ contains an element of order q, which commutes with that power of order p and so G has an element of order pq and so elements of order 1, p, q and pq whose centralisers have orders divisible by pq.
As the orders are different they must belong to distinct conjugacy classes.

Example 6: 120 = 1 + 5 + 20 + 24 + 30 + 40 is not a class equation because if it was the respective centralisers would have orders 120, 24, 6, 5, 4 and 3.

Theorem 4 (pN Test): Suppose p is prime and $p\mathrm{N} = 1 + n_2 + n_3 + \ldots + n_{k-t} + \mathrm{N}*t$ is the class equation for a group G where $\mathrm{N} > 1$, $t \geq 1$ and $n_{k-t} < \mathrm{N}$
(that is, G has precisely t classes of size N).
Then: (i) $t \mid p - 1$ and

(ii) $\mathrm{N} \equiv \frac{p-1}{t} \pmod{p}$.

Proof: Let Γ be a class of size N and let $g \in \Gamma$. Then $|C_G(g)| = p$ and so $C_G(g) = \langle g \rangle$.
If $g^s \neq 1$ then $C_G(g^s) = \langle g \rangle$ and so g^s lies in a conjugacy class of size N.

Let Ω be any conjugacy class of size N and let $\langle g \rangle$ act on it by conjugation.
The orbits have sizes 1 or p. But orbits of size 1 correspond to non-trivial powers of g, and there are $p - 1$ of these altogether, so the number of orbits of size 1 in Γ' is at most $p - 1$.
Now if $N = np + r$ where $0 \leq r < p$ there must be exactly r orbits of size 1 in Ω.
So there are exactly r powers of g in each of the t conjugacy classes of size N and hence

$p - 1 = rt$. Hence $N \equiv r = \frac{p-1}{t} \pmod{p}$.

Example 7: 216 = 1 + 8 + 27 + 54 + 54 + 72 is not a class equation.
Here $p = 3$, $t = 1$ and $N = 72 \equiv 0 \pmod 3$.

§2.6. The 2N Test

The largest possible size of a conjugacy class, for a non-trivial group of order M, is M/2. Of course there can only be one of these and its elements must have order 2.In fact the class equation of such a group is completely determined by this property.

Theorem 5 (2N test): Let |G| = 2N and let Γ be a conjugacy class of size N.
Then N is odd and the class equation for G is $2N = 1 + 2 + 2 + \ldots + 2 + N = 1 + 2*\left(\frac{N-1}{2}\right)$.

Proof:

(1) The elements of Γ have order 2 and commute only with 1 and themselves:

This is because the centralisers of these elements have order 2N/N.

(2) H = G – Γ is a normal subgroup of G:

H clearly contains 1 and is closed under inverses. Let x, y be distinct elements of Γ.

If $xy \in \Gamma$ then $(xy)^2 = x^2y^2 = 1$, so $xy = yx$ and hence $y \in C_G(x)$, a contradiction. Hence H is a subgroup of G and, being a subgroup of index 2, it is a normal subgroup.

	H	**Γ**
H	H	K
Γ	Γ	H

(3) H is abelian:

Let $h \in$ H and $k \in \Gamma$. If $hk \in$ H then $k \in$ H. Hence $hk \in \Gamma$ and so $(hk)^2 = 1$.

Thus $k^{-1}hk = h^{-1}$ for all $h \in$ H and so $h \to h^{-1}$ is an automorphism of H.

If $h_1, h_2 \in$ H then $(h_1h_2)^{-1} = h_1^{-1}h_2^{-1} = (h_2h_1)^{-1}$ and so $h_1h_2 = h_2h_1$.

(4) N = |H| is odd.
If |H| is even then H would contain an element h of order 2.
Since $h = h^{-1}$ it follows that h commutes with k, a contradiction.

(5) The class equation for G is $2N = 1 + 2 + 2 + \ldots + 2 + N$.
Since $k^{-1}hk = h^{-1}$ for all $k \in$ K and all non-trivial $h \in H$, the conjugacy classes, apart from {1} and Γ, are all of the form $\{h, h^{-1}\}$.

(6) N is odd.

Example 8: 18 = 1 + 2 + 6 + 9 is not a class equation.