17. CLASS EQUATIONS

§17.1. 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 $m_1 \leq m_2 \leq \ldots \leq m_k$. 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 \( \leq 4 \):

<table>
<thead>
<tr>
<th>Length 1</th>
<th>Length 2</th>
<th>Length 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = 1</td>
<td>1 = ( \frac{1}{2} ) + ( \frac{1}{2} )</td>
<td>1 = ( \frac{1}{3} ) + ( \frac{1}{3} ) + ( \frac{1}{3} )</td>
</tr>
<tr>
<td>1 = ( \frac{1}{2} ) + ( \frac{1}{4} ) + ( \frac{1}{4} )</td>
<td>1 = ( \frac{1}{3} ) + ( \frac{1}{3} ) + ( \frac{1}{6} )</td>
<td>1 = ( \frac{1}{3} ) + ( \frac{1}{3} ) + ( \frac{1}{6} )</td>
</tr>
</tbody>
</table>

**Example 4:** Class equations of length \( \leq 3 \):

1. \( 1 = 1 \) corresponds to the trivial group;
2. \( 1 = \frac{1}{2} + \frac{1}{2} \) gives the class equation \( 2 = 1 + 1 \) which corresponds to \( C_2 \) only;
3. \( 1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6} \) gives the class equation \( 6 = 1 + 2 + 3 \) which corresponds to \( S_3 \) only;
4. \( 1 = \frac{1}{2} + \frac{1}{4} + \frac{1}{4} \) gives the class equation \( 4 = 1 + 1 + 2 \) which doesn’t arise in either of the two groups of order 4;
5. \( 1 = \frac{1}{3} + \frac{1}{3} + \frac{1}{3} \) gives the class equation \( 3 = 1 + 1 + 1 \) which corresponds to \( C_3 \) only.

§17.2. Some Elementary Tests for Potential Class Equations

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 cannot 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
If the class equation for a group $G$ 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 $g \not\in Z(G)$. Then $|C_G(g)| = N/n_i$ for some $i > m$. Since $g \in C_G(g)$, $Z(G)$ must be a proper subgroup of $C_G(g)$ 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 that $p$ 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 $pN = 1 + n_2 + n_3 + \ldots + n_{k-t} + Nst$ is the class equation for a group $G$ where $N > 1, t \geq 1$ and $n_{k-t} < N$ (that is, $G$ has precisely $t$ classes of size $N$).

Then: (i) $t | p - 1$ and
(ii) $N \equiv \frac{p-1}{t} \pmod{p}$.

**Proof:** Let $\Gamma$ 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 $\Omega$ 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 $\Gamma^s$ 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 $\Omega$. 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 $N = 72 \equiv 0 \pmod{3}$.
§17.3. The 2N Test

The largest possible 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 $\Gamma$ be a conjugacy class of size $N$.

Then $N$ is odd and the class equation for $G$ is $2N = 1 + 2 + 2 + \ldots + 2 + N = 1 + 2^{N-1}/2$.

**Proof:**

1. The elements of $\Gamma$ have order 2 and commute only with 1 and themselves: This is because the centralisers of these elements have order $2N/2$.

2. $H = G - \Gamma$ is a normal subgroup of $G$: $H$ clearly contains 1 and is closed under inverses. Let $x, y$ be distinct elements of $\Gamma$. 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.

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 $(hk)^2 = 1$.

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 $\Gamma$, are all of the form $\{h, h^{-1}\}$.

6. $N$ is odd.

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

§17.4. The 3N Test

**Lemma:** If $z = a + b\omega$ where $a, b \in \mathbb{Z}$ then $|z^2| \in \mathbb{Z}$.

**Proof:** Multiplying $z$ by its conjugate we get

$$|z|^2 = (a + b\omega)(a + b\omega^2) = a^2 + b^2 + ab\omega + ab\omega^2 = a^2 + b^2 - ab \in \mathbb{Z}.$$
Theorem 6 (3N Test): Suppose $|G| = 3N$ and $G$ has precisely 2 classes of size $N$. Then $|G'| = N$ and the class equation for $G$ is $3N = 1 + 3t_1 + 3t_2 + \ldots + 3t_k + N\cdot 2$ where $N = 1 + t_1\cdot 3 + t_2\cdot 3 + \ldots + t_k\cdot 3$ is the class equation for $G'$.

Proof: The elements of $\Gamma$ have order 3 and commute only with their powers. Suppose $\Gamma$ is a class of size $N$. If $\Gamma = \Gamma^{-1}$ then there exists $g \in \Gamma$ and $x \in G$ such that $x^{-1}gx = g^{-1}$. Then $x^2 \in C_G(g)$. But $|C_G(g)| = 3$ so $x \in C_G(g)$. Hence $g^2 = 1$, a contradiction. Hence the two conjugacy classes of size $N$ are $\Gamma$ and $\Gamma^{-1}$. By column orthogonality there must be a non-real entry in the $\Gamma$ column of the character table for $G$ and, since the eigenvalues of the corresponding matrix must be cube roots of 1, this entry must have the form $a + b\omega$ where $a, b$ are integers and $b \neq 0$.

The character table for $G$ contains the sub-table:

\[
\begin{array}{ccc}
\text{class} & 1 & \Gamma & \Gamma^{-1} \\
\text{size} & 1 & N & N \\
\chi_1 & 1 & 1 & 1 \\
\chi_2 & n & a + b\omega & a + b\omega^2 \\
\chi_3 & n & a + b\omega^2 & a + b\omega \\
\text{order} & 1 & 3 & 3 \\
\end{array}
\]

where $a, b \in \mathbb{Z}$ with $b \neq 0$.

By the lemma, $|a + b\omega|^2 = |a + b\omega^2|^2$ are positive integers and since the sum of squares of the entries in each of the last two columns is $3N/N = 3$, we must have $|a + b\omega|^2 = |a + b\omega^2|^2 = 1$ and all other entries in these columns must be zero.

So, by orthogonality with the first column, $0 = 1 + n(a + b\omega) + n(a + b\omega^2)$

$= 1 + n(2a - b)$,

so $n = 1$. Thus $G$ has at least 3 linear characters.

But if $\chi$ is any linear character then $\chi(\Gamma) \neq 0$ and so $G$ has exactly 3 linear characters and so $|G'| = N$. Clearly $G' = G - \Gamma - \Gamma^{-1}$.

The elements of $\Gamma + \Gamma^{-1}$ have centralisers of order 3 so can’t commute with any non-trivial element of $G'$. Hence if $1 \neq g \in G'$, $C_G(g) = C_G(g)$. Thus if $g \in G'$ has $t > 1$ conjugates in $G'$ then it has $3t$ conjugates in $G$.

Example 8: If $G$ has class equation $48 = 1 + 3 + 12 + 16 + 16$ then $G'$ has class equation $16 = 1 + 1 + 1 + 4 + 4 + 4$, which fails the Z Test.