§17 Number of Conjugacy Classes, Inner Automorphisms

In this section we look more closely at topics related to the action by conjugation of a group G on itself, i.e. the map $G\times G\to G$ sending g, x to $x^g = gxg^{-1}$, for $g\in G, x\in G$.

DEF The orbits in the action of G on itself by conjugation are called <u>conjugacy classes</u>. Elements x' and x in G are <u>conjugate</u> if they are in the same conjugacy class, i.e. if $x' = gxg^{-1}$ for some $g\in G$. The stabilizer of x in this action is denoted by $C_G(x)$, is called the centralizer of x, and consists of all the elements $g\in G$ which commute with x. We denote the number of conjugacy classes of G by $k(G)$.

THM A For each finite group G, and each element $x\in G$,
(a) the size of the conjugacy class containing x equals the index $|G/C_G(x)|$ of the centralizer of x, and is therefore a divisor of $|G|$;
(b) the number of conjugacy classes of G is given by

$$k(G) = \frac{1}{|G|}\sum_{g\in G} |C_G(g)|.$$

Proof. (a) This is a special case of THM B(4) on 16.4.
(b) This follows from the Cauchy-Frobenius formula on 16.5, since, in the conjugation action of G on G, g fixes $x \Leftrightarrow gxg^{-1} = x \Leftrightarrow x\in C_G(g)$.

THM B (Landau, $\simeq 1900$). If G is a finite group with $|G| = n$ and $k = k(G)$, then

$$\boxed{n \leq k^{(2^{k-1})}}$$

In particular, $k\to\infty$ for $n\to\infty$.

REMARK Much effort has been expended on getting larger lower bounds for k in terms of n than what $\boxed{}$ implies. The best bound so far is due to Pyber (1993).

Proof. Let A_j $(j=1,\ldots,k)$ be the conjugacy classes of G, and put $n_j = |A_j|$. Then

$$\checkmark \qquad n_1 + \cdots + n_k = n.$$

Put $m_j = n/n_j$. Then each $m_j \in \mathbb{N}$ and the largest m_j is n, corresponding to the smallest n_j, which is 1 — consider the conjugacy class $\{1\}$. From $\checkmark$ we get

$$(1) \qquad \frac{1}{m_1} + \cdots + \frac{1}{m_k} = 1$$

We may suppose

$$(2) \qquad m_1 \le \cdots \le m_k (= n)$$

Now $\square$ is the case $j=k$ of the following more general fact:

LEMMA If $m_1,\ldots,m_k$ are positive integers satisfying (1) & (2), then for $j=1,\ldots,k$,

$$(3_j) \qquad m_j \le k^{2^{j-1}}$$

Proof of Lemma. Since m_1 is the smallest m_j, (1) implies

$$(3_1) \qquad m_1 \le k.$$

For $1 \le j < k$, write (1) as

$$\checkmark\!\checkmark \qquad \frac{1}{m_{j+1}} + \cdots + \frac{1}{m_k} = 1 - \left(\frac{1}{m_1} + \cdots + \frac{1}{m_j}\right)$$

As in the proof of (3_1)

$$\dagger \qquad \text{left side of } \checkmark\!\checkmark \text{ is } \le \frac{k-j}{m_{j+1}} \le \frac{k}{m_{j+1}}$$

The right side is a positive fraction with denominator $m_1 \cdots m_j$ (or smaller after reduction), so

$$\ddagger \qquad \text{right side of } \checkmark\!\checkmark \text{ is } \geqslant \frac{1}{m_1 \cdots m_j}$$

It follows from $\checkmark\!\checkmark$ and $\dagger$ and $\ddagger$ that for $1 \le j < k$,

$$\star \qquad m_{j+1} \le k\, m_1 \cdots m_j$$

Assuming that (3_i) is true for all indices i with $1 \le i < j$, it follows from $*$ that

$$m_{j+1} \le k \cdot k^{1+2+\cdots+2^{j-1}} \doteq k^{1+(2^j-1)} = k^{2^j},$$

which proves (3_j). This completes the proof, by induction, of the Lemma.

Here is a cute inequality which has been used in some of the work on $k(G)$:

THM C. For each finite group G, and each $N \lhd G$,

$$k(G) \le k(G/N)\,k(N).$$

Proof. We will use the formula in Thm A(1), for G, G/N and N. Since

$$|G| = |G/N|\,|N|,$$

it will suffice to prove that

$$(*)\qquad \sum_{g\in G} |C_G(g)| \le \sum_{f\in G/N} |C_{G/N}(f)| \sum_{n\in N} |C_N(n)|.$$

For each $g \in G$,

$$C_G(g)/(C_G(g)\cap N) \simeq C_G(g)N/N \subseteq C_{G/N}(gN),$$

the $\simeq$ by the 2nd isomorphism theorem and $\subseteq$ since $h\in C_G(g) \Rightarrow hN \in C_{G/N}(gN)$.
It follows that

$$(\checkmark)\quad \sum_{g\in G}|C_G(g)| \le \sum_{g\in G} |C_{G/N}(gN)|\,|C_G(g)\cap N| = \sum_{f\in G/N} |C_{G/N}(f)| \sum_{g\in f} |C_G(g)\cap N|.$$

For each $f \in G/N$, the inner sum on the right in $\checkmark$ is

$$(\checkmark\!\!\checkmark)\qquad \sum_{g\in f}\ \sum_{\substack{n\in N\\ gn=ng}} 1 = \sum_{n\in N}\ \sum_{\substack{g\in f\\ gn=ng}} 1 = \sum_{n\in N} |C_f(n)|$$

the set of $g\in f$ with $gn=ng$

Thus to get from $(\checkmark)$ and $(\checkmark\!\!\checkmark)$ to $(*)$ it suffices to show that

$$(\#)\qquad |C_f(n)| \le |C_N(n)| \quad \text{for each } f\in G/N \text{ and each } n\in N.$$

Each $f \in G/N$ is of the form $f = hN$ for some $h \in G$. Thus

$$g \in C_f(n) \Leftrightarrow g = hm \text{ for some } m \in N \text{ and } n^g = n$$
$$\Rightarrow n^{hm} = n$$
$$\Rightarrow n^m = n^{h^{-1}}.$$

If m_1 is any one of these m's, then each of the m's satisfies

$$n^m = n^{h^{-1}} = n^{m_1}, \text{ so } m \in m_1 C_N(n),$$

so $g \in hm_1 C_N(n)$, which is a certain coset in G of $C_N(n)$, of size $|C_N(n)|$.

THM D For each $g \in G$, the conjugation map $x \mapsto x^g$ from G to G is an automorphism π_g of G, and the map $\pi : G \to \mathrm{Aut}(G)$ given by $g \mapsto \pi_g$ is a homomorphism from G to $\mathrm{Aut}(G)$, with kernel $Z(G)$ and image $\mathrm{Inn}(G)$, the set of all <u>inner automorphisms</u> of G; so

$$(1) \qquad \mathrm{Inn}(G) \simeq G/Z(G).$$

Furthermore,

$$(2) \qquad \mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G).$$

Proof We know $x \mapsto x^g$ is a permutation of G, for each $g \in G$, and the map $\pi : g \mapsto \pi_g$ is a homomorphism from G to S_G. In fact the map is into $\mathrm{Aut}(G)$ since each π_g is a homomorphism from G to G:

$$\pi_g(ab) = (ab)^g = gabg^{-1} = gag^{-1}gbg^{-1} = \pi_g(a)\pi_g(b)$$

We have $g \in \ker\pi \Leftrightarrow \pi_g = 1_G \Leftrightarrow a^g = a \ \forall a \in G \Leftrightarrow g \in Z(G)$.
The first isomorphism theorem now gives (1). Finally for each $g \in G$ and $\alpha \in \mathrm{Aut}\, G$, and each $a \in G$

$$(\alpha \pi_g \alpha^{-1})(a) = \alpha(\pi_g(\alpha^{-1}(a))) = \alpha(g\alpha^{-1}(a)g^{-1}) = \alpha(g)\, a\, \alpha(g)^{-1} = \pi_{\alpha(g)}(a),$$

giving $\alpha \pi_g \alpha^{-1} = \pi_{\alpha(g)} \in \mathrm{Inn}(G)$. Thus $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$.